Pontifícia Universidade Católica
do Rio de Janeiro

Luísa Cruz Lobato

Unraveling the cyber security market:

The struggles among cyber security companies and the production of cyber (in)security

Dissertação de Mestrado

Thesis presented to the Programa de Pós-Graduação em Relações Internacionais do Instituto de Relações Internacionais, PUC-Rio, as a partial fulfilment of requirements for the degree of Mestre em Relações Internacionais.

Advisor: Prof. Monica Herz

Rio de Janeiro
June 2016

Pontifícia Universidade Católica
do Rio de Janeiro

Luísa Cruz Lobato

Unraveling the cyber security market:

The struggles among cyber security companies and the production of cyber (in)security

Thesis presented to the Programa de Pós-Graduação em Relações Internacionais do Instituto de Relações Internacionais, PUC-Rio, in partial fulfilment of requirements for the degree of Mestre em Relações Internacionais.

Profa. Monica Herz
Advisor
Instituto de Relações Internacionais – PUC-Rio

Profa. Anna Gudrun Christina Leander
Instituto de Relações Internacionais – PUC-Rio

Prof. Luis Manuel Rebelo Fernandes
Instituto de Relações Internacionais – PUC-Rio

Profa. Monica Herz
Coordinator of the Centro de Ciências Sociais – PUC-Rio

Rio de Janeiro, June 2nd, 2016.

Luísa Cruz Lobato

The author graduated in International Relations from Universidade da Amazônia (UNAMA), in 2012.

Bibliographic data

Lobato, Luísa Cruz

Unraveling the cyber security market : the struggles among cyber security companies and the production of cyber (in)security / Luísa Cruz Lobato ; advisor: Monica Herz. – 2016.
171 f. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, 2016.

Inclui bibliografia

1. Relações internacionais – Teses. 2. Segurança cibernética. 3. Companhias privadas. 4. Pierre Bourdieu. 5. Práticas. 6. Produção de segurança. I. Herz, Monica. II. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. III. Título.

CDD: 327

To my parents, Marina and Tarcisio, for
the unconditional love and support.

Acknowledgements

I would like to express the deepest appreciation to professor Monica Herz for supporting me and for believing in my work, no matter how challenging it appeared to be.

I would like to thank CNPq and PUC Rio for the institutional support without which this work would not come to life.

Thank you to professor Anna Leander, for challenging me by always asking the hard questions.

Thank you to my undergraduate professor, Mario Amin, for believing in my potential.

To the precious friends I made at PUC Rio and UNAMA, specially my dear friend and professor Brenda de Castro, for encouraging me to apply to the Master's, in the first place and for the unceasing advice in the course of these two years.

A warm thank you to my long-term "Fantastic Four" members, Giovanna, Haron and Meg, for keeping our bonds strong and emotionally supporting me, no matter how far from home I am.

And demonstrating the relevance and complexity of the technological developments investigated in this research, I appreciate all the help, love and support of one of the best friends I have: Juh, a person I could not have met if it weren't for those little, "dim", corners of the fandoms communities in the Internet.

I would like to dedicate a special and wholeheartedly thank you to my dearest friend, love and partner Miguel, for emotionally supporting me every time I need; for believing in my potential; for listening, questioning and debating this work with me; for being the first and main reviewer of the countless versions of this work; and for never giving up on me.

Thank you to all the friends and relatives who somehow encouraged and helped me.

I am grateful to my father, Tarcísio, for all the love and care, for everything that has been sacrificed for my well-being and education and for encouraging me so hard to embrace the academic life.

Finally, I cannot properly express how grateful I am to my mother, Marina, a person who has been like a true guiding light in the middle of a tempestuous storm. Thank you for being my best friend and confident. Thank you for doing absolutely everything for me.

Abstract

Lobato, Luísa Cruz; Herz, Monica (Advisor). **Unraveling the cyber security market: the struggles among cyber security companies and the production of cyber (in)security**. Rio de Janeiro, 2016. 171p. MSc. Dissertation – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

This dissertation examines the role of cyber security companies in the production of contemporary cyber security. The increasing pressures to securitize cyberspace have contributed to the growth of a lucrative market oriented at providing cyber security products and services to commercial and government customers. Using a Bourdieu-inspired framework, the work: analyzes the historical conditions under which information technologies gained ground within security debates; identifies the positions and investigates the practices of cyber security companies within the cyber security field and analyzes the ongoing struggles for the production of cyber security. Risk-based thinking is a cornerstone of the process of conceiving and commercializing products and services advertised by companies. In this sense, it is argued that both risk-based thinking and the commercial practices of cyber security companies produce specific forms of security. The work identifies three distinct forms of security produced within the field: defensive security, offensive security and active defense. It analyzes the implications of each form to the overall security of cyberspace and argues that whilst the majority of companies adopt an active defense approach in their products and services, some of them are leaning towards more offensive solutions to deal with current risks. It concludes the analysis with some thoughts on the implications of the current dynamics of the cyber security market for security and Internet governance.

Keywords

Cyber Security; Private Companies; Pierre Bourdieu; Practices; Production of Security.

Resumo

Lobato, Luísa Cruz; Herz, Monica (Orientadora). **Decifrando o Mercado de Segurança Cibernética: as disputas entre as empresas de segurança cibernética e a produção da (in)segurança cibernética**. Rio de Janeiro, 2016. 171p. Dissertação de Mestrado – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

A presente dissertação investiga o papel das companhias de segurança cibernética na produção da segurança cibernética contemporânea. A crescente pressão para securitizar o ciberespaço contribuiu para o crescimento de um lucrativo mercado voltado para a provisão de produtos e serviços para clientes comerciais e governamentais. Utilizando uma perspectiva inspirada em Bourdieu, o trabalho: analisa as condições históricas nas quais as tecnologias da informação ganharam terreno no debate de segurança; identifica as posições e investiga as práticas das companhias de segurança cibernética no campo da segurança cibernética e analisa as disputas em andamento pela produção da segurança cibernética. Abordagens voltadas ao risco são pilares na concepção e comercialização de produtos e serviços anunciados pelas companhias. Neste sentido, argumenta-se que ambas as abordagens voltadas ao risco e as práticas comerciais das companhias de segurança cibernética produzem formas específicas de segurança. O trabalho identifica três distintas formas de segurança produzidas no campo: segurança defensiva, segurança ofensiva e defesa ativa. Analisa-se as implicações de cada forma para a segurança, de um modo geral, e argumenta-se que, enquanto grande parte das companhias adota uma estratégia de defesa ativa em seus produtos e serviços, algumas tem se orientado para a adoção de medidas mais ofensivas para lidar com os atuais riscos. A análise é concluída com algumas reflexões a respeito das implicações das atuais dinâmicas do mercado de segurança cibernética para a segurança e governança da Internet.

Palavras-chave

Segurança Cibernética; Companhias Privadas; Pierre Bourdieu; Práticas; Produção de Segurança.

Table of Contents

List of Tables

Abbreviations

Advanced Persistent Threat (APT)

Association of Southeast Asian Nations (ASEAN)

Computer Science and Telecommunications Board (CSTB)

Critical Infrastructure Protection (CIP)

Critical Informational Infrastructure Protection (CIIP)

Department of Defense (DoD)

Department of Homeland Security (DHS)

European Union (E.U.)

Federal Bureau of Investigation (FBI)

Information and Communication Technologies (ICTs)

Information Technology (IT)

International Relations (IR)

Internet of Things (IoT)

National Security Agency (NSA)

North Atlantic Treaty Organization (NATO)

Public-Private Partnerships (PPPs)

United States (U.S.)

Information is power. But like all power, there are those who want to keep it for themselves.

Aaron Swartz, *Guerrilla Open Access Manifesto*

1. Introduction

The commonsense leads people to see information and communication technologies (ICTs) as a constitutive aspect of contemporary developed and developing societies, despite the existence of a digital gap between those with access to the Internet and a majority that is still deprived of it. In societies where these technologies have been successfully diffused, their pervasiveness in the execution of everyday tasks is so evident, and they have become so naturalized, that people tend to forget how much they depend on their correct and uninterrupted operation to do the most basic operations, such as shopping for supplies in the local supermarket or sending an e-mail to set or cancel a meeting, for example. It has become so natural that users have either forgotten or never been aware of what remains underneath the "surface[1]."

Annually, governments and private companies host hacking competitions across the world. The world's largest competition, DEF CON, happens in Las Vegas, in the United States (U.S.), since 1993. The event is attended by journalists, computer security professionals, lawyers, U.S. federal government employees, security researchers, students and *hackers*, and consists of speeches, social events and contests. These events are pools for companies and government agencies seeking specialized workforce and they are important in that they uncover security breaches and allow for the development of new software. In a *hacking* contest hosted by Google, in 2012, the former vulnerability company VUPEN gained worldwide fame when it refused to share with Google a newly discovered flaw in the Chrome Web browser. The company's CEO justified the reason it did so: "We wouldn't share this with Google for even $1 million," he said. "We don't want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers." (BEKRAR *apud* GREENBERG, 2012) (One of these customers was the U.S. government itself.) VUPEN has ceased its businesses and its CEO has founded a new company in the U.S. named ZERODIUM. The business of vulnerability exploit, however, still seems to be up.

[1] In the Internet language, the term "surface" refers to the layer of the Internet that is readily available to users and searchable through search websites, such as Google (also said to be "indexed"). There is a layer that is not directly accessible to users with the basics of the Internet, called the Deep Web.

VUPEN's behavior has partially uncovered some of the Internet dynamics that remain concealed from the everyday user. But as troublesome as it seems, it is still the tip of the iceberg. These dynamics involve intense disputes and adaptive alliances between private corporations and governments, conflicting interests between hackers and their governments and the active engagement of national security experts in trying to frame a given scenario as a threat.

Most users have little clue of the extent of the – sometimes very secretive – ongoing power struggles to control information fluxes. These struggles involve a multiplicity of public and private stakeholders and may affect, either directly or more subtly, the way people experience the Internet. They address issues of privacy and surveillance, security and freedom, and to a certain extent, all converge to a topic that has become quite a commonplace in the universe of policy-making. The name is cyber security.

The present research investigates the practices of private companies and their implications for cyber security. The research strategy adopts a Bourdieu-inspired approach to practices, considering the 'space' where these companies struggle for influence as *fields* and the services, advertisements and the discourses they offer as constituents of these practices. The main objective is to understand the role that a particular kind of private companies, labeled cyber security companies, plays in 'securing' cyberspace and the implications of their practices for 'security.' Fundamental to this purpose is to investigate how pressures to 'secure' cyberspace have contributed to the legitimation of these actors' practices and over which bases this process happens. Specifically, the work will analyze (1) the relationship that has been built between these agents and government actors, which the work will address as the phenomenon of the 'marketization of cyber security;' (2) the struggles between companies and between these and other actors for the rising cyber security market, as well as the practices employed; and (3) the role of 'risk' in the process of securing cyberspace.

This is relevant for understanding the dynamics of cyber security and its lucrative market as well as the consequences of private security not only in terms of the political arrangements it gives birth to, but also to individual privacy and political accountability.

The dissertation works with two main hypotheses. The first hypothesis considers that recurrent pressures to secure cyberspace have led to the development of

a dynamical cyber security market. One side of this market aims at securing cyberspace against cyber threats through the commercialization of cyber security solutions, from antiviruses to more specific and directed services oriented at identifying security breaches in computer systems. The other side of this market is oriented towards commercializing and exploiting 'insecurities' in computing devices, networks and critical infrastructures. This exploitation can happen when companies sell and operate invasive surveillance technologies for governments, or when they commercialize with governments distinct and sometimes obscure services, such as malwares, viruses, access to Internet Protocols (IPs) of public authorities' computers in foreign countries and so forth.

The second hypothesis is that risk-based thinking has become constitutive of the *habitus* of the agents in the field of cyber security. On the one hand, it is useful for making sense of a myriad of cyber threats and for justifying certain perceptions of security carried out by governments, security experts and the private sector. On the other hand, it orients the very actions of private companies in what concerns the development of security products and services. This mode of thinking is grounded on fundamental assumptions of the information society thesis, which addresses the implications of the development of information and communication technologies (ICTs) to societies. By orienting perceptions and actions towards cyber-threats, a risk-based thinking has implications for the solutions that are conceived to address them. In this sense, this 'background knowledge' of the cyber security field may lead to very specific forms of framing and responses to perceived cyber threats. A risk-based approach to cyber security may legitimize the adoption of preemptive measures to anticipate highly uncertain scenarios. It may as well mask certain forms of exploitation of cyberspace as 'solutions' to mitigate security risks.

Cyber security

For Hansen and Nissenbaum (2009), the term "cyber security" was first used in the early 1990s to stress the insecurities related to networked computers. It differs a little from the exclusively technical emphasis of computer/information security because of the potential devastating effects that digital technologies could have in society. In the Computer Science and Telecommunications Board (CSTB) report "Computers at risk: safe computing in the information age" these devastating

effects are seen as 'risks,' increased by the dependence on computers. The CSTB report (1991) argues that as much as these machines are trusted, they are vulnerable. The threats that could explore these vulnerabilities range from criminal and terrorist activities to systemic failures of hardware and software. The latter threats represent an "inherent ontological insecurity within computer systems" (HANSEN; NISSENBAUM, 2009:1160) stemming from their unpredictable and uncertain behavior.

The topic became popular in the last decade, triggered by a series of worldwide events and by experts' discourses. The cyber-attacks[2] against Estonia and Georgia, between 2007 and 2008, and the uncover of the Stuxnet exploit[3] to an Iranian nuclear power plant in 2010 figure as the most relevant 'cyber' incidents that gained broad international relevance. In the meanwhile, the body of policy-papers and books dealing with the topic only grew from the 1990s to the present.

These incidents are but a small parcel of the cyber-attacks launched on a daily basis against individuals, private companies, governments and non-governmental organizations. According to a report of the US Bipartisan Policy Center's Homeland Security Project (2012), between October 2011 and February 2012, over 50.000 cyber-attacks on private and governmental networks were reported to US Department of Homeland Security (DHS). The document considers that these incidents are representative of a small fraction of daily attacks directed against the country's informational infrastructure. Worldwide, the number multiplies to millions or even billions daily. The Symantec's 2014 Internet Security Threat Report shows that around 568,700 web attacks were blocked per day in the last year. The year faced 253 data breach incidents, a number 16% higher than in 2012. These breaches resulted in the exposure of at least 10 million identities in an only incident. In the totality, around 552 million identities were exposed that year, a number 493% higher than in 2012.

[2] A cyber-attack is an offensive that targets the theft, destruction or alteration of computing devices, infrastructures and networks. There are several categories of cyber-attacks. Among them, are the Distributed-Denial-Of-Service (DDoS) attacks, which overwhelm servers' capacities with illegitimate information requests originating from multiple sources, the so-called "zombie" computers remotely run by a central data processor. This category of attack was deployed against Georgia and Estonia.

[3] The stuxnet is a worm, a malware computer program that replicated itself to infect other computers. It was developed to attack Siemens' control systems and it damaged the centrifuges used in Iran's nuclear program. The worm is considered the most successful cyberattack to date in terms of material effects. See Dunn Cavelty (2011).

Similar to the early CSTB report's characterization, the DHS regards cyber security as the securing of the cyberspace and its underlying infrastructure against a wide range of 'risks' (DHS, 2015). In the same vein, the International Telecommunications Union (ITU) understands it as the attempt to ensure the attainment and maintenance of security properties of cyber environment's organization and user assets, which involves the totality of transmitted and stored information online, against relevant security risks (ITU, 2008). The ITU considers cyber security in relation to distinct threats against data communication. These are the theft, destruction, removal or loss of information or other resources, the corruption or modification of information, the disclosure of information and the interruption of services. Activities like espionage and cyber-crime are currently seen as the main and most pressing 'threats' in cyberspace (CSIS, 2011).

Cyber security, thus, comprises the attempts to protect digital information, flowing through vulnerable networks or stored in vulnerable databases, from internal disruption or from disruption by 'malicious' third parties. The diffusion of the use of computer technologies in society, whereas it was originally a defense project employed by some research networks, has fed some concerns with the security of the informational fluxes and the material that assures their uninterrupted functioning. Cyber security is, today, understood as a primary national security concern in the US (CSIS, 2008; 2010; 2011).

As it is possible to observe in the definitions presented above, the entanglement between cyber security and national security tends to be made in terms of the risks that vulnerabilities in security systems and networks may pose to the latter and to international security as well (see, for example, CLARK; KNAKE, 2010; BRITO; WATKINS, 2011). The CSTB report (1991) argues that computer risks and the societal effects they may generate dialogue with the field of security, which has been traditionally discussed in terms of vulnerabilities, threats and countermeasures. As a reaction to a scenario of uncertainty, risk seems to play an important role in orienting the imaginary and practices concerning technology, in general, and cyber security, in particular. It is also an essential component of the threat-framing process, as it refers to what agents interpret as unsecure and how they will answer to it (DUNN CAVELTY, 2008). Experts say that the risks faced by computers are due to their vulnerability (to third parties' exploitation or to systemic failures, for example). Accordingly, advances in IT and the increased

dependence on these systems would result in a decreasing capacity to control risk and secure information (DUNN CAVELTY, 2008).

There has been a certain inflation of the cyber threat in political circles and by the industry, particularly regarding the risks it poses to national security, critical infrastructure, and concerns with an eventual 'cyber war' (CARAFANO, 2015; ARQUILA; RONFELDT, 1993), with the possibility of 'cyber-terrorism' and with the use of military language to address cyber-threats (DUNN CAVELTY, 2012).

This overemphasis on the cyber threat has been pointed as responsible for fueling the multibillionaire market of cyber security (BRITO; WATKINS; 2011; DEIBERT; 2011). As the numbers presented above may indicate, pressures to secure cyberspace turn out to be a great business opportunity for private companies, which struggle for a parcel of the cyber security market. Yet, considering how cyber security seems to be linked to private enterprise, one has to question what this cyber security market is about and what would be the consequences of what Anderson (2001) calls 'perverse incentives'?

Private actors

As a core aspect of the Internet governance (DENARDIS, 2014), existing attempts to ensure security in cyberspace bump into the specificities of the historical and technical development of ICTs. The particular, almost innate, distributed architecture of the Internet is one of its strongest characteristics, but also a source of concerns in security policy making circles, because of the potential vulnerabilities it may create. The ownership and operation of cyberspace is another case-in-point, and one to which governments have played a special attention. Profit and non-profit private actors share the responsibility for the ownership and operation of virtual infrastructures and the physical infrastructure that allows its functioning. Hence, national security concerns are dependent on the private sector, which has been a main driver in the evolution of ICTs.

A lot of attention has been given to the role of the state in shaping cyber security (GOLDSMITH; WU, 2006; ERIKSSON; GIACOMELLO, 2009; BETZ; STEVENS, 2011), but the same does not occur when other agents involved in disputes over the definitional and practical aspects of cyber security are concerned. This is worrisome when one considers the importance of the private sector, and in

particular of private companies, which can be primarily distinguished from other private agents because of their profit-seeking activities, for the maintenance and operation of cyberspace. There are groups of private companies that hold a special relation to (and concern with) cyber security: banks, risk-management corporations, IT firms, and so on. A whole market of software and services is oriented towards the protection of corporate and private information against security breaches. Cyber security and the private sector are a topic of strategic interest of some actors in the US government, according to whom the protection of the country's critical infra-structure is a joint task between public and private actors[4] (DHS, 2015).

Perverse incentives

Private companies not only contribute to the development of core information technologies; they concurrently play an important role in the production of security in the virtual domain, either by developing software and hardware, by running *online* platforms and networks or by commercializing products and solutions to make the *online* experience more 'secure.' Technology development and the security concerns that follow are symbiotic in the sense that together with the development of information technologies comes the development (or not) of security solutions for the use of these technologies.

Perverse incentives refer to the negative outcomes of the interaction between economics and computer security, on one hand, and of the political and market choices of companies, on the other. They are also related to the structure and functioning of most IT markets, which are marked by the competitive development of applications and by corporate warfare. To either entrench or undermine monopolies, companies have had a tendency to develop flawed systems with an obscure architecture, or rather opted for 'security by obscurity' in order to increase the investment that competitors might make to create compatible products. The politics of product development are one aspect of these incentives. But in this competitive environment, companies have also, for some time, opted for feeding an

[4]The DHS coordinates the information sharing between federal agencies and the private sector, stressing the strong interdependency of infrastructure systems across the US, both virtual and physi-cal.

information warfare scenario, on the basis that in the complex universe of cyber-space, offense tends to be easier than defense (ANDERSON, 2001).

The market in which these companies act is diversified and includes commercial, governmental, organizational and individual customers, all of which, to different degrees, sustain their own interests and practices regarding cyber security and the usability of cyberspace. The market is a core part of the *field* of cyber security, and is particularly important in that it is the *locus* of most of the practices that produce and shape its contours.

Division of the work

To give the reader a robust understanding of the dynamics and implications of current practices in the cyber security market, the work will be divided in four chapters. In a first moment (chapters 1 and 2), the idea is to familiarize the reader with the research strategy, as well as with the theoretical and historical accounts of the research object. In a second moment (chapter 3), the intention is to present the empirical application of the concepts and the context explored in chapters 1 and 2 to the reader. Then, the work discusses the tendencies manifested in the practices of the companies analyzed (chapter 4). Lastly, (chapter 5), the work develops a critical analysis of the implications, for cyber security, of the practices of cyber security companies and the political arrangements between these actors and government agencies. This way, the aim is to provide the reader with an understanding of the contributions of a Bourdieu-inspired approach to cyber security and to international relations, as well as an overview, followed by a critical analysis, of the consequences of the practices adopted by agents struggling within this field.

The first chapter discusses the theoretical framework of the dissertation. This framework involves a double investigation: firstly, on the contribution of private security studies for understanding the practices of private companies in cyber security; and, secondly, on the relevance of Bourdieu's sociology as an analytical ground for making sense of these agents' practices, the struggles they become involved with and the nature of other actors within the cyber security field (sections 2.5. and 2.6.). The main argument developed in the course of the chapter is that Bourdieu's sociological theory is relevant for making sense of the working and

implications of private security in international relations (IR), on the one hand, and of the dynamics within the field of cyber security, on the other. A reading of cyber security as a social 'field' or '*champ*,' where agents struggle for political influence, allows visualizing how the practices of private companies within it are constituted by attempts to influence, through their services, advertisement, risk-oriented practices and discourses, the politics of the field. In what concerns the contributions to private security studies, the "thinking tools" and the Bourdieusian sociological approach are fruitful for visualizing the patterns of conflict and cooperation among private companies and governments that often escape the conventional reading of 'privatization,' as the transfer away of security functions from the government to the private sector.

In this regard, the chapter employs the concept of marketization of security as an alternative to the conceptual limitations of the term 'privatization', as the former embraces more complex arrangements between public and private agents within the context of international security (section 2.2.). The central argument for the term marketization is that it makes possible the analysis of the hybrid relations between public and private actors and of the implications of such enmeshment. Subsequently, the chapter analyzes the formation of "industrial complexes," or alliances between governments and private industry, as a direct implication of these dynamics (section 2.3.) and investigates the correlation between private security and cyber security, sustaining that the phenomenon of the "marketization" of security has been important in this context, once the technologies that anchor cyber security have been developed in a 'hybrid' context of public-private initiatives and arrangements, and these patterns have marked the formulation and application of cyber security policies in the United States (section 2.4.).

The chapter also situates the private security debate within the context of security studies in IR (section 2.1.). Processes of broadening and deepening of 'security' are open contestations to dominant readings of the discipline, and allowed the involvement of a variety of subjects and objects to the realm of international security, including both the debates over private security and over cyberspace as a source of (national and international) insecurity.

The second chapter analyzes the evolution of ICTs and the perceptions that have been built to make sense of their impact on society. The process of sketching the history of information technologies is important for apprehending the space of

positions and position-taking in the field of cyber security, as well as a necessary step in the identification of the background knowledge that sustains and gives sense to the practice of the agents within the field of cyber security. For such purpose, the chapter analyzes the information society thesis and its treatment within the discipline of IR (section 3.1.). The argument is that the attempts made by exponents of the thesis to make sense of technological changes have contributed to reshaping security thinking, by altering fundamental perceptions about the nature of security threats. The chapter shows that the private sector has played an important role in this sense, as the exponential development of computer and networked technologies and their diffusion to society have been closely related to the 1980s privatization of cybernetic technologies. But these technologies have not been simply privatized: from their inception, the process that best describes their evolution is that of marketization. As it will be argued, the development of ICTs has been marked by an interesting combination of public funding and private initiative, on the one hand, and its diffusion has been boosted by the commercialization of such technologies, on the other (section 3.2.).

The central argument of the chapter is that ICTs and the perceptions of their impacts on society are part of a broader effort to legitimate the cyber security market. These two phenomena have contributed to fundament and boost existent regimes of justification in cyber security. As the argument goes, it is sustained that the strong presence of the market in the development and operation of information technologies strongly influences how to think and conceive the security issues that arise because of them. The debate on Critical Infrastructure Protection (CIP) illustrates very well this phenomenon, as it has been associated with threats coming from and because of cyberspace (section 3.3.). The association between critical infrastructure and information technologies has been fundamental to the cyber security debate, as it relies on a vision of threats associated to risks and vulnerabilities in informational systems.

The CIP debate is also helpful in situating the place of risk in the field of cyber security. The chapter argues that risk-based thinking is part of the background knowledge that orients agents' practices in the field, and has become almost inseparable from cyber security, which has been marked by a confluence of distinct, but complementary, positions regarding uncertainty (section 3.4.). The marketization of ICTs is strategic in that it has contributed to the centrality of risk-based thinking

within cyber security. This naturalization of threat-assessment in terms of risks, in turn, sets forth the possibility for agents invested with the power to mobilize risk-based arguments to play a central role in the characterization and definition of what constitutes a threat and what constitutes a necessary measure to strengthen security.

The third chapter is the empirical part of the work. It analyzes mainly what the work addresses as the 'cyber security market.' This market is deeply entangled to the very field of cyber security and the practices that take place in its context can directly alter the perceptions towards security in cyberspace, privacy and international security (for example, when companies commercialize military, ICT solutions with governments for purposes of policing and war-making). The main objective is to situate the practices of private companies within the field of cyber security. For that purpose, the chapter applies the theory discussed in the previous chapters to initially provide a mapping of the struggles within the field. This involves the identification of the main agents concerned, their positions and interests and the conflicts between them (section 4.1). The aim is to give the reader a situational framing of the existent struggles in the field in the recent years, as well as a visualization of the most relevant and influential practices of agents. This scenario helps capturing some of the most central points of convergence and divergence between agents, as well as the way by which these agreements and disagreements contribute to shaping cyber security.

In a second moment (section 4.2.), the chapter is dedicated to analyzing the practices of three categories of private companies: antivirus or endpoint security companies, cyber security companies and defense contractors providing cyber security services. It analyzes the practices of traditional businesses and new start-ups alike, considering the extent of their relationship with governments and other companies in the process. The main argument is that it is important to pay attention to the practices of these companies in order to understand the functioning of the cyber security market. It is through practices enacted in this market that these companies may actually produce cyber security and, thus, influence the dynamics in the cyber security field.

In the analysis of the advertisements of companies' products and services, three dominant approaches to cyber security are identified: defensive security, offensive security and active defense. These three forms of security are marked by the kind of approach they make to risk and uncertainty. The chapter analyzes the

characteristics of these forms of security in the context of the companies and solutions that support each. The predominance of active defense in the solutions' portfolio was a pattern found in the research.

The fourth chapter analyzes the patterns the work has found, as well as their implications for the idea of security. The aforementioned approaches to cyber security are a manifestation of the disputes between private companies in the field, and serve as strategies for assuring a place in the market (section 5.1.). These disputes are also evident in the arguments for a certain solution, rather than the others (subsection 5.1.1.). The argument is that opting for active defense based solutions is strategic to the companies' relation with state-actors, particularly because it relies mostly on an anticipatory, prevention-focused, approach to security (subsection 5.2.1.). Active defense is marked by near-offensive measures against an intrusion as a justification for enhancing the possibility of anticipating potential attacks. These measures include, but are not restricted to: geolocalization and IP tracking, threat intelligence gathering and intelligence, broadly speaking; annoyance measures so as to induce the attacker to commit mistakes; and offensive measures that include hacking back. As argued in subsection 5.1.3., the predominance of this approach is further facilitated by the entanglement between governments and private companies, once that the established bridges between the two spheres have contributed to the sharing of threat-perceptions and potential security solutions.

The chapter also establishes the argument that active defense has further implications for the concept of security (section 5.2.). It can be regarded as a security paradigm that authorizes the adoption of security measures as a form of risk anticipation, and is rooted on the utopic dream of a riskless cyberspace.

The fifth and concluding chapter casts a critical analysis of the tendencies identified in the third and fourth chapters. Its main focus is on the implications of the marketization of security in cyberspace for security and privacy. The chapter pays a particular attention to the relationship between private companies and governments and analyzes the implications of this relationship in the form of political arrangements between these actors. As a result from the analysis carried out in chapter three, it identifies two particular arrangements: one between the cyber security industry properly said (which includes cyber security companies, the antivirus industry and defense contractors) and the government; and the other

between other kinds of information technology companies, such as telecommunication companies and internet/online service providers (ISPs and OSPs). These arrangements vary in their nature (as the first one is strongly marked by cooperation and the second marked by more conflicting relations) and in the way security is produced by private companies in each case (section 6.2).

In the chapter, it is argued that the struggles to assert power over the internet have resulted in or reinforced these political arrangements between private companies and governments. The main concern is with how those arrangements seeking to explore the potentials of offensive or near-offensive cyber security solutions affect security and privacy in cyberspace, as well as with the implications for international security.

The relationship between cyber security and markets is analyzed at the beginning of the chapter (section 6.1.). By taking the current approaches to cyber security as a part of a paradigm of security based on securing 'fluxes' (of people, of information, and so on), the chapter explores the three consequences of this paradigm. Firstly, the strong logic of the market is part of the provision of cyber security and has contributed to its commodification, contributing to establishing a 'culture of fear' over cyber threats; secondly, it leads to a differentiation in the provision of security based on costs, in which the efficacy is amenable to how much one can pay to have it; and thirdly, involves the constitution of public-private arrangements in cyber security policy-making.

The chapter calls attention to the impacts of these struggles both in the U.S. field and beyond. The argument is that the networked nature of current information technology devices makes this field particularly relevant in a global scale. The struggles and their particular outcomes in the U.S. context may affect other parts of the world, as it happened with the revelations of the NSA's global surveillance program (section 6.3.). Companies originally operating within the U.S. field expand to other parts of the globe to seize lucrative opportunities, some of which are not exactly legal or morally acceptable in their host countries.

The consequences of these tendencies to global governance are also addressed in the chapter (subsection 6.2.1.). It is argued that in the long term, it becomes difficult to visualize any of the identified actors actually controlling the internet by themselves. Thus, there is a tendency that existent political arrangements between relevant and powerful actors in the field prevail or be slightly modified to

accommodate certain conflictive interests. The chapter shows that the broader tendency in internet governance is that it keeps being marked by a tension between attempts to assure the uninterrupted flow of information and attempts to filter, control and interrupt it and urges for a more careful attention to the political arrangements underneath such tensions.

Cyber security has become a pressing security concern in many countries, with the U.S. on the lead. The marketization of computer technologies, with the public funding and private development that accompanied their development, and the security concerns that became crescent with their diffusion into society, have set the stage for the formation of political arrangements oriented to mitigating the vulnerabilities and risks perceived as inherent aspects of computer technologies. The process of broadening the object of security in the field of security studies within IR has enabled for the topic to be a part of the debates in the discipline. The inherent vulnerabilities in systems and the risk of internal/external interruption of informational fluxes, materialized in the CIP debate, seem to be now pressing security concerns that could not only affect a given territory, but also diffuse globally. A new paradigm of security, anchored on a risk-based thinking and on attempts to secure information fluxes, reinforces the position that cyber security has acquired in security debates both in policy-making circles and in the academia. The participation of the markets in the production of security practices, however, raises fundamental issues concerning existent accountability mechanisms, something that should not remain obscured by a hyped perception of cyber threat.

2. The relevance of Bourdieusian thinking tools for understanding private security

The present chapter undergoes an analysis of Bourdieu's thinking tools and their relevance for understanding the practices of private companies in what concerns cyber security. For this purpose, it will be divided into two main sections that will discuss, consecutively, the contributions of private security studies in situating the practices of private companies in the field of cyber security and how the Bourdieusian thinking tools can offer a rich analytical ground for understanding the practices of private actors in cyber security.

The first part of the chapter situates the place of private studies in IR theory and security studies and argues that processes of broadening and deepening of security have benefited the latter field by opening up a disciplinary space for debates about private security. Then, the chapter introduces the concept of marketization of security as an alternative analytical tool to the idea of privatization, by arguing that 'marketization' not only makes it possible to better capture the object of the present research, but also provides a better understanding of the shifts in global governance highlighted by the specialized literature on private security and of their implications. Next, among these implications the work highlights how the formation of industrial complexes, which encompasses complex and often hybrid relationships between governmental agencies and private companies, is an important aspect of marketization and of the concurrent phenomenon of hybridization between the public and the private. Finally, it situates cyber security in the private security debate, underlying the relevance of the concepts employed in the work for understanding the role of private companies in this specific arena.

The second part of the chapter explores Bourdieusian sociology, its contributions to thinking about 'practices' and analyzes two thinking tools the thesis will primarily work with: *champ*[5] and capital. In what concerns private security studies, authors like Leander (2014) and Bigo (2011a) have employed Boutrdieu's

[5]Bourdieu's notion of field (*champ*, in French) does not always coincide with the most common use of the word "field" to refer to a certain area of the human activity. It is possible for one to speak of "the field of IR" and refer to either the set of works that make the discipline or, distinctly, to the field of IR, in a Bourdieusian sense, to make sense about the social dynamics and struggles for a specific stake within IR. To avoid further confusion, the word "field" in this work refers to the area of human activity, whilst the word *champ* is used to the Bourdieusian notion of field.

rationale and concepts to question the public/private dichotomy that marks studies concerning the practices of private security/military companies and state bureaucracies alike and to take current security governance as a complex enmeshment between the public and the private. Reading the practices of private actors in terms of *champ* and capital allows thinking outside the 'black box' of the nation state and picturing a distinct (transnational) dynamic of security in which hybridization is a ubiquitous trend (BIGO, 2011b).

It is argued that looking at cyber security as a *champ* makes possible capturing the attempts of private companises to gain influence through their services, advertisement and risk-oriented practices and discourses. Bourdieusian thinking tools give a different reading of the involvement of private and state actors in cyber security. This is a complex involvement marked by patterns of competition and cooperation not only between private actors themselves, but also between private actors and state bureaucracies. At stake is the definition or delimitation of what constitutes a 'risk' to cyber security. This 'act of naming' (BERLING, 2012; BOURDIEU, 1990) is important because, for private companies, it grants access to the cyber security market. Moreover, precisely because of this definitional power, cyber security also works as a regime of justification (BOURDIEU, 1998; 2004) for distinct market practices aiming at 'strengthening' the security of software, data and critical infrastructure.

2.1. IR theory and Private Security Studies

Private security initially had little space in IR debut as a disciplinary field. The imaginary of the discipline has been strongly tied to the notion of the nation state, as have been the concepts of anarchy and sovereignty (WALKER, 2006). Realist theory takes this political entity as its primary object and its worldview is based on a distinction between internal and international politics (MORGENTHAU, 2002; GUZZINI, 1998; WALTZ, 1979). This distinction has contributed to foster a very specific political imaginary associated with the most fundamental set of Realist assumptions, composed by an anarchical international system in which states, portrayed as rational actors, seek to maximize their security and situate themselves in a never-ending competition with other states. Most of these conditions were taken as objective sources of autonomy in the field. As

Guzzini (1998) notes, the confusion between the discipline of IR and Realism was only possible because the latter was understood as a theory that contributed to distinguish IR from other social sciences.

The fundamental set of Realist assumptions was questioned by scholars in IR because of their analytical insufficiency for capturing a set of other relevant phenomena for international politics and the political life, as well as the limitations it imposed to the political imagination (ASHLEY, 1988; WALKER, 2006). These assumptions were epistemologically anchored in the common sense that IR should be studied considering the existence of objective facts; the rejection of theories if new observations were inconsistent with the expectations created by them, and that, for any problem-domain, there would always be an adequate theory (CHERNOFF, 2007). This 'scientific' vision of IR, as vindicated by Realism, served in turn as a blind spot for the role of realist theorizing in shaping and being shaped by US international policy concerns and scholarly criteria of social science (GUZZINI, 1998).

State-centrism in Realist theory was initially questioned by liberal pluralists in the 1970s, in what Hobson (2003) terms the 'first state debate.' The neo-realist assumption of the state as a rational, coherent and autonomous actor with a focus on the high politics of 'security' was questioned in face of a perception of a higher focus on the 'low politics' of economics, distribution and welfare over military security. For liberal pluralists, international interdependence led to a fragmentation (and sometimes weakening) of the state in relation to non-state actors (especially multinational corporations) (see also KEOHANE e NYE, 1987; 1998).

'Reflectivist' approaches[6] to IR, in turn, offered a critical view of the role of the state and anarchy as objective conditions in the international system, providing distinct angles for understanding this controversial but long established political entity. These approaches laid the groundwork for questioning the very prominence of the State in the field and are constitutive of what Hobson terms the 'second state

[6]Those approaches which fall into the 'reflectivist' category tend to challenge the dominant, scientific view of how IR should be best studied and to rule out the possibility of objective knowledge in the field. Also termed 'Critical', they are usually not oriented to problem solving and most of them avoid 'prediction' on the basis that social facts are distinguishable from natural facts. Reflexivity works as a double process of self-consciousness of one's own historical time and place and how both determine the questions at stake and as an effort to understand the historical dynamics of the conditions in which these questions came into being. For more discussions on critical theory in IR and the opposition between scientific and reflectivist approaches, see Devetak (2005) and Chernoff (2007).

debate' (HOBSON, 2003). The author contends that the first debate provides an inadequate framework for understanding IR theory and its various approaches to the state, once it reifies international structure over the 'state-as-agent' theorization (HOBSON, 2003:217). The second debate, on the other hand, would be interesting insofar it locates IR theory within the agent-structure problematic.

These state debates in IR were strongly influenced by other social sciences. As Hobson (2003) observed, there has been a parallel between emerging debates in the disciplines of Sociology, Comparative Political Economy and IR. This parallel is also observed in the 'shift' to the 'second state debate' away from a state-centric *versus* society centric perspective. Attention to how state power derives from their embeddedness in society and to the co-constitution between state and society became central.

The challenge to the 'scientific' view of IR and its fundamental assumptions had implications for the concept of security, which provision is a function that has been traditionally associated with the state (FOUCAULT, 2007; ELIAS, 2000). They indicate that theory has struggled to expand its comprehension of the complexity of real world instead of sustaining political and social reifications of either 'structures' or 'agents.' The objective image of the state as a unit in an anarchical international system came under scrutiny, as well as the premises that underpinned this worldview. Additionally, critical accounts of the role of theory in shaping social reality opened the way for theoretical considerations of topics beyond the state-as-structure and military power, and also they helped in building a bridge for IR to have a better dialogue with other social science disciplines.

Security studies, in particular, have benefited from this environment of contestation of the 'bases' of IR theory and from theoretical efforts to expand the discipline's understanding of social reality. Inspired by the methodological challenges posed by, broadly speaking, constructivist and post-modern approaches, critical approaches to security have contested the categories over which the subfield relied on, in particular the focus on the nation state as a reified entity, on the predominance of military power over other categories of power, and on the idea of security as an objective situation necessarily derived from the anarchical condition

of the international system. These contestations led to a substantial broadening[7] and deepening of the main object of security to encompass more than just State-related and military security issues (ULLMAN, 1983; KRAUSE; WILLIAMS, 1997; KRAUSE, 1998; BOOTH, 2007; BUZAN e HANSEN, 2009). Mainstream, realist-inspired assumptions were criticized by what Krause and Williams (1997) term critical security studies[8] – a broad field that accounts for distinct approaches to security, threat construction and production and their shifts over time and space.

Nye's (2004) account of the concept of US national security is representative of the nature of some of the main contestations that 'security' has faced since early attempts to contest the prominence of military threats in security politics:

> National security – the absence of threat to a country's major values – is changing. Damage done by climate change or imported viruses can be larger in terms of money or lives lost than the effects of some wars. Even if one frames the definition of national security more narrowly, the nature of military security is changing. As the US Commission on National Security in the Twenty-first Century pointed out, the country has not been invaded by foreign armies since 1814, and the military is designed to project force and fight wars far from our shores. But the military is not well equipped to protect us against an attack on our homeland by terrorists wielding weapons of mass destruction or mass disruption or even hijacked civil aircraft. Thus in July 2001, the secretary of defense, Donald Rumsfeld, dropped from the Pentagon's planning priorities the ability to fight two major regional conflicts and elevated homeland defense to a higher priority. As the US discovered only a few months later, however, military measures are not a sufficient solution to its vulnerabilities (NYE, 2004:85).

Private security was introduced into the discipline favored by the theoretical and meta-theoretical debates that took place in IR theory since the mid-1980s and that questioned the position assigned to the state and how it was approached by theory. The field's initial concern was with attempts of understanding how privatization transformed the state, particularly through perceived shifts in the monopoly of the use of force and its consequences for security (LEANDER, 2010; see SINGER, 2002; AVANT, 2005). This involved dealing with more complex

[7] The idea of broadening has generally been employed to refer to the inclusion of non-military security issues in the security agenda (see ULLMAN, 1983; KRAUSE; WILLIAMS, 1997; BUZAN; HANSEN, 2009). Booth (2007), however, suggests that this is a recurrent misconception that places the idea of broadening in a level-of-analysis move. According to the author, broadening suggests a critical move instead of a technical and strategic one: the critical turn happening through deepening is concerned not with turning all politics into practices of security, but with interpreting security issues as questions of political theory. For a more detailed discussion on this specific conceptualization of broadening, see Booth (2007).

[8] According to Krause (1998) and Krause and Williams (1997), the term encompasses several critical and reflexive approach to security, from Feminist studies to the varied strands of Post-modernism and Constructivism.

dynamics of security and distinct actors by inquiring which socio-political, cultural and economic dynamics have stimulated the expansion of private security, as well as considering the growing role of non-state actors, in particular private companies, in the governance of security and recognizing their influence on the overall threat formation and perception.[9]

Initial studies appeared still in the mid-1990s, but it was from the early 2000s on that private security studies gained considerable projection in IR (ABRAHANSEN; LEANDER, 2016). Several works have strived to discuss distinct, although interrelated phenomena such as the tendency of "privatization" of the use of force (SINGER, 2002; AVANT, 2005; LEANDER 2008), of security, in general (ABRAHANSEM; WILLIAMS, 2009; LEANDER, 2009a), the role of private military/security companies in creating (in)security (SINGER, 2002; AVANT, 2005; LEANDER, 2005; LEANDER; VAN MUNSTER, 2007; ABRAHANSEM; WILLIAMS, 2009), as well as contestations over the public/private divide as a point of departure (BERNDTSSON; STERN, 2011; BIGO, 2013; 2015). Further, broadening the notion of privatization, authors like Petersen and Tjalve (2013) study how security tasks are transferred not only to private actors *strictu sensu*, but also to all the range of actors that do not fit the category of 'private companies.'

2.2. Introducing the idea of "marketization of security" and its implications

The idea of a 'privatization' of security, which commonly underlies the body of studies on private security, suggests a shifting away of security governance from government to market actors[10] (LEANDER, 2010; DUNN CAVELTY, 2016). Contemporarily, this changing mode of governance finds its roots in the

[9] Discussions on threat formation/construction became recurrent in IR influenced by the securitization approach in the mid-1990s. The constructivist bias of the securitization school suggests a focus on the social construction of threats. The main argument is that an issue does not become a security issue because of its objective reality in relation to the referent object, but because an actor has defined it as a threat to some object's survival. See Buzan et al. (1998); Balzacq (2011) and Huysmans (1998).

[10] In a first moment, to conceive privatization as a transfer of powers to private actors may suggest that power was never in these actors' hands. This is nothing but misleading. As Avant (2005) notes, the private sector has been playing a role in providing security for some time. What deserves attention is how the last two decades faced a growth and enlargement of such a role.

'deepening' of the 1970s neoliberal policies, which lead to intense deregulation and outsourcing[11] of central government functions to the private sector (ABRAHANSEM; WILLIAMS, 2009).

Despite having introduced the topic with the term 'privatization,' for semantical reasons, this work will employ the term 'marketization' of security to refer to the expanding projection of market actors in the field of security. The phenomenon of marketization is part of a 'new public management' and refers to the integration of competition and price mechanisms into public services in order to improve states' efficiency. Although privatization is the most common form of marketization, the latter is not limited to the former. Outsourcing, management contracts and market testing are also forms of marketization (BEVIR, 2009). This movement is justified by an attempt to better capture the main object of the thesis – private actors and the cyber security market – and by the most common implications of using the term 'privatization' to refer to a broader attention to the 'private' sphere of the market.

The option for the term marketization is a political choice that involves refusing the oversimplification implied by talks about the 'privatization' of an issue and the overall idea that markets are dominating what used to be public spaces and activities; it is also an attempt to understand the cyber security market as marked by distinct practices emanated from public and private actors. This has important consequences regarding how one should conceive the state and its practices and allows questioning the state/market separation that is pervasive in neoliberal theory.

The cyber security market is dynamical but it is hardly restricted to the activities of the private sector. Apprehending the role of private companies in cyber security through the phenomenon of marketization implies recognizing the role of state actors in authorizing market practices in a given field, by contracting out a wide range of services with market actors or sharing the 'management' of an issue, without necessarily having to abdicate of its own participation in certain aspects of it. The security of military and civilian computer systems or the development of new cyber security solutions for governmental spheres tend to involve services

[11] In a 2008 report of the U.S. Congressional Research Service (CRS) definition, "'outsourcing'– which is also termed 'contracting out' by some authors – refers to an agency engaging a private firm to perform an agency function or provide a service (…)" (CRS report *apud* BRUNEAU, 2015:236).

delegated to (and sometimes shared with) private companies, a fact that is often associated with the strong private bias of the cyber security *champ* (DUNN CAVELTY, 2016).

This work takes the development of cyber security as a hybrid process triggered by both market practices and distinct discourses and practices emanated from states, think tanks, hackers and hacker communities, security experts and private companies. Despite the common understanding that cyber security has been developed primarily in the private sector (CSIS, 2008; DUNN CAVELTY, 2016), focusing on this process without considering how it is part of a broader movement where actors compete to make sense of "security" may implicate in overlooking the extent to which perceptions and practices related to the concept arose as objects of struggles among the aforementioned constellation of actors. The 'struggle over the cyber security market' dynamics will be discussed in chapter 3. In the moment, it is important to note that the very idea of marketization of (cyber) security suggests a deepening of neoliberal policies in which decentralization leads states to rely on firms as partners in government (LEANDER, 2010).

Furthermore, the adoption of the term 'privatization' risks reducing the scope of the public-private entanglement that has been formed in some of the most influential liberal states nowadays. The term marketization suggests an analytical tool most suitable for understanding the meanings of security, delimitations of security spaces and of the practices of security emanated from public and private institutions, once it takes the role of both kinds of actors in shaping these practices, for example, through advertising, regulations, authorizations, contracts, technical studies and so on. Thus, instead of focusing *specifically* in the shifts from the 'public' to the 'private' – as does the idea of privatization – the idea of marketization comprises meaningful shifts in the politics underlying the public *and* the private[12] (LEANDER, 2010).

The concept of marketization is useful for understanding the way in which states have tried to govern security through markets from the end of the Cold War to the present (LEANDER, 2008). If the current working of Private Security Companies (PSCs), Private Military Companies (PMCs) and other security-related companies tells us something about current trends in global governance, it is that it

[12] Leander (2009b) employs the term 'commodification' to refer to similar dynamics.

was never a static process where power is transferred from the 'higher' authority, or the state, to the 'lower' authority, the market. Whilst concerns with privatization, the most extreme form of marketization, are important, they alone are unhelpful in making sense of the broader patterns of relations between private actors and states. Thus, it is important to pay attention to the logic and politics of security production in light of the functioning of neoliberal and sovereign forms of governance in the field of security (LEANDER 2008; BERNDTSSON; STERN, 2011).

It is important to note that a common concern underpinning most studies about private security is related to the significant transformations in the governance of security, which has been shifting together with broader changes in global governance (ABRAHANSEM; WILLIAMS, 2009). Whilst the literature on private security initially focused on issues involving PMCs and the use of force by private market actors (SINGER, 2002; AVANT, 2005; LEANDER, 2005; LEANDER; VAN MUNSTER, 2007), these changes go beyond the scope of 'traditional' security activities, most of which are also related to national defense.

Private companies in the field of security do not operate exclusively in the context of armed conflicts, nor are they exclusively related to military functions. Instead, for a long time, they have been part of everyday security in 'consolidated liberal democracies' (BERNDTSSON; STERN, 2011) and their competences for a wide range of security functions keep expanding. The U.S. is by far the country that most encourages contracting out with private companies, for a diverse range of services (BRUNEAU, 2015). As Berndtsson and Stern (2011) contend, despite the dilemmas posed by PSCs in conflict zones and the attention they attract, a distinct, less violent, dynamic of security practices occurs globally. Thus, "in many societies globally, commercial forms of security are increasingly being used to provide security and maintain public order in public and semi-public places" (BERNDTSSON; STERN, 2011:411).

According to Abrahansem and Leander (2016), in IR, a considerable number of accounts take private security as an implication of the changing geopolitics of the post-Cold War, which includes but is not restricted to military downsizing and the end of superpower rivalries. The authors, however, suggest that this way of approaching the matter hinders a series of other factors that have encouraged the expansion of private market in security, as is the case of the reorganization of the

economy and production in the 1970s and the integration of ITs to the defense sector, in what has become known as Revolution in Military Affairs (RMA).

The phenomenal expansion of commercial security activities varies from guarding functions to risk analysis and surveillance (ABRAHANSEM; WILLIAMS, 2009). Examples of the current range of private security studies and the ubiquity of the activities of private companies are their activities in airports (BERNDTSSON; STERN, 2011), issues of gender (EICHLER, 2016); activities of intelligence and surveillance (BALL et al., 2012); cyber security (DUNN CAVELTY, 2016) and so on. Governments' attempts to streamline bureaucracies and tighten welfare budgets, by normalizing privatizations, outsourcing and public-private partnerships, mark the state participation in its own 'disassembly'. In this sense, the 'marketization of security' is part of a broader restructuring of the 'public-private', which started in the last decades of the 20th century under the label of neoliberalism. The fact that the development of cyber security practices occurred mostly at the heart of the private sector appears to be directly related to this broader tendency in global governance (DUNN CAVELTY, 2016).

In classical liberal theory, markets and states are exhaustively distinguished one from another, a distinction based on a view of the state as the *locus* of a political, power seeking behavior and of the market as the *locus* of an economic, wealth-seeking behavior. Liberalism's 'renewed' version, neo-liberalism, has fostered an opposite trend. The history goes as follows: the relationship between markets and states has been one of constant 'struggles' between opposing groups, which initially opposed the aristocracy and the bourgeoisie, and later capitalism and socialism. But the last decades of the 20th century saw social and economic shifts, among inflationary shocks, state attempts to stabilize markets and the growing importance of financial capital, which would back neoliberal claims that economic theory was able to provide a better analysis of public policy than political science (CROUCH, 2004).

Neoliberalism starts from the classical liberal state/market separation assumption, but takes a practical detour. Crouch (2004) shows that political and economic systems are vulnerable to particular forms of state-market entanglement, as is the case of the relationship between state officials and private firms and *lobbying*. Neoclassical economics, which inspired neoliberalism, argues that the state, as it is not a market actor, is unable to act rationally and anticipate the

consequences of its actions. Remediating this is partly a task of leaving the state out of the market and partly improving its capacity to become like a firm. Thus, in this sense,

> the neoliberal state defers to business interests; it believes that its own internal processes have been discredited by the years of social democratic compromise, and wishes to clean itself out by borrowing as many practices and procedures as possible from private firms" (CROUCH, 2004:247).

The many policies adopted to fulfill such a goal, from privatization and outsourcing to sharing regulation with firms, point to an 'erosion' of the perceived boundaries between the state and the market.

The aforementioned discussed shifts in governance that mark what is understood as marketization of security matter when making sense of 'security'. Leander (2009b) discusses the phenomenon of 'commodification' of security as an implication of the expansion of private security and the aforementioned shifts in governance that have made the marketization of security a widespread tendency. She argues that security is a 'contested commodity' in the sense that there remains a fundamental disagreement or "an ongoing and unsettled symbolic struggle" (LEANDER, 2009b:2) over whether it is a commodity in the first place. The consequence of these struggles over 'security as commodity' is that they influence the organization of markets' practices. And,

> because the legitimacy of the market as such is questioned and under threat, market practices are bound to be organized in ways which diminish the significance of this threat and makes the market appear as 'normal' and uncontested as possible. (LEANDER, 2009b:4-5).

Extremely relevant for understanding the critique that will be advanced further in this work, the idea of a spiraling insecurity is one articulated form of contestation of the commodification of security and, in some aspects, it is similar to Booth and Wheeler's understanding of a possible outcome of IR's classical security dilemma[13], or a *security paradox,* in which attempts to increase security

[13] Herz (1950), who coined the term security dilemma, considers that it results of the anarchical condition of the international system. His description of the phenomenon follows the logic that groups and individuals living in a constellation where anarchy reigns have high concerns over their own security against attacks and domination by other groups/individuals. Striving to attain more security, there is a tendency for these actors to acquire more power. "This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on." (HERZ, 1950:157). According to the author, this dynamic is beyond the discussions over the 'nature' of the human being. The notion of security dilemma is at the core of Kenneth Waltz's (1979) defensive realism.

actually can lead to increasing insecurity[14] (BOOTH; WHEELER, 2008). In the case of market actors, the main concern is that "those selling protection are in reality selling protection against threats that are more or less a direct consequence of their own activities and that these sales (…) increase (…) the prevailing insecurity" (LEANDER, 2009b:13). The securitization strand of the same argument emphasizes the role of companies in advertising and lobbying for understanding specific issues as threats, which induces the same kind of spiral of insecurity (LEANDER, 2009b). Market reactions to this specific critique consist in arguing that market practices are a response to a demand, in the sense that "it is the security needs (of states, organizations, private businesses and individuals) pre-existing and independent of the company they respond to" (LEANDER, 2009b:14).

2.3. "Hybrid" security and industrial complexes

An important implication of the marketization of security is related to the growing enmeshment between the practices of public and private actors. In this sense, a recent trend in the literature concerning private security, drawn from the contestation over the public/private distinction, has been to focus on a process of hybridization of security governance instead of focusing on the transfer away of security functions to market (LEANDER, 2009c; BIGO, 2013; 2015). This process of hybridization is sometimes addressed in terms of a security assemblage (BERNDTSSON; STERN, 2011) or a 'chimera' (LEANDER, 2009c; 2014), and it refers to the difficulty in understanding the enmeshment between public and private actors from the point of either 'the public' or 'the private'. The idea has been fruitful for understanding the dynamics of the intelligence sector in the U.S. (LEANDER, 2014), of practices of surveillance (BALZACQ, *et al.*, 2010; BIGO, 2011a; 2013; BAUMAN, *et al.*, 2014) and of the functioning of airport security administration (BERNDTSSON; STERN, 2011), for example.

[14] Booth and Wheeler (2008) definition of the security dilemma takes it as a two-level strategic predicament, where the first level corresponds to a dilemma of interpretation, in which actors shall decide over whether the perceived military developments are of offensive or defensive nature; and the second level corresponds to a dilemma of response, in which actors need to determine how to react. The notion of a *security paradox* arises from the latter, in a context where "leaders resolve the dilemma of response in a manner that creates a spiral of mutual insecurity" (BOOTH; WHEELER, 2008).

A representative trend of this hybrid approach to security governance dates back to the Cold War and the buildup of U.S military-industrial power. The enmeshment between practices emanated from the government, on one side, and defense contractors, on the other, has been addressed in previous studies (ADAMS, 1968; LEANDER, 2009c; 2014), but very few gave attention to the literature on 'industrial complexes', despite addressing its dynamics in more indirect ways.

The notion of a military-industrial complex gained attention in former U.S president Dwight D. Eisenhower's farewell address, in 1961. On the occasion, Eisenhower warned against an 'unwarranted influence' of the conjunction between U.S military establishment and arms industry (EISENHOWER, 1961). Since then, a robust body of literature has been created to discuss the phenomenon of "industrial complexes", be they military (EISENHOWER, 1961; ADAMS, 1968; DUNNE; SKÖNS, 2011; HARTUNG, 2011), or of other diverse nature (DEIBERT, 2011; 2013; BALL; SNIDER, 2013; HARRIS, 2014; see also HARTUNG, 2011).

Dunne and Sköns (2011) argue that the concept lacks analytical strength, but is quite valuable as a descriptive tool that refers to

> coalitions of vested interests within the state and industry, which could lead to decisions being made which were in the interest of the coalition members and not necessarily in the interests of national security (DUNNE; SKÖNS, 2011).

The military-industrial complex is perhaps the classical example of this kind of political arrangement between state and industries. The marketization of security functions has led to an expansion of the military services industry that does not necessarily imply a dominance of the public by the private. Governmental action is at the heart of Adams' (1968) account of industrial concentration in the late 1960s. Accordingly, the formation of military-industrial complexes illustrates some of the power issues constitutive of the "new industrial state", in which specific institutional arrangements – anchored in defense contracts, support to research and development in the private sector, patent policy, tax privileges, subsides, etc. – are encouraged by government actors seeking to establish alliances with the private enterprise. Military-industrial complexes are an evident aspect of how the

> government not only permits and facilitates the entrenchment of private power but serves as its fountain-head. It creates and institutionalizes power concentrations which tend to breed on themselves and to defy public control. (ADAMS, 1968:653).

Adams did not view the complex as a conspiracy between "merchants of death and a band of lusty generals", to quote the author's own terms, but as a natural coalition of interest groups with stakes in the defense sector that included distinct

governmental spheres, the industry, labor unions, lobbyists and legislators alike (ADAMS, 1968:655).

The post-Cold War momentum brought relevant changes for this political arrangement between the market and the state. This includes a geographical dispersion of the US/European supply chains; the restructuring of traditional arms producers – many of which have oriented themselves to the cyber security and surveillance markets; – the emergence of new companies and new security areas; and the inversion of the dual use logic for technology from military-to-civilian use to civilian-to-military use (DUNNE; SKÖNS, 2011). But whilst this may have altered important components in this political arrangement, the dynamics and impact of the vested interests seem to have endured (DUNNE; SKÖNS, 2011).

Chomsky (2004) argues that these complexes are, in fact, the core of modern economy: they are not necessarily military nor representative of a free-enterprise economy. The development of new technologies for the use of the public sector, as it was the case of the Internet or of the computer, took a while to span to the civilian market. He gives the example of IBM and how, through public funds, it was able to develop and produce advanced computers for the NSA and government agencies, still on the 1960s – curiously, almost paralleling with the ending of Eisenhower's term.

A meaningful shift has happened in this industry with the introduction of new security issues to the political agenda. In particular, there is a new orientation of traditional and new private companies that both directly contract out with governments or that are located in a broader supply chain towards the cyber security and surveillance industries (HARTUNG, 2011; DEIBERT, 2011; 2013; BALL; SNIDER, 2013; HARRIS, 2014). This was partially stimulated by the advancement of civilian technologies – with an emphasis on electronics – in relation to military ones. As a consequence, a distinct dynamic took place in what concerns ICTs:

> companies in the electronics and IT sectors, that in the past had little involvement with arms production are finding themselves part of the defence industrial base and sometimes the target of diversification efforts by the major arms producers. (DUNNE; SKÖNS, 2011:4).

2.4. Cyber security and private security

The discussion on the hybridization of the public/private is very relevant for thinking the role of the private sector in the *champ* of cyber security. As Dunn

Cavelty and others have noted, the operation of both cyberspace and critical infra-structures is distributed among private sector's actors (DUNN CAVELTY, 2007; DEIBERT; ROHOZINSKI, 2010), as a direct result of the 1970s privatizations. Extensive and penetrating surveillance systems are legitimized by a legislation and counter terrorist policies that remove existing operational constraints and are increasingly operated and controlled by private actors instead of the State. The same can be said about telecommunications and the role of cyberspace as a communication environment, both of which are usually hosted, operated and controlled by a distinct mix of private companies and public institutions. As Deibert and Rohozinski (2010) argue, the locus of authority in cyberspace has been shared between public and private spheres and people's lives are not only mediated through the state, but also dispersed through ICTs owned, operated and exploited by private companies.

The operation of these actors in and through cyberspace varies. Companies specialized in commercializing offensive 'cyber warfare' and surveillance technologies, or what Deibert (2013) calls "shadowy security services", are amongst the variety of private companies that operate in and through cyberspace. This particular burgeoning group includes some of the biggest defense companies in the United States (U.S), most of which in recent years have oriented themselves to the lucrative cyber security market.

The perception that distinct, complex threats arise from cyberspace and inside it, and the concurrent attempts to militarize it (DUNN CAVELTY, 2012; 2013; DEIBERT, 2011) fuel a multibillionaire market with an estimated value of US$150 billion annually (DEIBERT, 2013), that includes companies advertising cyber security solutions that go far beyond conventional antivirus protection. In a trend that seems to emulate the involvement of private companies in military/security issues, new companies and big, traditional defense contractors orient themselves towards serving the growing pressure to secure cyberspace. As the literature on the military-industrial complex made clear, this cyber security or internet military-industrial complex, as Deibert (2011; 2013) and Harris (2014) term it, is in direct connection with governmental instances in the U.S., to the point that it becomes difficult to dissociate the public and the private in the ocean of public-private partnerships that are invoked as a solution to the pernicious insecurity of cyberspace.

The link between private security studies and the role of private actors in cyber security is not always easily established in IR works. Both traditional and critical security studies in IR have failed to adequately assess the central role of private companies in cyber security. As Dunn Cavelty notes, "while private security actors play an important role in all forms of cyber-aggression and countermeasures, this topic is a non-issue in the emerging literature." (DUNN CAVELTY, 2016:93). Research in economics of information security, on the other hand, has dealt with this object in a more satisfactory fashion (see DUNN CAVELTY, 2016; ANDERSON, 2001).

The literature on Public-Private Partnerships (PPPs) gives a good account of the dynamics of the public and the private in what concerns cyber security. Seen as a panacea for the issue of cyber security, PPPs still find obstacles that range from the difficulty of governments sharing sensitive information to the concern of companies with their reputation if they share information about their own vulnerabilities (DUNN CAVELTY, 2016). But most importantly, it should be noted that PPPs seem to be but one kind of answer to a perceived difficulty in providing security from one standpoint only, be it 'the public' or 'the private'.

As a matter of conclusion, it is important to observe that what most of the distinct ideas underlying the critique to the public/private divide as a starting point have in common is a theoretical background inspired by Bourdieusian sociology (LEANDER 2009c; 2014; BIGO, 2013; 2015) – with a notable exception of those who employ the Deleuzian notion of assemblage (ABRAHANSEN; WILLIAMS, 2009; BERNDTSSON; STERN, 2011). By employing distinct conceptual tools, these studies have approached issues of international security and private security in a distinct and original fashion, and posed important questions regarding the practices that together constitute security governance

From this moment on, the chapter will address the contributions of the Bourdieusian theory for the theorization of "practices" in the social world. The next section will briefly present the so-called 'practice turn' in IR and discuss the implications of thinking in terms of practices. Then, the following section will analyze the thinking tools developed by Pierre Bourdieu, with a special attention to the ideas of *champ* and *capital*. In the course of the section, a dialogue between Bourdieu's concepts and their application to cyber security will be established. Thinking the practices of private actors in terms of *champ* and capital allows a

visualization of the complex dynamics and practices of security in consonance to the concept of marketization here employed. These understandings further fundament the way our conceptualization the *champ* of cyber security and of the strategies of private sector in it.

2.5. Practice theory and the practice turn in IR

This section will briefly address the theoretical and methodological path the work has undergone by focusing on the practices of private actors and discussing its implications. Up to now, the word 'practice' has been unduly employed without any further consideration of what does exactly mean to speak of it and what are the implications of paying attention to 'practices'.

According to Reckwitz (2002), practice theory is a unifying label to a group of approaches interested in how social beings make and transform the social world. It focuses on the routine and performativity of social action, as well as on its dependence on tacit knowledge and implicit understanding. The author argues that exponents of contemporary practice theory share a common viewpoint indebted to cultural theory, as they recognize the blind spot shared by theories grounded on the classical figures of the *homo economicus* and the *homos sociologicus* in the sense of "they both dismiss the implicit, tacit or unconscious layer of knowledge which enables a symbolic organization of reality" (RECKWITZ, 2002:246).

Practices can be collective, in the sense of being "both structured and acted out by communities of practice, and by the diffusion of background knowledge across agents in these communities, which similarly disposes them to act in coordination" (ADLER; POULIOT, 2011:8). Adler and Pouliot (2011) call these collective practices 'corporate practices.' The notion of corporate practices can be well-adjusted in order to understand the practices of state bureaucracies and private companies, for example. In most cyber security companies, CEOs and engineers shared a common background knowledge of code and computing that informs partially or totally the policies, product development and other practices of the company.

In IR, the practice 'turn' is based on the idea that it is necessary to pay attention to the everyday life's practices in order to understand dynamics of order and change (BUEGER; GARDINGR, 2015). Initially influenced by the

poststructuralist critique, works focusing on the importance of practices to understand world politics gained strength among IR scholars (see NEUMANN, 2002; JACKSON, 2008; POULIOT, 2008; ADLER; POULIOT, 2011; ADLER-NISSEN, 2013), with some theoretical disagreements among them about what constitutes practice theory. For example, there is a strong influence of Pierre Bourdieu's work in IR's practice turn (JACKSON, 2008; POULIOT, 2008; POULIOT; MÉRAND, 2013; BIGO, 2013; BERLING, 2013; ADLER-NISSEN, 2013;), as well as critique against equating practice theory to Bourdieu's work (BUEGER; GARDINGR, 2015; for non-Bourdieusian approaches to practice theory see also: SCHATZKI; KNORR-CETINA; SAVIGNY, 2001).

As Bueger and Gradingr (2015) themselves note, there has been a degree of compatibility between Bourdieu's concern about domination and IR's historical concern about power relations, conflicts and hierarchical structures, and a correspondence between some categories dear to the discipline and Bourdieu's thinking tools (ADLER-NISSEN, 2013; BUEGER; GRADINGR, 2015). Although it is wise to avoid equating the whole of practice theory with Bourdieu's theorization, it is argued that, in the case of the present work, the thinking tools made available by his approach to practice may help in situating the social struggles in the social universe around 'cyber security'.

Bourdieu's practical reason is a product of his theoretical puzzle of concepts. It rests on the notion that the logic of practicality is not that of the 'logical' logic nor that of rational calculation (BOURDIEU, 1998, POULIOT, 2008). In this sense, "agents may engage in reasonable forms of behavior without being rational; they may engage in behaviors one can explain, as the classical philosophers would say, with the hypothesis of rationality, without their behavior having reason as its principle" (BOURDIEU, 1998:75). Practices are, in this sense, "self-organizing and propagating manifolds of activity" (RECKWITZ, 2002).

This approach distances itself from textual analysis in that practical theorists see little value in analyzing political discourses and text internally, without further considerations of the wider social frame within which they find themselves. Further, the poststructuralist analysis of "discourses as practices that constitutes the objects of which they speak" (ADLER-NISSEN, 2013:6) contrasts with Bourdieu's view of language as embedded in social hierarchies and bodies, manifesting the agent's position in the social world. This critique to pure textual analysis is enacted by

Pouliot (2008), when he points that some postmodernists distort the practical logic of discourses.

Practice theory is believed to contribute to explaining and understanding the actual working of world politics. Reading social action according to socially meaningful patterns of action, performed more or less competently and simultaneously embodying, acting out and even reifying background knowledge and discourse in and on the material world, instantiates an engagement with the relationship between agency and the social milieu (ADLER; POULIOT, 2011).

In this work, discourse and practices are both important components of the analysis on how private companies act in the social world. As theory shows, in some cases, practices are embodied in discourses (NEUMANN, 2002; ADLER; POULIOT, 2011), whilst in other cases, practices are legitimated or, conversely, obfuscated by enacted words. Companies act primarily according to an economic logic, but other factors may as well instantiate the set of policies and dispositions they hold publicly, in their relations with other companies and with the government, and internally. Having considering this, in the work, practices and the discourses they instantiate have been interchangeably investigated: marketing strategies and products have been interrelated with press releases and with the broader businesses in which the companies are involved, some of them quite secretive. With this, the aim is to show how, by offering and arguing for the advantage and utility of a given security solution – for example, "active defense" – instead of another – for example, "passive defense" – and by a series of other strategies that go from expanding its market shares by acquiring specialized start-ups and contracting out with the government, cyber security companies contribute to shaping understandings of security in cyberspace.

2.6. The sociology of Pierre Bourdieu and the importance of the 'thinking tools'.

In the introduction of *Réponses*, Loïc Wacquant (BOURDIEU; WACQUANT, 1992) argues that for Pierre Bourdieu the task of sociology is to bring into light the 'deep structures' buried in the social worlds that constitute the social universe, which is structured according to a first order objectivity and a second order subjectivity. First order subjectivity refers to the distribution of material resources and to the means of appropriation of capital. Second order

objectivity is composed by the mental and embodied schemes working as the symbolic matrix of practical activities and perceptions, sentiments and judgements of social agents. Bourdieu (1990) himself points that the social world is composed by both symbolic systems, language, myth, structures of perception and subjective elements of all kinds, on the one hand, and objective structures "independent of the consciousness and desires of agents and (…) capable of guiding or constraining their practices or their representations" (BOURDIEU, 1990:123), on the other hand.

Bourdieu's sociology is one of the symbolic power. This notion entails a perception of domination carried out by symbolic manipulation, which has become predominant in Western societies, instead of forms of overt coercion and the threat of physical violence. Symbolic systems, such as culture, science, religion or language, are seen as instruments of domination (BOURDIEU; WACQUANT, 1992; SWARTZ, 1997). The belief in the naturalness of the affairs in a social *champ* is stimulated by the involvement of the agent in it (and by his/her belief in the legitimacy of it) and includes both the dominant and the dominated. As Berling (2012) notes, the *champ* exerts symbolic power on agents in subordinated positions, once they misrecognize their own positions and reproduce the hierarchies of social distinctions of the *champ* (see also SWARTZ, 1997). The right to monopolize the symbolic violence, or the power to define, is a stake in any *champ*.

Social reality is both composed of objective structures and a product of representation (BOURDIEU, 1990; 2004; BOURDIEU; WACQUANT, 1992). This work is Bourdieu-inspired in that it proposes using Bourdieu's thinking tools to make sense of the practices of private companies in the *champ* of cyber security. It does not intend to fully capture the theoretical complexity of his sociological approach nor to exhaust the concepts through which the author chose to make sense of the social world. The aim of this section is, otherwise, to show that thinking in terms of *champ*s and capitals is fruitful for understanding two phenomena, the first of them corresponding to the dynamics of 'marketization' of security presented in the previous section. The use of Bourdieusian concepts is aimed at reinforcing the relevance of this particular term for apprehending the enmeshment between public and private actors (following the line adopted by LEANDER, 2014; BIGO, 2011b; 2013; 2015). By focusing on the concepts *champ* and capital, however, the work does not dismiss the relevance of the habitus, which will be less directly addressed along the section.

The second phenomenon that Bourdieusian concepts make 'readable' is the existence of struggles over 'cyber security.' This chapter will present the theoretical support and introduction for the empirical reading of the *champ* of cyber security and the practices of private companies that the work will address. The present work regards cyber security as a smaller field crosscutting with the broader *champ* of security, and due to the former's particular dynamics and stakes, being relatively autonomous from the latter. More specifically, by the end of the work, the reader should perceive how a Bourdieu-inspired reading allows taking cyber security as a *champ* in which private actors, among others, struggle for access to an expanding cyber security 'market' and strive for influence using their services, advertisements and discursive constructions based on 'risks.'

The task of showing the helpfulness of Bourdieusian sociology in thinking the entanglement of state and market actors and how it provides analytical power to make sense about distinct social *champ*s is supported by the 'thinking tools' (LEANDER, 2011:308) elaborated by the author. These thinking tools are nothing but those concepts through which one comes to make sense about both the objective and subjective dynamics of the social world. But they are, at the same time, a result of Bourdieu's concerns with practical questions that social science theory used to overlook. As the author stresses, it is necessary to overcome the opposition between objective structures and subjective representations in social science, a task that falls into his conceptual outline (BOURDIEU, 1998; see BOURDIEU; WACQUANT, 1992:71). Thus introduced, the broader aim of the sociological – albeit inspired by philosophical and anthropological accounts – approach of Pierre Bourdieu seems to aim for a science capable of building social facts which are in themselves total (BOURDIEU; WACQUANT, 1992).

Attempts to wed Bourdieu's concepts and IR are expanding (JACKSON, 2008; MÉRAND, 2010; ADLER; POULIOT, 2011; BIGO, 2011b; 2013, 2015; LEANDER, 2011; BERLING 2012; 2013; ADLER-NISSEN, 2013; POULIOT; MÉRAND, 2013) covering a wide range of issues, from studies about the *champ* of European security and its policies of defense (BERLING, 2012; MÉRAND, 2010), to private companies (LEANDER, 2005) and practices of border control (BIGO, 2002; 2005). It has further inspired what is called the 'practice turn' in IR (NEUMANN, 2002; ADLER; POULIOT, 2011; ADLER-NISSEN, 2013; POULIOT; MÉRAND, 2013).

This inclination for Bourdieu in IR is in part due to the fact that his theory has been seen as a source of useful tools for thinking world politics out of the 'black box' of mainstream IR theory, which includes conceptions about the domestic and the international as well as views about the state (POULIOT; MÉRAND, 2013). In his work Bourdieu is strongly critical of ascribing agency to the state. His critique goes far beyond conceiving the state as some entity that can 'act,' once his main worry is to avoid being trapped within the logic of the state – by validating its existence without even questioning it – as the state is nothing more than a well-founded illusion that is validated through a consensus (BOURDIEU, 2014).

In addition, as set forth in the beginning of the chapter, the disciplinary debates that have challenged Realist objectivism and opened up the field to the dialogue with other social sciences and the particular influence of sociology in the formulation of critique – as evidenced by the diffusion of constructivism as a method – were marked not only by challenges to the existing theorization about the state, but also by a reflexivity about the researcher's own role in producing theory – a topic that is constitutive of Bourdieu's sociology.

As Adler-Nissen (2013) pinpoints, using Bourdieusian theory in IR makes it possible to understand the constitution of lines of inclusion/exclusion and the enactment of practices of assimilation and distinction by social groups; it allows for analyzing the power mechanisms at the disposition of actors and observing the constitution, usage and change of political ideas through economic, cultural and social practices. In other words, its appeal is to open up the possibility for analyzing everyday practices, symbolic structures and arenas of conflict that brings distinct actors into perspective other than nation states (ADLER-NISSEN, 2013).

Proponents of the adoption of Bourdieusian approach in IR argue that it provides useful tools for understanding the complexities of international security as well as a distinct reading of IR and of the constellation of agents, *champ*s and capitals that inform current understandings of the international (BIGO, 2011b; LEANDER, 2011; BERLING, 2012). Nevertheless, it does not come without concerns over how the concepts and theory have been addressed by IR scholars. Berling (2012) notes, for example, that IR conceptualizations of Bourdieu's thinking tools have not taken the concept of capital systematically, as an analytical device for understanding the international. She also notes how scholars tend to favor individual concepts instead of providing a "comprehensive action framework" that

could help setting the boundaries around a *champ* (BERLING, 2012:429). This concern is also voiced by Pouliot and Mérand (2013:24). Similarly, Adler-Nissen (2013) points the lack of a "general dialogue on the advantages and disadvantages of importing Bourdieu into IR" (ADLER-NISSEN, 2013:1).

Whilst the present work does not intend to resolve these critiques, it attempts to contribute to the dialogue revolving Bourdieusian sociology in IR, and in what concerns security studies, most specifically, by employing the concepts of *champ* and capital to understand the practices of private companies concerning cyber security. In what Leander (2008) calls the "Field-*Habitus*-Practices" (FIHP) approach, there is a visible tendency to not rely on all thinking tools in the same way. This is not foreign to Berling's (2012) work, for example. This option for choosing one, two or as many concepts as it is possible to work with depends on the ambitions, context and interests of the researchers (LEANDER, 2008). Overall, the Bourdieusian approach is interesting for IR and Critical Security Studies in that it provides tools within which it is possible to visualize shadowy power dynamics that are often covered by the appearance of common sense – in Bourdieu's words, *symbolic power*.

By reading IR through Bourdieu's sociology, the most traditional object of analysis in IR mainstream and critical theories alike, the state, does not appear as the main nor the only actor in struggles over position (BIGO, 2013). In fact, the state does not figure as an actor at all, as it is taken to be a *champ* itself – a *champ* of power, more specifically (POULIOT; MÉRAND, 2013). Bourdieu criticizes the way the state is often pictured as a well-defined, delimited and unitary reality. For him, in fact, the state is an ensemble of bureaucratic and administrative *champs* in which agents struggle over the power to rule a particular sphere of practices. These agents themselves may belong to their own specific *champ*s (as is the case of the public and the private sectors). In a sense, the state works as a 'meta' *champ* which concentrates different kinds of capital. The construction of the state, thus, goes along with the construction of the *champ* of power (BOURDIEU; WACQUANT, 1992).

But what is, exactly, a *champ* and how thinking in terms of *champs* influences how one makes sense of IR and of the social world? In Bourdieu and Wacquant's (1992) terms, "*um champ peut être défini comme un réseau, ou une configuration de relations objectives entre des positions*" (BOURDIEU; WACQUANT 1992:72).

In other words, the *champ* is a network which works as a 'structured space' around which perceptions are built (BOURDIEU, 1988:784; BOURDIEU, 2004). Simultaneously, it structures the *habitus*, understood as the 'feel for the game' that represents a practical sense that structures perceptions (BOURDIEU 1988; BOURDIEU; WACQUANT 1992; JACKSON 2008; BIGO 2011b).

Functioning as a relatively autonomous social microcosmos in which positions are defined according to the distribution of capital among agents, every *champ* has its own set of inter-subjectively shared and taken for granted values, or doxa, which can be called into question in some occasions.[15]

Serving as a 'vector of power' (POULIOT; MÉRAND, 2013), the notion of *champ* does not work just as a social space of shared norms, but as something bisected by conflict between distinct actors. Generally, binary oppositions, such as the public/private one, structure the *champ*. As Bourdieu and Wacquant (1992) indicate, the boundary of a *champ* depends on where the effects of this *champ* cease. In other words, it is specific to the dynamics of each case. To apply the notion of *champ* to IR makes it possible to move beyond the level-of-analysis problem, as the level of analysis itself is always the *champ*s – whether local, international or transnational – hierarchically organized within the social space (POULIOT; MÉRAND 2013).

However, hierarchy in Bourdieusian terms does not presuppose a static social world. Instead, *champ*s are essentially dynamic. The visualization of the *champ* as a space where agents act interestedly helps to account for it as a site of power relations permeated by struggles over certain stakes. According to Bourdieu (1998; 2004), incessant struggles happen between actors within a *champ* (these actors being holders of specific types of capital) to reinforce their own position in it, and to define what functions as reality and its truths. Similarly, these struggles aim to reinforce the strength of a given *champ* vis-à-vis others, "in order to increase the value of their investment" (POULIOT; MÉRAND 2013:35).

In what concerns the limits of the *champ* there remains a vagueness – "*les limites du champ se situent au point où cessent les effets de champ*" (BOURDIEU;

[15] Berling (2012) calls "doxic battles" the mobilization of different types of capital in a field in which the doxa has been called into question. The term expresses a situation in which changes in the fundamental assumptions of a field are more abrupt and profound than the case of the incremental changes in which the doxa usually undergoes.

WACQUANT, 1992:76) – that obeys Bourdieu's idea that the boundaries of a *champ* cannot be defined but by empirical research.

There are as many *champ*s as one can conceive. In the course of his vast career, Bourdieu himself has dealt with numerous *champ*s, from the university *champ* and the *champ* of intellectuals (BOURDIEU, 1990) to the cultural (BOURDIEU, 1993) and scientific *champ* (BOURDIEU, 2004). In IR, Bourdieu-inspired scholars have worked with the most distinct *champ*s, as is the case of the humanitarian *champ* (LEANDER, 2008), the European security *champ* (MÉRAND, 2010; BERLING, 2010), transnational *champ*s of professionals of (in)security (BIGO, 2011b; 2013) and IR itself (ASHLEY *apud* LEANDER, 2008).

The universe of the cyber security *champ*, in the same fashion, is composed by distinct actors not only from the public bureaucracies and the private sector and their experts, but also from experts in the think tank *champ* as well (see MEDVETZ, 2012 on the *champ* of think tanks). Some actors transit between the most distinct *champ*s. For example, public bureaucracies and private actors are well known for taking part in struggles in the *champ* of power (BOURDIEU; WACQUANT, 1992; LEANDER, 2008). Last, but not least, the importance and the part taken by the hacker community in this struggle can be glimpsed in the impact that their practices have for ordinary users' cyber security, corporate cyber security and states prerogative to secrecy, as is case of *Anonymous* (DUNN CAVELTY; JAEGAR, 2015).

Bourdieu uses the expression 'game' to make sense of *champ* dynamics. This idea refers to the nature of the involvement of agents in a *champ*, the investment in the game which he terms *illusio*. The notions of illusion and interest play the role of synonyms in Bourdieu's lexicon, despite the author's later preference for the first (see BOURDIEU, 1990:48 and 87; BOURDIEU; WACQUANT, 1992:91). Each *champ* has a specific form of *illusio*, which also varies depending on the agents' structural position (how much capital he/she disposes, for example) and trajectory in the *champ* (the agents' habitus)[16], or system of predispositions acquired through a relation within a given *champ*. Interest and *illusio* express an idea of an investment

[16] Bourdieu stresses that the notion of habitus, contraposing that of Rational Actor Theory, aims to show that behavior is not necessarily the product of a conscious strategy or mechanical determination. Agents "act" according to a practical sense, a social nature, acquired through their historic of relations to the field. He argues that agents "fall" into practices instead of freely choosing them. (See: BOURDIEU, 1990:90).

that is opposed to the very idea of indifference, once, in Bourdieu's words, "*l'illusio (...) c'est le fait d'être investi, pris dans le jeu et par le jeu.*" (BOURDIEU; WACQUANT, 1992:93). This investment is, in a nutshell, both a condition of the functioning of the *champ* and what makes agents get together, compete and struggle with each other. It is, furthermore, a product of the way in which the *champ* functions (BOURDIEU, 1990).

The relation between the *champ* and the capital is one of dependence. In Bourdieu's words, "*un capital n'existe et ne fonctionne qu'en relation avec un champ*" (BOURDIEU; WACQUANT, 1992:77) and it may acquire a variety of forms, the economic, the cultural and the social being the three fundamental types (BOURDIEU; WACQUANT, 1992). It is the capital, this resource in a specific *champ*, that confers both a power over the *champ* and the conditions to an agent to have access to the profits at stake in it[17]. And, due to its dependence on the *champ*, the hierarchy between forms of capitals vary in relation to the *champ* under analysis. In that vein, the different kinds of capitals held by agents in a *champ* influence their position in it and, hence, the concept of capital is relevant for establishing an agent's position within the *champ*. The notion of capital is not one to be assimilated to the economics conception of it in terms of money or property, although both conceptions may crosscut (LEANDER, 2008).

Berling (2012) suggests that in IR "the concept of capital can provide a discussion of points of access to a certain domain—a *champ*—for different types of agency" (BERLING, 2012:455), once capital is important in the selection of agency in a given *champ*, as well as in the establishment of a boundary for participating in the international domain. She thus argues that a Bourdieusian approach to IR can provide a multi-dimensional analysis of power which can

> turn the question of powerful agency into an empirical analysis in which different types of field-specific capital serve not only as power bases in the struggles in a field, but also as points of entry to the field for different types of actors. (BERLING, 2012:464).

Issues of power in the cyber security *champ* do not vertically emanate from either the private actors or the government. What the concepts developed in Bourdieu's sociology allow is visualizing the state, the *champ* of power, as the

[17] In IR, the role of capital remains underexplored. An exception is Berling's (2012) work which stresses its role as a condition of access to the field.

principle of organization that serves as the basis for dissent across the most varied *champs*. As the author notes, it is necessary first to have a consent regarding the ground of disagreements and how these disagreements are to be expressed (BOURDIEU, 2014). This allows for problematizing the 'state' and visualizing what are the agents, either in the form of individuals or organizations, that struggle in the *champ*.

The practical outcome of analyzing the social world through Bourdieusian thinking tools is that they enable visualizing the relationality of power dynamics within society, where power and domination are manifested through social struggles and agents' positions in the *champ*. These struggles do not happen isolated in time and space, but concurrently with other struggles in separated – though often overlapping – *champs*. In the case of private actors, it makes it possible to avert the neoliberal idea that their interest is purely economic and to see the politics of their investment in a given *champ*. Social reality, in turn, hardly follows the pernicious separation between economics and politics present in economic theory.

Current practices and competing understandings of cyber security can thus be seen as resulting from competitions between agents about what counts as insecurity. Examples are disagreements over important questions such as: what kinds of phenomena constitute a cyber security risk and which is/are the most urgent? Are viruses the most pernicious form of insecurity or are vulnerabilities in networked systems? When are *hacking* practices 'lawful'? Should 'security' be constituted a core value in cyberspace?

The resulting practices and understandings are not restricted to what state actors say or do to increase/decrease cyber security; they are also products of distinct forms of characterization and perception of threats by market actors, when they advertise their products/services or attempt to provide technical assessment over a perceived security issue. The most recent move in the antivirus industry, for example, has been to question the value and utility of this technology in face of networked technologies and evolving security issues, such as the case of zero-day vulnerabilities (DUNN, 2014; MCAFEE, 2015).

The investment in the cyber security *champ* is directly related to the stakes in it. Primarily, at stake, it is the power to 'define' what cyber security is. The power to name is constitutive of the symbolic dimension as it influences all the material dimensions also at stake. The security/freedom dichotomy is a constitutive part of

this particular struggle, as it is the security/privacy one, in which more security requires less privacy (for the regular user). Influenced by this defining power, is the possibility of having access to, profiting from or even expanding the lucrative cyber security market – which is not an exclusive interest of private companies, but also of freelancer computer experts and hackers acting in the black market.

For entering the cyber security *champ*, agents need a combination of two resources: economic capital and technical expertise on ICT and computer security. Expertise and technical knowledge of ICTs figure as the most relevant among them – hackers, private companies and government bureaucracies are all imbued with it. This very specific form of knowledge is necessary for individuals and groups to 'master' the *champ* of computer security (HANSEN; NISSENBAUM, 2009). Even in cases where technical expertise might, at first, seem to not be involved, it is actually required, as it is the case of public policymaking (NISSENBAUM, 2005). But even if it grants access to the *champ*, technical skills alone do not suffice to guarantee an agent's position in the structure of the *champ*. Just like in the economic *champ*, the economic capital of the agent is of great importance to assess its power.

Governments and technology corporations figure as powerful actors in the cyber security *champ* because in each case there is a specific combination between technical expertise on ICTs and economic power that represents both an improved ability and availability of resources to strengthen security standards and protocols and either develop or buy specific goods, as it is the case of zero day vulnerabilities (see FIDLER, 2014).

But there remains an important concept developed by Bourdieu that is extremely useful for understanding the dynamics of the *champ*, which is the notion of strategy. This is another concept that is actually relevant for understanding how things happen in a *champ*, the nature of agents' practices and relations. According to Swartz (1997) the notion is intrinsically related to that of action and interest: "action as strategy conveys the idea that individual practices are fundamentally interested, that actors attempt to derive advantages from situations" (SWARTZ, 1997:67).

In that vein, it is possible to read some practices of private companies, such as the selling of their products, the advertisements and their own discursive constructs – in the media, in their own websites, blogs, by writing reports and even

hosting their own online magazines[18] – as strategies to expand their power in the *champ* of cyber security. This notion of power is strongly associated with the number of clients, as well as their nature (governmental actors, other corporations, regular users, and so on) and, fundamentally, the profits the company makes through its products/services. The expansion of the market is thus a fundamental end that guides these practices and a stake that is a particular result of the working of private interests in the cyber security *champ*. A better and detailed account of how these agents strategize about cyber security will be provided ahead in the work.

To summarize, a Bourdieu-inspired reading of IR brings power dynamics to the fore through a link between social practices and discourses (LEANDER, 2008). Both the concepts of the *champ* and the capital are useful because they can guide the research towards uncovering the variety of relations, practices and perceptions (*habitus*) that structure a given social reality, or, in Berling's (2012) words, the material and symbolic forms of power make up for struggles in a *champ*. In what concerns cyber security, it provides a reading of the practices of private companies as strategies. These agents struggle and cooperate over distinct ends: to guarantee a contract with the government; or to contest attempts to restrain their activity; to surpass concurrence; to sell products and services and so on. Often portrayed as partners and strategic actors in governmental speeches to 'secure' cyberspace[19] these actors' practices tend to be overlooked or receive little attention when one comes to make sense about who creates cyber security/insecurity.

Once it becomes possible to deconstruct the notion of the nation state and thus visualize the practices of agents of the most varied nature within a *champ*, the role of private companies in cyber security and this very specific social universe can be problematized. More than that, these practices can be read under the lens of the phenomenon of marketization of security, which suggests that the dynamics between the public and the private are more complex than the term privatization, a

[18] It is not uncommon for companies to host their own publications and cyber security awareness section. See Symantec's (https://www.symantec.com/security_response/publications/) and Kaspersky's (http://www.kaspersky.com/internet-security-center) websites. The US defense contractor Raytheon, for example, hosts its own technology magazine (http://www.raytheon.com/news/technology_today/2015_i1/).

[19] See the 2011 Strategy to Secure Cyberspace, which stresses the importance of public-private partnerships to construct cyberspace security; see: White House (2011); see also the Cyberspace Policy Review, which emphasizes the shared responsibility of public and private sectors in the security of cyberspace. See: White House (2009).

term often used in the literature of private security studies (see SINGER, 2002; LEANDER, 2009a), can capture.

How these agents contract with the government, the extent through which functions traditionally conceived as a 'monopoly' of the state are shared with large and small companies, the issue of secrecy and the extent through which, to gain space in the *champ* of cyber security, these companies have adopted the most distinct strategies, ranging from economic actors' practices of selling and advertising to perception building through discourses about risk and vulnerability, are all matters that can be captured and analyzed with the concepts that have been present in the chapter.

The next part of the work will provide an empirical account of the cyber security *champ*. The intention is to show how the practices of private companies can produce specific understandings of security, threats and risk. The second chapter introduces the historical constitution of the technologies and mentalities underpinning the background knowledge collectively shared among the agents invested in the *champ* of cyber security. These technologies and mentalities are strongly related to the strategies adopted by private actors. Then, the third chapter investigates the dynamics of the *champ* itself, providing a contextualization of the struggles and an assessment of the practices and strategies of private companies in the cyber security market. Next, the fourth chapter analyzes the disputes between companies for the prominence of certain approaches to cyber security. Lastly, the work provides some concluding thoughts about the implications, for security, of the struggles among private companies in the cyber security *champ*.

3. Computers at risk: legitimizing the cyber security market

The current state of affairs in cyber security is, in part, an outcome of the evolution of information technologies and of the perceptions of its impacts on social life. Sketching the history of this set of technologies is an important step in apprehending the space of positions and position-taking in the cyber security *champ*. Further, it helps identifying the background knowledge that informs the practices of agents in the struggle for cyber security.

Thus, in order to understand how struggles in the cyber security *champ* legitimize the cyber security market, this chapter will explore the historical evolution of information and communication technologies (ICTs), paying attention to the information society thesis as an attempt to make sense of the social impacts of these technologies. The main argument is that these two phenomena, ICTs and the perceptions of its impacts on society, take part in the broader effort to legitimate the cyber security market. Both phenomena have contributed to fundament and boost some of the existent regimes of justification about the importance of securing existing networked technologies. The idea of an information age has been pervasive in recent analysis about the influence of technological developments in society (NEGROPONTE, 1995; KARATZOGIANNI, 2009; CASTELLS, 2010; SIMMONS, 2011) and it has consequences for how securities and insecurities are understood.

The development of computing technologies to their current stage and the exponential growth in the number of people connected to the Internet are directly tied to the privatization of cybernetic technologies in the 1980s (DUNN CAVELTY, 2016). In turn, the strong presence of the market in the evolution of these technologies also influenced how to think and conceive the security issues that arise because of them, hence the variety of actors addressing them as 'risks' (CSTB, 1991; PCCIP, 2000).

The first part of the chapter will explore the pervasiveness of the information society thesis in sociological and IR thought. The goal is to understand how these attempts to make sense of technological changes have contributed to reshaping security thinking. Next, the chapter will trace the development of computing technologies in order to assess the social context behind advances in ICTs. Our argument is that these technologies flourished among public funding and the private

initiative. Marketization allowed their exponential diffusion to everyday life and has informed the main security concerns underpinning the information society thesis. The case of the Internet is somehow paradigmatic, as it started as a public funded research network and became marketable in the 1990s.

Then, the chapter will explore the marriage between securing Critical Infrastructure Protection (CIP) and ICTs. CIP grounds many calls to 'secure' cyberspace and is central to cyber security. The debate incorporates the thesis that ICTs change the way security is understood. The notion of 'threat' as something imminent, direct and very diffused is replaced by the notion of 'risk', to make reference to the uncertain and future nature of most security challenges of the 'information age' (DUNN CAVELTY, 2009a). Risk-based thinking is characterized by the confluence of different attitudes (providence, prevention and precaution) in face of the uncertain and it orients the practices of agents in the *champ* of cyber security, particularly in attempts to reduce the 'inherent vulnerabilities of cyberspace'.

The marketization of ICTs can be read as a strategic move that have altered the dynamics and set important grounds for the development of the cyber security *champ*. The effort made in the chapter aims to lay the groundwork for the analysis of the positions agents take in the *champ*. The way in which security breaches in systems and software are understood as "vulnerabilities" and risk-based thinking represents an attitude in face of the phenomena that remain 'unknown' to this market, as well as the translation of risks to cyber (in)security, are useful for unraveling the intricate dynamics of the cyber security *champ*, and they will further allow the visualization of agents' positions, the struggles among them and the strategies they use, to be set forth in the next chapter.

3.1. The information society thesis

Technological developments have been a source of fascination not only for people involved in their creation, but also for people concerned with their impact on society. Western societies have been rarely at ease with the technological advancements they often celebrate. New inventions tend to be followed by concerns with their impacts on everyday life and on broader societal organization. And, most often than not, the ideas associated with new inventions come to inform how their

importance for every life is conceived. A computer with access to the Internet can be just that or it can be a revolutionary tool capable of changing the most central aspects of modern economy, culture and politics.

Terms such as "the global information age" (SIMMONS, 2011); "information society" (WEBSTER, 1997); "information age" (ALBERTS; PAPP, 1997; DAY, 2001); "network society" (CASTELLS, 2010); and "information technology revolution" (NYE, 2004; CASTELLS, 2010) are employed to make sense of technological changes triggered by advances in micro-electronics and communication technologies. Although it is possible to speak of information society 'theses', the use of the term "information society thesis" in this chapter aims to provide a common ground for all these conceptualizations as their core concerns converge to address the extension and impact of ICTs within society[20].

The information revolution concerns the set of technologies subsumed under the heading of ICTs, characterized by the application of knowledge and information to knowledge generation, information processing and communication devices and marked by a global reach integration between computer and telecommunication technologies, with the use of information to overcome distance, time and location[21] (DUNN CAVELTY, 2002; 2007; CASTELLS, 2010). These technologies have allegedly benefited networked (instead of centralized) forms of organization and communities where information flows play a central role (NYE, 2004; CASTELLS, 2010; SIMMONS, 2011).

Castells' (2010) version of the information society thesis[22] is the most diffused, holding that ICTs are transformative technologies that alter the conditions through which social and economic relations take place. These technologies are as

[20] Criticism to the information society thesis stresses the failure of most accounts in setting out clearly in what ways and why is information becoming so central to the point it ushers a new type of society. In the same vein, it expresses a concern with the overdependence of quantitative measurements – or the question of how 'more information' is altering qualitative aspects of societal life (see WEBSTER, 1997).

[21] For Castells (2010), it also includes biology and artificial intelligence.

[22] Castells (2010) establishes a distinction between the terms 'information' and 'informational' societies based on specific forms of social organization. The idea of an information society emphasizes the role of information within a given society and is not necessarily representative of the mode of organization of the current societies. Distinctly, the term informational society indicates a form of organization based on how new technological conditions make possible for information generation, processing and transmission to be sources of productivity and power. The author's main concern is with the impacts of technology in the organization of society and it considers the 'information economy' as a transition in world's industrial history (see also: WIENER, 1989; ROSZAK, 2005).

central to the information revolution as the steam engine, electricity, fossil fuels and even nuclear power were to the previous, successive, industrial revolutions. The new paradigm is characterized by: having information as its raw material; the pervasiveness of its effects; applying the logic of the network in any system or set of relationships depending on ICTs; its flexibility; and the indistinctness between its constituent parts, due to the convergence of their technological trajectory into a highly integrated system.

The evolution of ICTs is marked by the deep integration between digital computers and human living. The imbrication of software and ICTs in everyday life comes as a consequence of the growing interconnectedness and flexibility of digital technologies and is what makes them so powerful. Computers can be programmed to do a variety of things and so, they become pervasive and ubiquitous (HOVEN; WECKERT, 2008; CASTELLS, 2010; KITCHIN; DODGE 2011). Disruptions in the normal functioning of objects and infrastructures dependent on these technologies range from minor nuisances to major incidents with serious economic, political effects and even life-threatening situations (KITCHIN; DODGE 2011).

The logic of ubiquitous computing fed debates about a fourth industrial revolution, based on the integration of cyber-physical systems, on the Internet of Things (IoT), big data, cloud computing, nanotechnology, biotechnology, artificial intelligence and robotics (SCHWAB, 2015; EUROPEAN COMMISION, 2016). The information revolution would be the third revolution in history, preceded by the mechanization of production – the first revolution – and by the advent of electrical power – the second. The discourse does not change much: the distinction of this revolution in relation to the previous one is because of the greatest (and disruptive. And unprecedented. Also exponential) speed, scope and impact of today's transformations (SCHWAB, 2015).

In IR, strong attention has been paid to the impacts of the 'information revolution' – understood more or less commonsensically as the society's widespread dependence on ICTs and their growing importance to international affairs – on security (ERIKSSON; GIACOMELLO, 2006; 2007). In fact, concerns with technological change affecting international security affairs are not new: they have accompanied theorization since the early 1900s, and have been particularly strong during the Cold War's fears of a thermonuclear Armageddon (MCCARTHY, 2015). But the technological revolution has fostered in the discipline a whole new

commonsense focused on a global interdependence enabled by the transnationalization of production and by the development and continuous spread of communication technologies since the 1970s (KEOHANE; NYE, 1998; NYE, 2004; MCCARTHY, 2015).

The adoption of some core concerns of the information society thesis by IR has been partially influenced by a growing dialogue with other disciplines, particularly sociology. This dialogue has resulted in a contestation of the domestic/foreign divide, with a focus on issues that either transcend or merge domestic/foreign issues. Nevertheless, IR has unevenly addressed the information society thesis *per se* and its core focus has been on the impacts of technology on matters of security, power and global politics (see ERIKSSON; GIACOMELLO, 2006; NYE, 2004).

McCarthy (2015) pays attention to the role of information technologies for theory-making in IR and argues for its centrality to the core concerns of the discipline (for example, the changing nature of global governance and transnational regulation; the transformation of the state; possibilities for democracy and concerns about hegemonic transition in the international system). This is an important move to bring information technology to the core of IR debate – instead of treating it as an exogenous phenomenon. Yet, whilst the author addresses some core points of the information society thesis, less attention is given to the thesis itself.

Within the discipline, theorization on technological change, and particularly on the social and political impact of ICTs, has been criticized for being either too instrumentalist or too essentialist (MCCARTHY, 2015). In this vein, when a technological object is not judged by its use, without major considerations of its characteristics, it is otherwise perceived to "cause" social and political change through its inherent characteristics. McCarthy (2015) argues that this deterministic bias precludes possibilities of understanding ICTs as forms of social power.

State control, or the gradual loss of thereof, over certain forms of power is an underlying preoccupation in IR considerations about ICTs (NYE; OWENS, 1996; NYE, 2004; SIMMONS, 2011; MCCARTHY, 2015). A common assumption is that the global information age, this age where information is considered to be a central asset and resource (NYE; OWENS, 1996; NYE, 2004; DUNN CAVELTY, 2007; CASTELLS, 2010), casts doubt on the traditional notion of power associated with coercion and military weapons and marks the increasing importance of non-

state actors, such as firms, interest organizations social movements and transnational networks, in security politics (ERIKSSON; GIACOMELLO 2007; DUNN CAVELTY, 2007). As Nye (2004) argues, the effects of 'information' on 'power' takes foreign policy out of the exclusive control of governments:

> What this means is that foreign policy will not be the sole province of governments. Both individuals and private organizations, here and abroad, will be empowered to play direct roles in world politics. The spread of information will mean that power will be more widely distributed and informal networks will undercut the monopoly of traditional bureaucracy (NYE, 2004:82).

Dunn Cavelty (2007), on the other hand, provides a distinct insight of this process of power redistribution allegedly facilitated by ICTs and by the centrality of the information paradigm. At the heart of her argument is the idea that complexity and change are two distinctive characteristics of the information age. They allow understanding this historical moment as marked by persistent opposites in which order comes from episodic patterns with contradictory outcomes. Thus, instead of providing some alarming or thrilled account of the 'loss' of state power, she argues that the outcome of the rearrangement perceived in the challenge to state's position as the major player in economics and in the international system:

> will likely be a skewed, complex and volatile pattern of power distribution, as transfer of authority occurs in diverse directions, and as changes are absorbed and operationalized by different actors, at different levels, in different ways and at different speeds (DUNN CAVELTY, 2007:90)

From a critical viewpoint, the information society thesis captures the centrality of information in Western thought. The working of modern ICTs relies on the production, storage, communication and use of information. In addition, the development of the cybernetic science, which anchors these technological advances, granted information the privileged status of an asset, or a valuable quantity, as information is considered the central element of such scientific approach (ROSZAK, 2005; DAY, 2001). As Day (2001) notes, the central place granted to information in the 'informational age' makes information both a synonym for knowledge and an 'economically valuable thing' (DAY, 2001:1).

Conceiving information as a valuable asset has consequences for thinking security in the digital age[23], as the integrity of information becomes object of

[23] Digital age security includes both the information infrastructure run by ICTs and cyber threats, while the means of attack can either target physical infrastructures underlying ICTs, such as telecommunication cables, or virtual, targeting networked communications and systems (DUNN CAVELTY, 2007).

protection and the risk of losing it is attributable to a perception of increased vulnerability and loss of control resulting from the move from an industrial to an information society (ERIKSSON; GIACOMELLO, 2007). As such, it enhances security policies' focus on the vulnerability of governmental and military digital infrastructures, on the one hand, and on the commercial providers that own and operate most of these infrastructures, on the other, as well as the security requirements for their operation worldwide (PAPP; ALBERTS, 2000; DUNN CAVELTY; BRUNNER, 2007).

Digital age security hinges on risk: from the inherent risk of system-failure to the risk of an attack by a third party. As information technologies spread through the social fabric, and the operation of everyday activities, from communications to finances, became dependent on them, vulnerabilities started to be perceived as risks to security (CSTB, 1991). A particular feature of computing technologies is that "a computer may be under attack for an indefinite length of time without any noticeable effects" (CSTB, 1991:15), which incurs in the possibility of overlooking the traces of attacks by mistaking them for benign events or simply because they leave no clear traces. Computerization presents security challenges stemming from the nature of informational technologies, which include the vulnerabilities derived from the programmability of computers, the interconnection of systems and their use as a part of complex systems that comprise infrastructures dependent on software (CSTB, 1991). The relation between critical infrastructure and risk grounds most of the appeals to secure cyberspace and will be addressed later in the chapter.

The adoption of the information society thesis by IR allowed visualizing certain security challenges associated to the pervasiveness of ICTs in society. Theoretical, policy-oriented and even critical approaches to cyber security tend to incorporate these concerns, in part or in their totality, in an almost naturalized way (ARQUILLA; RONFELDT, 1993; DUNN CAVELTY, 2002; ERIKSSON; GIACOMELLO, 2007; LIBICKI, 2007; DEIBERT; ROHOZINSKI, 2010), to the point that some of the core assumptions of the information society thesis can be

read as a commonsense grounding cyber security[24]. The problem with this naturalized adoption of the information society thesis is that it also adopts a naturalized view of technology in accordance to how it is described by some information society theorists. In this context, a certain technological determinism has prevailed. But as the information age comes to be seen as the natural consequence of technological developments, their impact on issues of justice, equity and politics becomes obfuscated (MAY, 2002).

The next section will dissect in more detail the technological developments behind the commonsense. Both the development and diffusion of ICTs are closely tied with varying degrees of processes of marketization, intensified with the 1970s capitalist crisis and involving distinct patterns of public and private enmeshment. It will approach the development of ICTs and its social context, focusing on the institution fostering them. Social fluidity between military, academic oriented research and commercial practices contributed largely to the booming of ICTs and of the Internet and such fluidity remains useful for comprehending the main dynamics of the cyber security field.

3.2. Marketizing ICTs: the growth and diffusion of information technologies from the 1970s to the present.

The trajectory of the "development of ICTs" is quite difficult to approach, among other reasons because of the lack of consensus regarding where one should start when talking about ICTs – or about what set of technological advances adequately represents it. Contemporarily in IR and Political Science, the term came to refer to the set of information-based digital technologies developed in western countries, as it is the case of the digital computer, of networks such as the Internet, smartphones and others. In some cases, however, the interpretation is far more extensive so as to refer to any form of communication technology, from signal fires to flags (PAPP et al., 1997). Even if one sets its limits to the modern era, there is still a wide range of technologies falling into such category, as the case of the television. For the purpose of clarification, the section will approach technologies falling into Papp et.al. (1997) concept of the third information revolution. The focus

[24] These assumptions involve the information technology revolution and the alleged shifts in work, economy and production it generated, the centrality of information for the organization of modern societies and the concurrent social impacts of these tendencies.

is particularly on computing, which comprises machines and software, networked and telecommunication technologies. Distinctly from Castells (2010), the present analysis does not include genetic engineering, although the interrelation between informatics and biology is a promising and very interesting trend in debates regarding artificial intelligence.

The history of the development of ICTs can be divided in two moments: the first one concerns the development of micro-electronics[25] and other machine-related technologies and the second one concerns the development of networked technologies, among which the most successful example is the Internet. There is no clear-cut temporal division between the two processes, although the impact of the Internet was only felt in the early 1990s (NEGROPONTE, 1995; CASTELLS, 2001; 2010). ICTs are still developing and at a fast pace, and it is a difficult task to catch up to the most current trends in these areas. Yet, at the end of the section, the work pinpoints some recent developments that are influencing cyber security thinking, as is the case of the IoT.

The World War II and its aftermath are the birthplaces of both the first programmable computer and of micro-electronics, with the invention of the transistor[26]. Early computers were developed in Germany and in the United Kingdom, as war efforts to acquire technological superiority and defeat the enemy. In the US, also resulting from a war effort, the ENIAC computing system was built to be faster than any previous concurrent. All these wartime machines were enormous: ENIAC alone occupied more than 1,000 square feet and weighted about 30 tons. With their penetration into the civilian sphere by the 1960s, the use of computers, albeit difficult, became more available. The development of the transistor, patented by Bell Labs in 1947, and further advances in micro-electronics would allow for a gradual diminishment of these machines.

These advances were competition-driven, as a dispute in the electronics market began to materialize and government contractors entered the race for the computer age, as is the case of IBM in 1953, with its 701 vacuum tube machine.

[25] Micro-electronics refers to the subfield of electronics that studies and manufactures very small electronic designs and components.

[26] Transistors are semiconductor devices that amplify or switch electronic signals and electrical power. They are fundamental components of modern electronic devices, and are often embedded in integrated circuits.

The company would later dominate the computer industry, populated by companies such as Sperry, Honeywell, Burroughs and NCR. Except for IBM, none of these companies lasted to the present (see PAPP et al., 1997; CASTELLS, 2010).

Commercially, the application of the transistor remained restricted until the development of the junction transistor, in 1951. The later invention of the planar process[27], in 1959, by Fairchild Semiconductors, allowed integrating miniaturized components and precision manufacturing. The diffusion of micro-electronics in all machines came only in the 1970s, with the invention of the microprocessor[28] by Intel. The effects of miniaturization would spread to consumer's everyday living:

> (…) greater miniaturization, further specialization, and the decreasing price of increasingly powerful chips made it possible to place them in every machine in our everyday life, from dishwashers and microwave ovens to automobiles, whose electronics, in the 1990s standard models, were already more valuable than their steel. (CASTELLS, 2010:41)

For Castells (2010), the 1970s represent the core of information technology revolution with the diffusion of ICTs. The combination of "node" technologies, such as electronic switches and routers, and new linkages or transmission technologies revolutionized telecommunications and, additionally, the development of these technologies involved certain degree of market competition between Bell Companies and Canada's Northern Telecom. But, as the author notes, it was the convergence of most electronic technologies developed from the World War II on into the field of interactive communication that led to the development of the Internet.

Jordan (1999) suggests that the interest of US defense contractors in computers, as part of defense research, forced the Department of Defense's Advanced Research Project (ARPA) to give a significant step in the direction of the unification of the use of computers in a single terminal by conceiving a project to network computers, what would be later known as ARPANET, or Internet's "mother". Castells (2001; 2010) argues that the US government was motivated by great power competition with the Soviet Union, and felt alarmed by the 1950s

[27] The planar process is an advance in the manufacturing of small components in the semiconductors industry, as it is used to build individual components of a transistor and to connect them together. This is the primary process by which integrated circuits are built.

[28] Castells (2010) calls the microprocessor "a computer in a chip". The device incorporates the function of a computer's central process unit (CPU) by accepting digital data as input, processing it, and providing results as outputs.

launching of the first Sputnik. The author describes the creation and development of the Internet in the last decades of the 20th century as resulting "from a unique blending of military strategy, big science cooperation, technological entrepreneurship, and countercultural innovation" (CASTELLS, 2010:45). This enmeshment between science, the public and the private sector is also emphasized by Papp et al. (1997) in what concerns the development of computer technologies:

> A third generation of computers based on integrated circuits emerged as computer technology continued its rapid advance. Much of the ongoing research was funded by the U.S. Department of Defense. The unique relationship that developed between the government, the military, and industry helped create an innovative environment for the invention of information and communications Technologies. (PAPP et al., 1997:26)

ARPANET went online in 1969, connecting the University of California, in Los Angeles, Stanford Research Institute, the University of California in Santa Barbara and the University of Utah. Its basic objective was to allow communication between computer terminals, but it ended up being a tool of communication for researchers and scholars in defense projects. The intense flux of personal communications caught the designers of ARPANET by surprise because "rather than people using ARPANET to communicate with computers, as the designers expected, people used it to communicate with other people" (JORDAN, 1999:38).

Because of this particular application, other networks were developed. For example, in the 1980s, the National Science Foundation (NSF) became involved in the creation of two distinct networks: CSNET, and, in cooperation with IBM, a network for non-science scholars called BITNET. ARPANET was, however, the backbone communication system of both networks. What is nowadays known as the Internet derives from this specific use of ARPANET as the network of the networks – although ARPANET itself was closed in February 1990.

The Internet was "privatized" in 1995, with the extinction of the existing NSFNET – NSF's own network, developed still in 1984. Castells (2010) suggests that among the 'forces' that led to the closing of this last governmental operated Internet backbone there were commercial pressures and the growth of private corporate and non-profit cooperative networks. Since then, global networks have expanded enormously and significant shifts in the operation of the Internet occurred. A current trend is that technology companies that traditionally operate software, like Google or Facebook, now design their own hardware as a way to reduce costs and improve efficiency. Telecommunication companies, like AT&T

and Verizon, have signaled interest in pursuing this model, which will have implications for businesses of traditional hardware suppliers, like Cisco, Dell, HP and IBM (METZ, 2016). The Internet's architecture today derives from the competition among these companies.

This brief account of the development of ICTs tells us something about the relations and forces behind technological development. As stressed by Castells (2010), scientific, institutional and personal networks between the Defense Department, the National Science Foundation, major research universities and technological think tanks were behind the development of the Internet. The node of private companies should be added. Some companies were behind think tanks such as ATT's Bell Laboratories and Palo Alto Research Corporation, which was funded by Xerox, and many others. Computer scientists enjoyed great mobility between these various institutions, creating a "networked milieu of innovation which dynamics and goals became largely autonomous from the specific purposes of military strategy or supercomputing linkups" (CASTELLS, 2010:48).

The Silicon Valley is perhaps the best example of market's participation in the information revolution. In the 1970s, the site saw the development of core technologies in micro-electronics[29], thanks to the convergence between a large pool of skilled engineers and computer scientists from the major universities in the area; an assured market dependent on the generous funding of the Defense Department and the development of an efficient network of venture capital firms[30]. Besides, the dynamism of its industrial structure in relation to the rigid, large and well-established companies in the East, allowed the diffusion of new startup firms and knowledge diffusion through job hopping and spin offs. Investors in venture capital firms in Silicon Valley would also distinguish themselves for being knowledgeable about the projects in which they were investing due to their origins in the electronic industry (CASTELLS, 2010).

This conjunction of factors is, according to Castells (2010), also behind the ease with which Silicon Valley was able to capture the industry of the Internet, in the occasion of its 'privatization':

[29] Examples are the integrated circuit, the microprocessor and the microcomputer.
[30] Castells (2010) also notes the importance of the early institutional leadership of Stanford University.

> Leading Internet equipment companies (such as Cisco Systems), computer networking companies (such as Sun Microsystems), software companies (such as Oracle), and Internet portals (such as Yahoo!) started in Silicon Valley. Moreover, most of the Internet start-ups that introduced e-commerce, and revolutionized business (such as Ebay), also clustered in Silicon Valley. (CASTELLS, 2010:65)

Thus, defense spending, scientific research, private companies and individual entrepreneurs were all driving forces behind many of the emerging ICTs. The history of these technologies has been marked by an interesting combination between public funding and private research, both in academic and think tanks environments. In the case of the Internet, even before its 'privatization', to use Castells' term, establishing a distinction between what was exactly government, university and business (for instance, a Boston firm named BBN was contracted to build ARPANET) soon became a difficult task for those outside the booming technological environment. The naturalized 'job hopping' practice between distinct public/private institutional environments also contributes to such perception.

The commercialization of these technologies is accountable for their all-embracing diffusion. In fact, as Castells (2010) notes, technological innovation has been market-driven since the 1970s. In a sense, the US has been the core of this burgeoning market. Some of today's biggest IT companies were born in the country, and, searching for new market niches in products and processes, foreign companies often establish their business there too. In addition, in the US, the state played an important role in fostering such markets by funding and contracting out with these companies (CASTELLS, 2010).

Before resuming this topic, a few words about current trends in information technology are important, due to their impact on cyber security thinking. Since the commercialization of the Internet, in the early 1990s, navigation and connectivity were improved, and spread around the world. The expansion and increased marketization of the Internet are leading to the gradated shift from IPv4 to IPv6 protocols. In practice, this means that there is need for more room *online*, since today's Internet is so 'overpopulated' that the availability of IPv4 addresses has run out. Recent developments in information technologies have contributed to this shift and one worth stressing is the phenomenon of the IoT.

Also named industrial internet, Machine-to-Machine communication (M2M) and ubiquitous computing, the IoT represents the most recent trend of embedding computers in *things* (WEISER, 1999; EVANS, 2011; KELLMEREIT;

OBODOVSKI, 2013). The IoT is a network of coded objects, devices, vehicles, buildings and others, that collect and exchange data[31] (see ITU, 2012). Put simply, it is about machines 'talking' to other machines and providing data for Internet businesses so they can act upon it (KELLMEREIT; OBODOVSKI, 2013). Modern smartphones are representative of this trend, as are smart TVs, houses, cities and all the "smart" stuff. In this sense, "IoT describes a world where just about anything can be connected and communicate in a 'smart mode' by combining simple data to produce usable intelligence." (BARAJAS, 2014). Sterling (2014), on the other hand, criticizes this discourse for being a 'slogan' that disguises what he terms "epic struggle" over power, money and influence between some of the information age biggest companies. For him, the IoT is an "all-purpose electronic automation through digital surveillance by wireless broadband" (STERLING, 2014:5).

The implications of ubiquitous computing for cyber security are manifold. Surveillance (both governmental and for marketing purposes) and third party exploitation are examples. Personal information and business data existing in the cloud[32] can be accessed/stolen due to exploitable vulnerabilities in at least one of the many devices that connect them. It suffices to have one weak link in the security chain to be vulnerable to third party exploitation. Thus, user privacy is a serious concern in this interconnected world of things (BARAJAS, 2014; GREENBERG; ZETTER, 2015). And, of course, hackable digital objects are not targeted only by malicious hackers. They are also attractive to government intelligence agencies (STERLING, 2014).

The IoT debate represents one of the most current trends in the development of information technologies. The commercialization of the Internet in the 1990s and its global expansion have been already pointed as directly related to the proliferation of security vulnerabilities, particularly in what concerns the security of critical infrastructures (PCCIP, 2000). Critical information infrastructure protection has been portrayed as a national security issue in the US and fundaments

[31] The Cisco Internet Business Solutions Group (IBSG) considers the IoT as the point in time when more "things or objects" were connected to the Internet than people.

[32] Cloud computing refers to the possibility of accessing files and executing tasks through the Internet. By definition, it is an on-demand computing model of autonomous, networked IT (hardware and/or software) resources. In practice, IT activities are outsourced to one or more third parties with rich pools of resources (HASSAN, 2011).

most of cyber *securing* moves from both governments and the private sector. The next section will present some considerations about the relation between CIP and risk-based approaches to security. This is an important link that supported cyberspace securing efforts and laid the groundwork for a burgeoning cyber security market.

3.3. Critical infrastructure protection, risk and public-private partnerships

The CIP debate has been, for some time, associated to threats coming from and because of cyberspace (ABELE-WIGERT; DUNN, 2006; DUNN CAVELTY, 2005, 2009c; 2015; ARADAU, 2010; PCCIP, 2000; PALLUAULT, 2011). The concept embraces a wide range of sectors in the economy, industry and government, such as energy and electricity, water supply, transportation, logistics and distribution, government services, emergency and rescue, as well as health services, banking and financal services and telecommunications and ICTs (DUNN CAVELTY, 2009, 2015; GAO, 2016). What is central in CIP are the economical and national security risks of having these infrastructures, in which modern societies are grounded, incapacitated or even completely destructed (ABELE-WIGERT; DUNN, 2006, ARADAU, 2010; PALLUAULT, 2011).

The argument sustained hereafter is that CIP debate has been marked by an urge to secure both physical and digital infrastructures. Efforts to secure infrastructures are anchored in the distinction proposed by Deibert and Rohozinski (2010) between risks to cyberspace, which include CIP, and risks through cyberspace, understood as risks that arise from cyberspace but do not target (physical) infrastructures *per se*. This distinction is not at odds with Denning's (2003) argument that cyber security should be viewed as an infrastructure in itself, if one accepts that digital infrastructure can coexist with, but be independent from, the physical ones. Attempts to secure cyberspace tended to include both aspects of infrastructures, once cyberspace can become a force-multiplier if the possibility of risks to cyberspace and risks through cyberspace are combined[33] (see DUNN CAVELTY, 2008).

[33] The section will not delve into the debate concerning the distinction between CIP and Critical Information Infrastructure Protection (CIIP). The latter's focus is on protecting data and software residing on computer systems that operate critical physical infrastructures. The distinction has become prejudicial for understanding how CIP has been conceptualized, once in the context of

It is worth noting that the concern with the protection of vital assets dated back to the World War II. But only in the 1970s and 1980s national security experts turned their attention to the possibility of infrastructure discontinuity due to disruptions or third party attack (DUNN CAVELTY, 2007; 2009; COLLIER; LAKOFF, 2008). In the 1990s, developments in information technology and the attention of policy-makers and security experts gave a new impetus to CIP in security debate, with a focus on cyber-infrastructures[34] (DUNN CAVELTY, 2008; 2015).

This focus was an answer to a growing concern with the interdependency created by information technologies that the US government had developed in the 1980s. According to the President's Commission on CIP report (PCCIP, 2000), the interlinkage between connected infrastructures has created a new dimension of vulnerability, that combined with the emerging constellation of non-traditional threats, was believed to pose "unprecedented risk" (PCCIP, 2000:225).

Information infrastructure has, thus, been a core aspect in CIP debate. Still in the 1990s, it was established in security and political circles that key sectors of modern society increasingly relied on a spectrum of interdependent software based control systems for their continuous operation (ABELE-WIGERT; DUNN, 2006). Today, ICTs have emerged as a common factor upon which distinct sectors of society converge and the topics of cyber security and CIP are often handled as one thing only (DENARDIS, 2014; DUNN CAVELTY, 2015). Vulnerabilities in critical infrastructures are attributed to the centrality of information infrastructure in the operation and functioning of core assets and infrastructures (DUNN CAVELTY, 2009).

Vulnerability is portrayed as an inherent feature of information infrastructures, due to not only third party exploitation, but also risks of internal

critical infrastructure policy debate, physical infrastructures have grown strongly dependent on information technologies. However, there have debates on the nature of cyber security as an infrastructure in itself. Denning (2003) advocates for this perspective. This view, however, tends to exclude aspects of information security that deal with information that is not digitalized. Yet, on the distinction between CIP and CIIP, Dunn Cavelty (2005) suggests that both should not be viewed as separate concepts, but instead, CIIP should be viewed as an essential *part* of CIP. In this sense, a focus on cyber threats would risk ignoring important physical threats, which would be as dangerous as neglecting the virtual dimension of the problem.

[34] The notion of cyber-infrastructure is anchored on interdependency. According to Deibert and Rohozinski (2010), through cyberspace, electronic clearances take place, irrigation systems are controlled, hospitals and educational systems interconnect, and governments and private industries of all types function. For CIP, this implies that critical infrastructures do not need to be attacked physically, but may be targeted through electronic or virtual means.

failure (PALLUAULT, 2011). The President's Commission report emphasizes how vulnerability constitutes a security problem in more than a single occasion (PCCIP, 2000:225, 228-229, 233). Collier and Lakoff (2008) argue that CIP is based on an understanding of security threats as *system-vulnerability*. This setting derives from a perception that 20th century's technological and political developments rendered existing security frameworks inadequate, which has led experts to invent new ways of identifying and dealing with emerging security threats, such as environmental catastrophes, major techonological accidents and terrorist attacks. One salient characteristic of these new threats is their incalculability and, thus, the impossibility of deterring them on the basis of the previous Cold War doctrine of deterrence[35].

A reading of vulnerabilities in terms of risk allowed experts to embrace the elements of unpredictability and uncertainty that has served to distinguish these new from previous, traditional, security threats, anchored on the notion of "threat" as something imminent, direct and certain (DUNN CAVELTY, 2009). Equally important, the idea of vulnerability sheds light on the possibility of internal failures in society (PAULLUAULT, 2011). Thence, the argument about risks to critical infrastructures is anchored on technical developments in information technologies: as new technologies rise, so do new vulnerabilities (ANDERSON, 1996).

By portraying vulnerabilities in information technologies as risks, security experts, policy makers and private corporations[36] can offer distinct political possibilities and security measures to deal with these informational society challenges. The move has an important political implication: the appeal to the necessity of establishing partnerships between governments and private companies has been considered a logical imperative in order to deal with insecurities in digital infrastructures (ANDERSON, 1996; DUNN CAVELTY; SUTER, 2009; PCCIP, 2000). Critical infrastructures are owned, operated and supplied largely by private

[35] Early CIP debates focused on catastrophic disruptions in critical infrastructures, much like early cyber security debates focused on cyber war. Aradau (2010) criticizes that the securitizing move focuses on an all-hazards perspective to CIP follows the risk-based approach to security that is more concerned with the unpredictable and unexpected failure and ignores ordinary, everyday failures and disruption.

[36] The participation of private corporations can be both direct or quite subtle, as the case of the CSTB (1991) report. The board was then composed by distinguished members from the academy, computer scientists and representatives from private companies and think tanks, such as AT&T's Bell Laboratories and Xerox Corporation.

actors who, collectively, have more sophisticated technical resources and a better operational access to them than governments (DUNN CAVELTY, 2007).

The main political implication of the appeal to PPPs to secure the digital age – which has grown strong in the CIP debate during the 1990s – is placing a great part of the burden of "securing" it in the hands of the private sector. As Petersen (2008a) notes in her study of terrorism and insurance companies, the concept of partnership allows giving political importance to private entities by making private decisions on "how to act" a matter of national security. This process is very similar to the one inscribed in CIP and cyber security debate. Thus, the process of policy-making is also affected by the growing importance of PPPs: it is shifting from a "single-entity phenomenon to a multi-entity one, as it has become customary to involve representatives of all major stakeholders in the policy preparation process (DUNN CAVELTY, 2007:103).

3.4. Risk-based thinking and cyber security

Risk-based thinking has become almost indissociate from cyber security. The way threats are framed as "risks" has become constitutive of the *habitus* of the agents in the *champ*. Speeches, reports and documents of any kind tend to stress the risk that vulnerabilities in networks represent to the user, the corporation and the government. The same goes for the products and services being advertised against third parties, government or criminal, willing to exploit these vulnerabilities. Being connected is both a source of constant opportunities and dangers.

The task becomes one of identifying over which perception of risk the commonsense of the cyber security *champ* rests. There are several approaches to the notion, many of which explicitly carry distinct interpretations about the social function and meaning of 'risk', as well as about its relation to other ideas, such as danger or security. And the interplay between the latter and risk constitutes an important aspect of many sociological and economic risk studies (LUHMANN, 1993; PETERSEN, 2008a, 2008b, 2011).

Historically, risk and security were believed to express distinct ontologies (PETERSEN, 2008a; 2008b; 2011). Risk followed a domestic economic logic, functioning within a universe of self-governing, control and calculability. It "came to order our understanding of the possible societal futures inside the State by

describing how people lives are organized and how decisions are made (PETERSEN 2008b:407; see; LUHMANN 1993). Security, on the other side, was founded in the Westphalian political state and it has been associated with external affairs. The relationship between private persons, firms and security was one of 'protection' and security was a right to protection. This conception of security and national security gives private persons and firms a secondary role in terms of carrying out foreign policies on security (PETERSEN, 2008b).

The intersection between risk and security owes much to the rise of a common research agenda highlighted by a focus on 'new' transnational threats, that questions the possibility of calculation and the means-end rationality that were central for a previous concept of risk (PETERSEN, 2008a; 2011). Yet, the debate gained a distinct form, as risk came to refer to a wide range of everyday situations involving diverse themes and is subject to regulation by governments, companies and citizens (PETERSEN, 2011).

The diversity of conceptualizations around risk can be challenging and possibly lead to confusion. Petersen (2011), for example, identifies three approaches to risk: an economic approach, a cultural approach and a sociological approach. The first one considers risk a measurable and controllable analytical tool for capturing future threats; the second approach considers risks to be a matter of cultural perception and focuses on the institutional and social structures that shape perceptions of risk; the third approach sees risk as an ever-changing discursive construction.

It is intuitive to cast away assumptions that consider risk as a coherent perspective. As Petersen (2011) and O'Zinn (2008) suggest, risk studies compose more likely a pluralistic debate, sometimes with very few points in common between the existent perspectives. There is no consensus over whether risk is calculable or incalculable or even if it is an analytical or descriptive concept. Critical risk studies, for example, focus on the role of risk management decisions and security policies in establishing meanings of politics and political power. This approach to risk inside IR security studies understands that a risk based perspective to security offers qualitative distinctions in terms of policy prescriptions and governmental technologies, in relation to a threat-based one. Risk based interpretations are believed to emphasize more the systemic characteristics, such as

vulnerabilities, and less agency and intent between conflicting parties (ARADAU et al., 2008; ARADAU; 2010).

A guiding light in this labyrith of approaches to risk is to understand how it is conceived in face of the uncertain. Ewald's (2002) study on the philosophy of precaution is helpful in this sense, in that it highlights the tensions between the notions of risk and uncertainty in the context of a new, nameless, paradigm of security anchored on the notion of precaution. The author presents the divergences between the economic assumption of risk as a 'measurable uncertainty' and the principle of precaution by placing precaution in the category of 'nonrisk.' A nonrisk is not measurable nor assessable. It is a 'risk beyond risk' (EWALD, 2002:294). In his terms, precaution is not prevention, it is not applicable to what can be assessable; its focus is on what is uncertain.

Cyber security is in the middle of the tension between risk and uncertainty, amidst the confusion between providence, prevention and precaution. These are three, complementary, attitudes towards uncertainty. Providence is based on faith, prevention concerns reducing risks and precaution focuses on uncertainty, the uncertainty of scientific knowledge (EWALD, 2002). Exponents of critical risk studies contend, in consonance with the principle of prevention, that "risk" may indicate a specific relation to the future, one that requires monitoring it in order to calculate what it can offer in order to control and minimize its potential harmful effects or, in other words, "risk can be conceptualized as an estimation of the dangerousness of the future" (ARADAU et al., 2008:148).

Vulnerabilities in software and hardware are managed in terms of risk and, for the cyber security industry (to a certain extent), one thing is certain: it is not a matter of 'if' a device or network will be attacked anymore, but a matter of 'when.' (RAYTHEON, 2015a; MARGETTA, 2014). The appearance of certainty towards the pervasiveness of 'cyber risks' in fact conceals the unknown identity of the perpetrator and is at the heart of the 'attribution problem'[37]. The intensity of cyber-attacks creates the perception that attacks are imminent, and that such events are only a matter of time.

[37] The attribution problem refers to difficulty of finding the true identity of a cyber-attacker. For a detailed discussion on the problem of attribution, see Rid and Buchanan (2015).

But even if the language of risk seems to be predominant, the principle of precaution is part of many practices towards cyber security, particularly considering the existent concerns about the possibilities of critical infrastructure catastrophic disruption and cyber-terrorism (DUNN CAVELTY, 2009). Ewald argues that "the precautionary principle invites one to anticipate what one does not yet know, to take into account doubtful hypotheses and simple suspicions. It invites one to take the most far-fetched forecasts seriously, predictions by prophets, whether true or false." (EWALD, 2002:288). Anticipating the unknown may be as tempting as anticipating most tangible possibilities. When considering this, one can imagine all the existing predictions for cyber wars.

The set of preventive and precautionary attitutes towards the uncertain are indissociated from a preemptive posture towards security. This is an attitude towards security threats that conceives them as largely unpredictable and potentially catastrophic and acts based on conjectural knowledge: hunches, leads and suspicion. Preemptive security is not as interested in seeing the action of individuals as it is in premeditating potential dangers (DEGOEDE, 2014).

Cyber 'risks' are framed according to the uncertainty they represent. The more certain the threat, the more manageable it becomes. And vice-versa: the bigger the uncertainty, the more focused on anticipating it the practices towards it become. This complex *modus* of framing threats is particularly stronger in the market where private companies act, as risk-based thinking informs many of their practices. This is, again, the case of companies working with "active-defense", which are an object of this study. The very notion of active defense rests on the imperative of becoming resilient in face of the possibility of innumerous threats and, at the same time, using the technical knowledge available to prevent a potential attack from happening. It involves prevention on a large scale, and also precaution, in face of the remote possibility of an escalation of cyber conflicts.

Risk-based thinking is part of the background knowledge collectively shared in the cyber security *champ*. It is grounded on some fundamental assumptions of the information society thesis, particularly on the implications of the pervasiveness of networks in the current organization of society. The realization that attacks to infrastructure can have a networked effect, thanks to the code responsible for its undisrupted functioning, has led to threat characterizations of cyberspace as

ungovernable, unknowable and a source of vulnerabilities and threatening actors (BARNARD-WILLS; ASHENDEN, 2012)

Now, these characterizations indicate specific views of cyber security that are either reinforced or weakened once compared to the actual practices in the *champ*. Any endorsing or rejection of a given characterization of a cyber-threat must consider the underlying struggles over the meaning of cyber security, broadly speaking, and the practices of the actors concerned. Having considered this, the next chapter will explore the dynamics of the cyber security *champ*, identifying the agents involved and the stakes over which they struggle. It will pay a particular attention to the practices of cyber security companies and their implications.

4. (In) 'securing' cyberspace – the practice of cyber security companies and the working of the cyber security market

The present chapter will investigate the dynamics of the cyber security *champ*. The central thesis is that the main stakes involving private companies in the *champ* of cyber security orbit around their investment in a lucrative and diversified cyber security market, which has been fed by attempts from politicians, the military and security experts, to secure cyberspace. As argued in the previous chapters, the peculiar marriage between information technologies and the private sector contributed to placing cyber security in a distinct position in relation to other 'threats' to national security. The same marriage informs much of the dynamics of the *champ*, particularly the struggles between the government and the private sector.

To catch a glimpse of this relation, the chapter will be divided in two parts: the first part will situate the struggles in the cyber security *champ* in the United States, focusing on the points of agreement and disagreement between the agents concerned. The option for limiting the analysis to the U.S. has two justifications: the first one is based on the dynamic of the cyber security market in the country, which is diversified and highly problematic. In the U.S., not only have developments in ICTs been central: the country also concentrates the most intense efforts to secure and securitize cyberspace (DUNN CAVELTY, 2008). The second reason is a methodological one: expanding the analysis to other countries would require a more detailed account of the cyber security market's dynamics in each case, a requirement that, for reasons of time and resources, this research would not meet. Yet, despite focusing on a specific territorial location, the research shows that the practices of agents in this *champ* rebound beyond the U.S.

Despite initial difficulties in investigating the dynamics of the *champ* in the U.S. directly, access to classified documents highlighting them has been made possible thanks to WikiLeaks' disclosure of contracts of products and services of surveillance and cyber security services between the U.S. government and private companies.

The second part of the chapter will investigate the practices of cyber security companies – a category that includes both traditional defense companies that turned

their attention to cyber security and newer niches, composed by IT companies of varied sizes that sell cyber security solutions and surveillance technologies. Paying attention to these practices is fundamental to understanding some of the current dynamics of this market as a political consequence of the form of cyberspace securitization that has prevailed in the political and military circles in the U.S. The section also analyzes the burgeoning market of zero-day vulnerabilities and its implications for security in cyberspace.

In the analysis, the chapter identifies in the practices of cyber security companies certain tendencies that correspond to the adoption of three different (but sometimes complementary) approaches to cyber security. These approaches correspond to the features and measures that are the most valued in each selected product. They correspond to defensive security, openly offensive security and active defense. A distinction is made between openly offensive measures and active defense on the basis that the latter encompasses the former, but the contrary does not happen. In commercial cyber security, active defense involves a vast range of solutions among which offense is a silent possibility, while in the companies' relations with governments, it is a tacit option.

4.1. Struggles in the cyber security *champ* in the U.S.

As Pierre Bourdieu (1992, 2004) would note, the social world is constituted by struggles between distinct agents over certain stakes. These struggles are certainly marked by patterns of cooperation and competition aiming for a certain form of power, as is the case of the power to name some issue as something, and they are constitutive of the social *champs* that intersect with the field of power and dwell in the social world. Based on this view of the social world, this section will proceed into assessing the struggles in the *champ*. It will do so by mapping agents' position *vis-à-vis* one another, based on the amount of capital each disposes. The analysis of the existing conflicts and alliances will, in turn, provide an overview of the current stakes in the *champ*. The data-gathering process was based on the selection of official documents, advertisements, market analyses, job offerings, journalistic texts, classified documents and e-mails leaked in WikiLeaks, reports and webpages of companies offering cyber security services, defense-related government agencies and think tanks. The identification of agents was based on their involvement in the idealization, development, commercialization and

discursive justification of cyber security solutions. Each agent's position is assessed in terms of the technical and economic capital they dispose.

Cyber security is a puzzle constituted by distinct actors, among public bureaucracies, defense experts, computer experts and private companies, all of which struggle for making sense about its core elements. It is shaped by discourses and practices alike, and it often involves conflicting perceptions about the referent object being threatened. The following actors have been protagonists in struggles inside the *champ* of cyber security in the US: government's defense and intelligence agencies; the hacking community, independent IT experts; security experts working in policy-oriented think tanks, and private technology companies[38].

In the *champ*, the existence of a burgeoning market for securing computers and users (individuals, businesses and governments) is often accepted as a natural consequence of the recognition of cyberspace's inherent insecurity, to the point that the *champ* and the market juxtapose. The main dynamics of the *champ* involve, on the one hand, the commercialization of cyber security solutions, endpoint protection, consulting services, cyber risk management, and others, and, on the other hand, the construction of distinct representations of cyber threats by private companies, government agencies and think tanks, in order to gather resources to support activities that range from R&D to outsourcing and funds for policy advising.

Government agencies

If the defense and intelligence community's activities seemed to be smoldering since the end of the Cold War, the combination between 'big data', security threats and terrorism has renewed the purpose of their activities (DEIBERT, 2013), as well as added new players to the government bureaucracies' struggles. One example is the Department of Homeland Security (DHS), created in 2002, after the 11/09 terrorist attacks in the US. The DHS is formally charged with civilian security and is responsible for coordinating the efforts to protect US critical infrastructure from disruptions. Its approach to cyber security is similar to the

[38] The label embraces a wide range of sectors, from antivirus companies, to software and hardware developers, Internet service providers and online services providers.

industry and private sector perceptions, considering the vulnerability of cyberspace and its infrastructure to physical and cyber threats or hazards (DHS, 2016).

Early struggles between government's defense and intelligence agencies concern who would be in charge of cyber security initiatives (SCHNEIER, 2009), a function that today seems to be shared among the FBI, the NSA, the DoD and the DHS at different levels. These agencies enter the field provided with technical expertise on information technologies and risk management, which can come from inside employees or in the form of defense contracts with private companies, cooperation with other government agencies, partnerships with the private sector and networks with policy and risk experts working for think tanks. The size of the cyber security budget of each agency allows providing numerous jobs opportunities and investments in highly technological projects inside the agency or in private contractors and is determinant in setting their position vis-à-vis one another and in relation to other agents in the *champ*. Despite limitations in workforce and efficiency, the amount of economic and political capital they dispose makes these agencies powerful actors struggling in the field.

Table 1: Approximate discretionary Budget of U.S. government security and intelligence agencies in charge of cyber security - Fiscal Year 2015 (in U.S. dollars).

	DoD	**DHS**	**FBI**	**NSA**[39]
FY 2015 (enacted or projected)	$496.1 billion	$49.1 billion	$8.4 billion	*Classified*
Budget for CIP, cyber/IT security programs (enacted or projected)	$5.5 billion	$680.8 million	$1.5 billion	*Classified*

Sources: Fiscal Year 2016 Budget of the U.S. government
FBI's FY 2016 Authorization and Budget Request to Congress
Homeland Security Budget-in-Brief 2016.

Table 2: Job opportunities in U.S. government security and intelligence agencies in charge of cyber security (February 2016).

	DoD	**DHS**	**FBI**	**NSA**
"cyber" jobs[40]	67	20	19	26

Source: USAJobs.gov and intelligencecareers.gov

[39] NSA's budget is part of the intelligence budget of the U.S. government. According to Shorrock (2008), in 2007, about 70% of this budget went to outsourced activities. The 'black budget', as it is also known, is classified, but documents leaked by Edward Snowden showed that the agency was in line to receive $10.5 billion in 2013.

[40] According to the DHS, "cyber" or cyber security jobs tend to deal with the following tasks: cyber incident response, cyber risk and strategic analysis, vulnerability detection and assessment, intelligence and investigation, networks and systems engineering, digital forensics and forensics analysis and software assurance. It can also involve intelligence gathering and SIGINT.

Contestations often come in the form of questioning an agency's capacity to handle cyber security initiatives and have resulted in the strengthening of alliances between some governmental agencies. The DHS, for example, has been criticized for being too bureaucratic and technically incompetent by industry and security experts. The critique, in turn, led the department to adopt a strategy of allying with other agencies, such as the Departments of Commerce, Defense, Justice and State, in order to provide a coherent cyber defense policy and to develop international standards (GARCIA et al., 2014).

The agencies also adopt competing understandings and practices of cyber security. Operating at the level of defense, the DoD[41] considers that disruptions from third parties, state-owned and private, and cyber theft of intellectual property to undercut US technological and military advantage constitute core cyber security threats to the security of national networks, systems and information (DOD, 2016). The most polemical – and secretive – agency in the government bureaucratic milieu, the NSA, does little to define cyber security, but invokes the importance of increasing vigilance and resources to thwart cyber risks (ROGERS, 2015). The agency has built a huge and complex system of mass surveillance, which dimensions came to the public due to leaks by Edward Snowden. The NSA's known practices involve using hacking and mass surveillance to provide intelligence to the federal government.

The NSA's practices find some resistance in segments of the private sector, of the Department of Justice and the FBI, particularly regarding its surveillance program and the possibility of being charged of cyber security (SCHNEIER, 2009). The agency recently announced a reorganization that will consolidate its spying and domestic cyber security operations, thus unifying espionage and cyber defense capabilities for the US government (VOLZ, 2016).

Despite resisting the idea of concentrating cyber security in the hands of the NSA, the FBI has cooperated with the agency in data gathering for intelligence purposes and it has, itself, focused on intelligence attributions concurrently with its traditional law enforcement duties (BARRET, 2015; ACKERMAN, 2015; DEIBERT, 2013). This stronger orientation towards intelligence activities, also

[41] The DoD operates at the external defense level. It's "cyber" mission, to use the department's own terminology, concerns the defense of networks, systems and information against cyber-attacks and the provision of "cyber" support to military operational and contingency plans (DOD, 2016).

anchored in the FBI's interests in cyber security for law enforcement against cyber-crime, has placed the agency on the forefront of some core information age security debates. The encryption debate is perhaps the most known of them[42] and, in addition to placing the FBI against some powerful technology corporations[43], it highlights the distinct approaches to encryption inside the government apparatus[44], opposing the FBI's and the NSA's public position over the matter (MCLAUGHLIN, 2016).

Yet, in face of the leaked documents provided by Edward Snowden, NSA's strategy does not necessarily need to be read as a pro-privacy discourse. As the former NSA director Michael Hayden signaled, US intelligence agencies know how to gather information without weakening encryption. He also left unsaid that hacking allows both agencies to circumvent encryption to get content as well (MCLAUGHLIN, 2016; HACKETT, 2016).

Table 3: Main points of agreement and disagreement between U.S. government security and intelligence agencies.

Issue	DoD	DHS	FBI	NSA
Position regarding the distribution of cyber security initiatives	Coordinates cyber activities with other agencies	Wary of the power of NSA. The responsibility is to be shared between the government and private companies	Against concentrating it in the hands of the NSA; cyber security as a shared responsibility of government and private actors	Struggles to expand its powers and unify cyber defense and intelligence initiatives
Definition of cyber security	Focused on threats posed by third parties and on the theft of intellectual property considered vital to the U.S. national interests	Emphasizes the vulnerability of cyberspace and critical infrastructure to risks	Emphasizes cyber-crime and law enforcement; in practice, develops intelligence activities and concentrates on high level intrusions	Cyber security as a part of its Information Assurance mission and of network warfare, but is not defined
Encryption	-	Encryption is making it harder for the government to	Companies need to create backdoors in order for law	Argues for the importance of encryption. In practice, the

[42] Encryption is a military technology that went public and allows that communications be shielded from third-parties' access, including government's. The debate involves limiting general encryption for the sake of law enforcement and national security measures.

[43] Recently, the FBI started pressuring companies to change their business model and not offer true end-to-end encryption to customers (THIELMAN, 2015; MCLAUGHLIN, 2016).

[44] There is an apparent disagreement between the positions of the NSA and the FBI over the encryption debate, with the FBI director James Comey urging for law enforcement to have access to encrypted data, and Mike Rogers from the NSA stating that "encryption is foundational to the future" (MCLAUGHLIN, 2016).

		find criminal and terrorist activities.	enforcement agencies to have access to encrypted data	agency uses mechanisms to break encrypted communications
Strategies and attributions	Holds both defensive and offensive capabilities and is responsible for defending the U.S. against cyberattacks	Works with the private sector in cyber threat response and mitigation; is responsible for securing federal .gov world and critical infrastructure	Argues for prevention rather than only reaction to attacks	Is trying to merge defensive (Information Assurance Directorate) and offensive (Signal Intelligence Directorate) cyber security missions

In practice, cyber-crime and cyber-terrorism are portrayed as the great antagonists of government agencies and private actors (DUNN CAVELTY, 2016; DOD, 2016; FBI, 2016; DHS, 2016). These comprise a wide range of unlawful and illegal activities online and practices dependent on a certain degree of knowledge of coding, like sabotage and espionage. For example, the FBI definition of 'high technology crimes' englobes cyber terrorism, espionage, computer intrusion and fraud. But cyber-crime is complex in that it is far from being a disruptive act perpetrated by an individual with enough expertise in computers: black markets[45] have become a profitable venue for sophisticated, highly organized and financially driven groups (ABLON et al., 2014). Governments and private actors tend to describe hacking activities as either terrorist or criminal, in which the intent of the 'malicious hacker' is to exploit, disrupt and/or steal information (BETZ; STEVENS, 2011; DUNN CAVELTY; JAEGER, 2015; FRIEDMAN; BOUCHARD, 2015; FBI, 2016).

The hacking community

The hacking community is neither a homogeneous body of agents working towards an end nor the 'bad guys' out there in the Internet. As Betz and Stevens (2011) note, various typologies coexist. Hackers can be non-malicious or malicious, depending on their goal (testing a system security, hacking for profit or breaking into it for some other purpose). In the latter category fall cyber criminals, known for using diverse and quite innovative techniques for stealing. They can be

[45] Many authors use the term black or dark market to refer to unlawful, criminal activities commercialized through the Internet. (see DEIBERT, 2013; FIDLER, 2014; ABLON et al., 2014).

individuals working for their own sake or sophisticated organizations targeting specific institutions for purposes of espionage, intellectual property theft, immediate financial gain and so forth (BETZ; STEVENS, 2011). Hacktivism, as is the case of Anonymous and Lulzsec, differs substantially from profit hacking in that it is carried out of some political, religious, environmental or personal conviction (IDEM, 2011). Hacktivists tend to use their knowledge of code to target government and global institutions' websites (NYE, 2014).

Hence, hackers are fundamental players in the cyber security *champ*, but they are far from being a uniform group. Some of them are profit oriented and dispose of some degree of institutional organization and economic capital, as is the case of the Hidden Linx group (DOHERTY *et al.*, 2013), while others work in disperse networks around the world, with little economic capital or institutionalization and use hacking as a strategy to give visibility to certain political claims (NYE, 2014). Their position varies in terms of the impact of their actions to other agents' strategies and they exert considerable influence in authoritative definitions of cyber security.

Independent IT experts

IT experts have a similar knowledge of code and computers as hackers do, and they can be compared to non-malicious hackers in most of their activities. They are different in that they usually make a living of this knowledge, composing the 'cyber security workforce' in private companies, think tanks and the government. But these actors can transit among autonomous, lawful work and the black market, sometimes overlapping with the figure of the malicious hacker. In the current cyber threat scenario, this group can be really valuable: demand for IT professionals has been rising for some time, both in the government and in the private sector, as a response to the diffusion of computers and connectivity, the slow advance in secure software and the perception of insecurity arising from it and from awareness of hacking activities (LIBICKI et al., 2014). Individuals with expertise in IT can work independently or as part of a public/private organization, identifying vulnerabilities and advanced persistent threats (APTs) and either reporting them to the company

that develops the software or commercializing them in the gray market[46] or in the black market (FIDLER, 2014; DOHERTY et.al., 2013).

As hackers, the core capital these agents possess is (a deep) knowledge of coding. Knowledge of market dynamics can be equally important – all the more if the professional works independently (FIDLER, 2014). Because of this valuable 'asset', cyber security professionals often find themselves in the middle of struggles between government agencies and private companies for specialized workforce (LIBICKI et al., 2014). Their knowledge of computer technology is, thus, an important capital for these actors and each sector offers different incentives to attract IT experts: the private market usually offers high salaries and flexible benefits to attract professionals, but in turn grants less stability; the public market has less flexible wages and benefits. Yet, as Libicki et al. (2014) argue, a government employee has the privilege of carrying out certain operations that would be considered illegal if done by anyone else.

Because of the difficulties in hiring 'upper tier'[47] cyber security professionals, some agencies (e.g. the NSA) would rather 'make' than 'buy' professionals (by "making" the work refers to investing in qualification after the recruitment). Further, a recent strategy of the US government to deal with the problem of recruiting skilled individuals has been to outsource the work to private contractors. What happens to the provision of security is also applicable to the recruitment of security professionals: as governments are unable to adequately provide it by themselves, recruitment policies are predicated on the concept of sharing responsibility with private actors (DUNN CAVELTY, 2009b).

Security experts in policy-oriented think tanks

On a distinct spectrum of the map lie policy-oriented think tanks that have turned considerable attention to cyber security in the past years. The Global Commission on Internet Governance, supported by public and private actors, is an initiative launched by the Centre for International Governance Innovation (CIGI)

[46] The gray market for vulnerabilities describes interactions, conducted as legal businesses deals, between sellers and government agencies and sales between sellers and legal users of zero-day vulnerabilities, as is the case of cybersecurity firms (FIDLER, 2014)

[47] For Libicki et al. (2014), upper tier professionals are those few percent in the cybersecurity profession capable of commanding salaries of $200,000–$250,000 a year or more.

and Chatham House with a focus on articulating and advancing a strategic vision for internet governance. Think tanks' activities show the growing importance of the subject for policy-making. All the six most influential think tanks in the US[48] have policy topics and experts working with cyber security policy-making and publications have increased considerably since 2010[49]. Among them, the RAND Corporation has begun to address information security still in the 1980s, having entered the 'cyber' realm in the 1990s, with the well-known publication by Arquilla and Ronfeldt (1993) named "Cyber war is coming!".

Think tanks' involvement in cyber security comes as either a reaction to perceived vulnerabilities in computer security, as it was the case of the RAND Corporation's early involvement with the topic (see WARE, 1966; 1967a; 1967b), or to the increasing prominence that cyber security acquired in policy-making process (GARCIA et al., 2014; DUNN CAVELTY, 2016). Policy-oriented think tanks tend to produce perceptions about cyber threats and risks and revenues can influence the content-production in most cases. Recurrent sources of income for major think tanks include self-generated revenue, e.g., charging conferences and membership fees and selling their own books and periodicals, donations from foundations, individuals and corporations, and government grants and contracts.[50] Donations diverge in their symbolic effects: money from specific sectors of an industry often comes with a specific purpose, whilst donations from foundations can focus on broader stakes. In the case of cyber security, this may result in policy prescriptions focused on thinking about how government actions affect the private

[48] The top 6 most influential think tanks in the US are: Brookings Institution, The Carnegie Endowment for International Peace, the Center for Strategic International Studies (CSIS), the Council on Foreign Relations, the Wilson Center and the RAND Corporation. The classification is based on James G. McGann's 2014 Global Go To Think Tank Report. Available at: <http://repository.upenn.edu/cgi/viewcontent.cgi?article=1008&context=think_tanks>.

[49] A quick search in each website reveals this growth: Brookings started publishing about cyber security in 2010 and today has about 283 publications, among events, reports, commentaries, expert opinions and books. The RAND Corporation has about 164 publications only under the topic of cyber security, and much more under the topics of cyber warfare and information security. The CSIS has offered the biggest search results, totalizing 324 publications under the topic technology and cyber security. Both the RAND Corporation and the CSIS have offered diversified accounts of cyber-issues, addressing cybercrime, risk, cyberwarfare, surveillance and a broad range of topics concerning the impacts of ICTs on security. The Wilson Center and the Carnegie Endowment for International Peace are those with the more modest search results: they account for about 40 and 49 publications on the topic of cyber security, respectively.

[50] Think tanks often depend on three kinds of clients: political clients, e.g., policy-makers, parties and activist networks; economic clients, e.g., foundations, corporations and wealthy donors; and media clients, e.g., journalists, newspapers, periodicals, radio and television programs. In most cases, economic clients tend to be the main source of financial support (see MEDVETZ, 2012).

sector instead of considering the broader landscape. Partnerships with governments, in turn, can grant think tanks both political access and robust funding, but they are not always desirable, once there is a risk of undermining the perception of the institution as 'independent' (MEDVETZ, 2012).

The attention directed at cyber security is influenced by both think tanks' relations with economic and political actors and struggles for publicity and funding. The kind of relationship each think tank has with its sponsor and the professional background of its experts also influences the focus of its publications, as it is the case of RAND's attention to cyber war and cyber threats[51] and of CSIS' debates on CIP, governance and surveillance.[52] Think tanks are particularly influential in providing competing definitions for cyber security and cyber threats/risks, sometimes in alignment with governmental definitions and sometimes contesting them (DUNN CAVELTY, 2013). CSIS often publishes direct recommendations for policy-makers[53] and tends to focus on the importance of defending against intrusions from hostile countries, exploitation from cyber-crime and strengthening public-private partnerships (CSIS, 2008; 2010; ZHENG; LEWIS, 2015; ZHENG, 2015).

The private sector: private companies

The private sector's[54] cyber security landscape is complex and diverse. It involves the interests of banks, telecommunication companies, healthcare organizations, the energy sector, large and small technology companies and defense contractors. Private companies are responsible for the ownership and operation of physical and digital infrastructures, and thus, central actors in the CIP and in the Internet debate. The technology sector has backed much of the development in ICTs and in technology standards in the past decades. Companies within the sector range

[51] It should be noted that most of RAND's resources come from the DoD.
[52] Most of CSIS experts have career background in politics and are familiar with governance debates.
[53] One example is the 2010 report 'Cybersecurity: two years later' that makes an assessment of the implementation, by the federal government, of the recommendations formulated in the 2008 'Securing cyberspace for the 44th presidency'. Its evaluation is that difficulties in implementation of recommendations reveals internal political disputes over the importance of cyber security and the role of federal government in its implementation.
[54] By definition, the term 'private sector' encompasses pro-profit sectors of society that are not controlled by the state. In this work, the term is employed as a synonym of private companies.

from hardware and software developers, internet service providers (ISPs), online service providers (OSPs), the antivirus industry and cyber security companies.

The growing importance of these actors is also linked to the political implications of their commercial and corporate practices (DENARDIS, 2014). Corporations' policies for the usage of products and services and determinations over whether to interrupt hosting services are constitutive of the political power of private corporations. Individual privacy online, including policies of data collection for advertising purposes, is usually defined and delimited by social media end user agreements (DEIBERT, 2013; DENARDIS, 2014). Private actors respond to political events as much as they carry their core commercial functions[55], sometimes without the direct constraints faced by democratic governments. Hence, "where governments could be, and are, constrained by constitutional protections of free press and free speech, private industry is not necessarily subject to these same confinements" (DENARDIS, 2014:12).

Since the Internet infrastructure and operation is mostly a responsibility of the private sector, governments need its compliance to carry out their attempts to 'secure' cyberspace. Deibert (2013) calls this phenomenon a "downloading" of policing responsibilities. In practice, functions like monitoring users' activities online, filtering access and controlling content/information are delegated to private companies that run and operate the Internet. And when these actors are entrusted with powers and responsibility to police the Internet, issues of transparency and accountability arise (DEIBERT, 2013; DENARDIS, 2014). The risk is that, by granting lawful access responsibilities to the private sector, a market for the commercial exploitation of data is created. As Deibert argues, "as companies are forced to surveil/police their networks and data, products and services are emerging that enable them to do so more effectively and efficiently" (DEIBERT, 2013:223).

Public-private relations are filled with struggles between security agencies and private actors (DEIBERT, 2013; HERN, 2015). These struggles sometimes generate patterns of cooperation, as is the case of Google's cooperation with the NSA after reported attacks on its networks (NAKASHIMA, 2010; DEIBERT,

[55] DeNardis (2014) gives an account of that political power in the case of Wikileaks. She argues that the decision by the company hosting the website to cut off services to Wikileaks was a response to the release of sensitive diplomatic correspondence data. Similar attitudes by Amazon were taken because of "violations to its terms of service".

2013; HARRIS, 2014) or the case of AT&T's alleged participation in a NSA's wiretapping program (DEIBERT, 2013; HARRIS, 2014). But in most cases, there are conflicting interests. One example is how the US government and technology companies have struggled over the issue of encryption. The FBI took the lead, criticizing Apple Inc.'s 'ubiquitous' encryption because it supposedly brings more insecurity to the country by making it harder to catch terrorists and other criminals (HERN, 2015). Companies like Google, Facebook, Microsoft and IBM also conflicted with the NSA after the disclosure of their alleged participation in programs of data collection. The core of the conflict revolved around the possible, previous awareness these companies had of the NSA's program (ACKERMAN, 2014; REITMAN, 2014; GALLAGHER; GREENWALD, 2014). At stake were the economic consequences of an eventual cooperation with the agency's practices.

Neither of these companies, however, focuses on the commercialization of cyber security solutions or term their products and services so. It was the conflict or cooperation among themselves (and between them and government agencies) that generated concerns that were close to cyber security. Therefore, a particular group of private actors deserves scrutiny: companies that work or have oriented themselves to the cyber security market, or 'cyber security companies'. The denomination is broad and it does not intend to describe the wide range of products and services these actors may offer, nor does it give a clue about the possible relations these companies can develop with and within governments. But it signals a common ground between this group of companies, which is their focus on a market of cyber security service and solutions. Within this group, the work identified companies commercializing antivirus services and companies commercializing sets of services understood as 'cyber security solutions' for private companies and governments.

According to the Cybersecurity Ventures research and market intelligence's report (2015), the market for cyber security was estimated in about US$ 75 billion in 2015 and is expected to grow to US$170 billion by 2020. This burgeoning market has commercial and federal clients as main consumers: the antivirus industry plus hundreds of companies working with consulting and operational support, incident analysis and response, risk management, APTs, cloud and IoT security, security data, intelligence and big data analytics/security have oriented themselves to commercial demands from industry and other companies. Some of them also

commercialize with governments, although they do not work exclusively in the role of defense contractors, as is the case of Symantec. The defense and intelligence sectors are the largest contributors to cybersecurity solutions, as the report states.

Several regions around the world have expanded markets for cyber security as a direct response to rising cyber espionage and other information age security concerns (MORGAN, 2015; DUNN CAVELTY, 2009a; DEIBERT, 2013). This, in turn, has generated requirements for IT professionals, feeding the demand for a 'cyber security workforce' in both the private and the public sectors. It is the market fed by government agencies the main responsible for this expansion, particularly in the US. A report by Market Research Media suggests that "the annual cyber security spending of the US Federal government is bigger than any national cyber security market (…), exceeding at least twofold the largest cybersecurity spending countries" (MARKET RESEARCH MEDIA, 2015). Over the past decade, the US federal government has spent $100 billion on cyber security and $14 billion more have been budgeted for 2016. The DHS alone spent more than 3% of its 2014 budget on cyber security and budgeted about US$582 million just for its EINSTEIN intrusion detection system.

In face of the competitive atmosphere and the market prospects for information technology security, partnerships between public and private sectors become strategic. And once again, government funding fuels a parcel of this market. An interesting movement of the DHS was to announce the opening of an office in the Silicon Valley, in order to "improve relations between tech companies and the government, spread the government's ideology on cybersecurity throughout the tech industry, and recruit top talent that might otherwise head to the private sector" (MORGAN, 2015). Similarly, the DoD announced it would provide venture capital funding to Silicon Valley's startups to help the Pentagon in developing advanced cybersecurity and intelligence systems (CAMERON, 2015).

Struggling with cyber security companies for the federal market of cyber security are also some of the traditional contractors and giants from the defense sector. Defense contractors in the cyber security market focus on the federal government as a client, although attempts of expanding to the commercial market experiences exist (MORGAN, 2015). These actors' re-orientation from traditional defense activities to cyber security can be read as a strategy to capture a parcel of the crescent budget directed at the sector (BRITO; WATKINS, 2011). Through its

products, solutions and categorizations, these actors work to endorse or dismiss the versions of cyber security[56] proposed by the distinct governmental spheres, and enter in direct competition with information technology firms for government contracts.

In sum, the cyber security *champ* is constituted by the hacking community and independent cyber security experts, security and policy experts working through think tanks, governmental bureaucracies and private companies. The latter split into distinct categories that range from non-ICT related industry to ISPs and social media networks. Whilst conflicts between these categories and governments touch cyber security tangentially, the group of private companies commercializing cyber security solutions offers a more comprehensive view of the dynamics of marketized security. Agents in the *champ* dispose of distinct arrangements of capital: experts working in think tanks have their reputation and personal connections; independent professionals have their knowledge of code; private companies often benefit from economic capital and quality workforce and, on the other side of the spectrum, government bureaucracies hold a significant amount of symbolic capital and a bigger power to 'name' risks to cyber security. Particularly in the latter case, the power of naming comes accompanied by generous funding to private contractors.

Most of these actors struggle for economic resources, and federal spending has been particularly desirable for private firms, governments and politicians alike. In turn, the issue of definition becomes particularly relevant, as certain conceptions of cyber security may prevail over others and justify resource allocation to specific sectors, such as national security agencies or the military. As Brito and Watkins (2011) note, the inflation of cyber threat benefits not only calls for increased regulation, but also the government spending on the cyber security industry.

If, because of their prominence in the development, ownership and operation of computer and networked technologies, private companies are believed to have a role of greater importance in securing cyberspace, it is necessary to inquire about the implications of the activities of those companies commercializing security in cyberspace for security in cyberspace itself. Underlying this questioning is an

[56] See Eriksson and Giacomello (2007) on the distinct threat images constituted by distinct spheres of the government.

attempt to investigate further both the practices of these companies and the relations they establish to strengthen their position in the cyber security *champ.* In the attempt to answer to market tendencies and securing pressures, these companies also play an important role in defining understandings of cyber security through their practices and these practices can, perhaps unwillingly, have undesired effects for cyberspace security. The next section will delve further in the dynamics of the cyber security market by investigating the practices of some of these cyber security companies.

4.2. The dynamics of the cyber security market and the practices of private companies

From user agreement policies to software and services seeking to enhance the security of the Internet user, the practices of private companies within the universe of cyber security are pivotal for shaping perceptions of security and insecurity in cyberspace. Economic assumptions, which play a fundamental role in defining the nature of the service to be offered, are part of the logic of these practices, but they alone cannot explain the technical and market choices made by most of these companies. Risk-oriented thinking is part of the collective *habitus* in this *champ*, and also a fundamental factor in the development of cyber security solutions and on corporate decision-making. This can be observed in advertisements, threat and risk assessment reports, fact-sheets and other documents sponsored and published by companies in this segment, as well as what is made available in their websites.

The adoption of certain technical standards complements the background knowledge that informs the practices of these companies. This requires that companies have a specialized workforce with sufficient knowledge of code. Network security and resilience requirements are the most important technical standards for a company working with sensitive data and businesses. They are emphasized by public authorities and also are mandatory for companies contracting out with the government.

The cyber security market is populated by companies advertising for the most distinct products and solutions focused on enhancing security in cyberspace, as in the case of antivirus companies; on identifying and preventing cyber-attacks; and on helping governments and corporations in the task of securing their networks and deterring cyber-threats, as some specialized start-ups and bigger companies do –

and in the case of governments, some products and services can be quite useful for countering intrusions.

In order to understand the dynamics of the cyber security market, the work will investigate the practices of the group of companies advertising for cyber security solutions. Strictly, cyber security companies, independent of the size, advertise and commercialize products and services that offer a certain degree of protection against malicious software, cyber intrusions and cyber-attacks to the customer. In some cases, services can also include risk assessment. But there are so many possibilities other than 'defense' in the market for cyber security that other services, not directly suited to provide protection to the customer or the machine, can be found under the label 'cyber security solutions'. One example is the companies that commercialize zero-day vulnerabilities with governments. Another example is the commercialization of overtly 'offensive' cyber security solutions, which can be quite troublesome, particularly in face of the alliance between the private sector and intelligence agencies.

The work also pays attention to the 'solutions,' the products and services that the selected companies advertise in their websites and commercialize with government and commercial customers. It analyzes the nature of the security measures proposed in each case. The selection of the products and/or services was not exhaustive, as there is a variety of solutions out there in the market. Instead, the data collected was delimited to the products and services in which the target audience is comprised of governments and other companies; to the 'main' products and services within the companies' portfolio; and specifically, in the case of products, to those offering the most complex set features, instead of those offering the most basic ones (for example, the option was to analyze the 'pro,' 'advanced' and 'enterprise' solutions, instead of the 'free,' 'small business' ones). When it was possible, the selected solutions were combined with the main security strategy adopted by the company (for example, Endgame's "adaptive defense" approach).

Didactically, these companies are separated in three categories: antivirus (or endpoint security companies), IT companies advertising for cyber security solutions (with a special focus on those in the zero-day market), and traditional defense

contractors that had oriented themselves to cyber security[57]. This division suggests that, although said companies are all together in the cyber security business, competing for a part of the market, cyber security solutions are not the same, nor are companies' strategies to address them. In some cases, the partnership between companies and their clients can offer fruitful means of protection for individual users, but there are cases in which this alliance can result in violations of privacy and in the increasing of insecurity in cyberspace.

4.2.1. Antivirus companies

Among the private companies commercializing cyber security services, antivirus companies are perhaps those that seem to be closer to the individual computer user. The advent of antivirus technology dates back to the 1980s, but it became widespread with the development of connectivity and the diffusion of malicious software, such as viruses, through networked computers. Most antivirus companies made their name developing software for preventing, detecting and removing malicious software from the user's machine. Research and discovery of new 'threats' has been fundamental for this end and a complementary work by these actors (see KASPERSKY, 2016).

The work has scrutinized market strategies of some of the largest and most well-rated antivirus companies: Avast Antivirus, Kaspersky Labs, Symantec, McAfee, Bitdefender and Avira. These agents work with distinct strategies to consolidate, maintain or increase their position in the market. The acquisition of start-ups, a common strategy among companies working in the IT sector, allows them to have access to new technologies and to the qualified engineers working for start-ups. In 2014, Avast Antivirus has, for example, acquired the start-up Inmite, specialized in mobile technology. This move can be read as a response to market tendencies associated with the expansion of mobile technology and its adoption by millions of users (and, additionally, good acquisitions bring the attention of investors). These deals have cost millions of dollars, as the 2007 acquisition of the

[57] Although traditional defense contractors are placed in a category of their own, it should be noted that some antivirus and IT companies regularly contract out with (or at least sell products to) the U.S. government, as is the case of Symantec and Endgame.

data leakage prevention company VONTU by Symantec indicates (the deal cost around US$350 million).

Most companies opt for 'untangling' their products in different categories of protection, such as antivirus protection, internet protection and protection against (or removal of) ransomware, just to give a few examples (see BITDEFENDER, 2016; AVIRA, 2016). All the companies studied in the present work distinguish between threats to the home user and to businesses (small and large), offering distinct, more complex and diversified services to the latter, such as threat analysis and consulting. Companies like Kaspersky Antivirus and Symantec also provide publicly available and insightful threat analyses and reports on cyber security. Kaspersky labs has made long term predictions about the evolution of APT attacks and the 'balkanization' of the Internet[58], and also provided an overview of cyber security in 2015, describing it as "full of cyber-criminals that are proving hard to catch and cyber-espionage actors that are even harder to attribute" (KASPERSKY, 2016).

Symantec openly works with the U.S. government civilian and defense agencies. The company hosts an annual government symposium that works as a bridge between federal cyber security standards and requirements and the technology offered by the private sector. According to the company's website, "we've combined our proven private-sector technology with federally focused investments in R&D, and our people are well-versed in Federal standards and requirements. We understand the issues you face because we've examined them, and addressed them, for years." (SYMANTEC, 2016)

One important aspect of this niche is that the changing dynamic of cyber-threats forced the antivirus sector as a whole to reinvent itself and led some industry businessmen to declare the 'death' of the antivirus industry (YADRON, 2014; MCAFEE, 2015). The reality behind these exaggerated claims is, however, closer to an "antivirus is dead! Long live antivirus!" logic than to failures in businesses models. The word 'reinvention' assesses the way in which companies started commercializing solutions for dealing with the operation of malware, identity theft,

[58] The Balkanization of the Internet is a process where the Internet is 'divided by countries.' The risk is that the availability of Internet could be controlled by attacks on the service junctures that provide access across different boundaries (See KASPERSKY, 2016).

ransomware and vulnerability exploitation. Discourse goes as follows: protecting against intrusions in a computer is still a part of every product, but this alone is no longer enough. New strategies and solutions are required to deal with the always present risks of being connected: risks to intellectual property, to the safety of user information and to the operation of 'critical' sectors.

The declaration of the 'death' of the antivirus in practice is likely a market strategy for some companies to announce new products and services oriented at tackling risks other than computer viruses and worms. The conflict of terminology that distinguishes companies insisting on the relevance of the term 'antivirus' (SALMI, 2014; AVIRA, 2016; BITDEFENDER, 2016) from companies using the term 'endpoint protection' to describe the wide range of cyber security solutions for home users and corporate clients distinctly (SYMANTEC, 2016; KASPERSKY, 2016; MCAFEE, 2016) seems apparent. McDonald (2012), argues that this terminological struggle is misplaced, for "AV hasn't been AV for years". This market, which he terms "Modern Endpoint Protection Platforms" includes a variety of protection models: signature and non-signature based, corporate, home user or government focused (MCDONALD, 2012; see KASSNER, 2012). Most of these companies have added cyber risk management to the portfolio.[59]

Contemporary endpoint protection, or its less fashionable cousin "antivirus protection," are both anchored on a specific approach to cyber security, which focuses on defensive security. Defensive security focuses on the protection of informational devices, networks and *online* activities from possible cyber-threats, and is often characterized by its responsive nature, that is to say, the response comes after the threat is discovered (ROSEQUINST, 2013). It focuses on the system's environment and on hardening the endpoint's infrastructure against cyber-threats in such a way that the risk of intrusions is minimal.

Table 4: Antivirus companies' dominant approaches to security.

Company	Defensive	Offensive	Active defense
Avira	Avira Antivirus for Small Businesses	-	-
	Avira Antivirus Server		

[59] Symantec's DeepSight Managed Adversary and Threat Intelligence (MATI).

Avast	Endpoint Protection Suite Plus	-	-
	Avast Premier		
Bitdefender	Bitdefender total security 2016	-	-
	Bitdefender GravityZone Enterprise Security		
Kaspersky Labs	Kaspersky Total Security for Businesses	-	Kaspersky Anti-Targeted Attack
Mcafee	Endpoint protection products line	-	-
Symantec	Symantec Advanced Threat Protection	-	DeepSight Intelligence
	Endpoint Protection		
	IT Management Suite		

The table above shows some of the main products and services advertised in the studied companies' websites. These products were selected considering their target audience (businesses and governments, mainly), complexity and the fact that they are paid, instead of being for free. For strategic reasons, free solutions are often simpler and have a less sophisticated technology compared to the paid ones. Endpoint protection tends to include antivirus and firewalls in the same product. The products on the first column have as their main focus the detection and reaction to an unauthorized access within the system. They are characterized for having a defensive approach to cyber security, also termed 'passive defense'.

Although complex, the focus of this group of solutions is on detecting advanced threats and malware, fighting them off and securing data and *online* activities, such as shopping and e-mailing. Some include behavioral monitoring,[60] vulnerability protection and basic risk management platforms. The defensive approach includes what Dewar (2014) terms fortified and resilient cyber defense. Fortified defense includes measures such as installing antivirus software, firewalls

[60] Behavioral monitoring is an intrusion detection model that assumes that it is possible to detect an intrusion by observing deviations from the expected behavior of the user or system.

and other kinds of detection technologies. The main goal is to reduce the chances of an unauthorized access. Resilient cyber defense, in turn, involves ensuring the uninterrupted functioning of critical infrastructures and services that depend on networked communications. According to the author, "Resilience itself is predicated upon accepting that incidents will occur and focusing on the ability to recover from those incidents, either returning to the original state or adapting to generate a new, adjusted state" (DEWAR, 2014:16).

Two exceptions to the tendency to adopt more defensive solutions are presented by Symantec's *DeepSight Intelligence* and by Kaspersky's *Anti-Targeted Attack*, two services aiming at anticipating and mitigating cyber security risks. Focused on corporate clients, they advertise services oriented at keeping the customer's teams informed of vulnerabilities, providing advanced analysis of attacks and, in the case of *DeepSight Intelligence*, sharing the motivations and techniques of 'threat actors,' in order to improve decision-making and allow the implementation of 'proactive controls' before the attack occurs (see SYMANTEC, 2016). These services are provided by specialized teams, which are also capable of assessing and testing the customers' response program for security risks.

Symantec's *DeepSight* solution and Kaspersky *Anti-Targeted Attack* are labeled as active defense because of their strong investigative purpose. These two cases may indicate that at least a parcel of the antivirus/endpoint industry is slowly adopting a more open risk prevention and mitigation approach. The term 'active-defense' will be better discussed in the subsection 4.2.3., in this chapter, in face of the popularity of such measures in the universe of defense contractors. It is important to note, however, that active defense is distinguished from pure defense in that its focus is to guarantee security by going beyond the endpoint environment. It does not suffice to maintain the confidentiality, integrity and availability of the system or the network in the most cost effective and unobtrusive manner. Defending is crucial, but it is also necessary to investigate (and sometimes punish) the attacker.

The 'endpoint protection' terminology concurs with the main discursive strategies employed by security and defense circles to secure cyberspace, which tend to emphasize the risk of third party exploitation of systems vulnerabilities and the consequent possibility of loss, theft and/or disruption of (critical) information (see ANDERSON, 1996; and ANDERSON et al., 1999, for example). To counter these risks, a parcel of the antivirus industry is slowly turning its attention to

services oriented at identifying, understanding and/or mitigating risks in order not only to stop cyber-attacks as they happen, but also to prevent their emergency. But as this 'preemptive' approach becomes more and more popular within cyber security circles, it feeds the expansion of the cyber security market beyond the defense-oriented antivirus industry, with new companies being created and traditional defense companies orientating themselves to answer to this burgeoning market (DEIBERT, 2013; HARRIS, 2014).

4.2.2. IT companies

Some companies have diversified their products to offer cyber security solutions that go beyond endpoint security. Companies such as FireEye (and its subsidiary Mandiant) combine a set of strategies, from using the expertise engineers, computer analysts and researchers in order to develop real-time threat intelligence to prevent, monitor and respond to intrusions, to offering consulting services and risk analysis to clients (WOODS, 2014). These companies are not focused exclusively on 'defensive' cyber security (nor do they openly advertise for offensive solutions). Instead, they propose "adaptive" and active defense solutions (FIREEYE, 2016).

The cyber security company Mandiant became known in 2006, after the publication of the APT1 espionage report, where it presented documented evidence of cyber-attacks targeting the U.S. and other English-speaking countries' organizations perpetrated by the People's Liberation Army. The company is part of a group of private actors that focused on building its own sources and methods of intelligence collection and analysis and it was acquired by FireEye, another cyber security firm, in January 2014 for the sum of US$1 billion.

Mandiant's release of the APT1 report was a successful marketing move. The issue of Chinese espionage was known to government authorities, but very little diffused outside the government circles. The report not only made the company an authority on the subject, it also generated huge interest from the media and other sectors of society and raised the fear of APTs

But, as Harris (2014) notes, whereas Mandiant's business focused on investigating cyber intrusions, FireEye's aimed to prevent them. And with Mandiant as its subsidiary, FireEye could now both rely on its good reputation and

offer a more diversified set of solutions to its clients and lead a business model whereas cyber security became a form of "technology enabled insurance" (WOODS, 2014). Post-acquisition, Mandiant is now portrayed as a consulting subsidiary. As FireEye announces in its own website, Mandiant works in "responding to the most critical cyber-security incidents and empowering organizations to protect their most critical assets" (FIREEYE, 2016).

Another group of companies announces a radically distinct business: the business of zero-day vulnerabilities – and, in some cases, the potential exploits derived from them[61]. Some of them not only commercialize active defense, but also openly advertise for cyber "offense" solutions, as the case of Hacking Team and the already-out-of-business VUPEN (now ZERODIUM). This group is more often than not directly in touch with agencies in the intelligence and security community, but it also demonstrates interest in the commercial cyber security market. VUPEN, for example, had a threat protection program to both government and corporations, but the commerce of exploits was – at least, in theory – restricted to the first.

Fidler (2014) notes that the market for zero-day vulnerabilities is part of a lucrative trade in cyber weapons and "unlike cryptography and nuclear technologies, where the government played a strong role in development, the private sector zero-day vulnerability market and the discovery of zero-days by in-house government teams seem to have largely developed simultaneously" (FIDLER, 2014:10). One particularity of this market is the value of secrecy – an exploit of a vulnerability can only be developed if the vulnerability in question is not patched or explored by other agent.

Most "boutique" companies[62] operate in the "gray market" for zero-day vulnerabilities. The gray market involves the trade between sellers, governments and other non-criminal clients. Distinctly from the black market, the gray market is legal. But unlike the white market, composed by reward programs to researchers

[61] A zero-day vulnerability is a flaw in a computer or software code, often unknown by the programmer or the company responsible for its development. An exploit is a code written specifically to take advantage of this vulnerability (see FIDLER, 2014). For an empirical study on zero-day attacks, see Bilge and Dumitras (2012).

[62] Ollman (2012) employs the term "boutique" to refer to vulnerability vendors. The term implies that this group offers a niche of a high-priced product, if compared to the "exploit development ecosystem" that involves bigger companies and the government, on the side of the "gray" market, and the illegal activities in the black market.

that report vulnerabilities[63], despite its legality, this market can create adverse consequences for cyber security (FIDLER, 2014).

The Italian company Hacking Team serves as an example of this issue. Details about its business became available at WikiLeaks after the company was hacked. Publicly, the company offers offensive cyber security services to law enforcement and national security organizations, using malware and zero-day vulnerabilities to gain access to a target's network (HERN, 2015; HACKING TEAM, 2016). The company affirms it provides tools to the government to fight crimes and terrorism and that it does not sell to non-State actors nor to governments blacklisted by the U.S., the E.U., the U.N., NATO or ASEAN. But the leaked documents suggest that it could have been commercializing with non-State actors, as one invoice reveals a deal of a three-month access to its remote control tool, which allows hacking into Android, Blackberry and Windows devices, between the company and a private Brazilian firm (see HERN, 2015). The Citizen Lab of the University of Toronto has reported that a surveillance backdoor commercialized by the company was used to target a Moroccan citizen journalist group (MARQUIS-BOIRE, 2012), and that U.S. based data centers were used as part of foreign espionage anchored on Hacking Team's remote control tool (MARCZAK et al., 2014).

The DoD and the FBI are among the U.S. government agencies that contracted Hacking Team's services, according to the documents leaked in 2015. The FBI has been using the remote control software since 2011 in its Remote Operations Unit. The agency deploys malware in investigations, but details on these efforts are blurred (CURRIER; MARQUIS-BOIRE, 2015).

Besides Hacking Team, there are a few other companies that became known for their involvement in the zero-day market. Endgame is a good example of this. The company now orients itself to the wider market of commercial defense products, but the previous involvement with the zero-day market granted it the title of the 'Blackwater of hacking.[64]' As a contractor of intelligence and defense

[63] Some companies have reward programs for security researchers that communicate vulnerabilities in their software, but since it is not their main business, rewards are not higher as in the commercial market. For a detailed study on these vulnerability reward programs, see Finifter et al. (2013).

[64] The reference is made to the role of the polemical private security contractor Blackwater (and of private security companies, broadly) in the Iraq War.

companies, Endgame used to sell zero-day exploits for millions of dollars a year, promising it would not disclosure the discovered vulnerabilities to software makers that could patch them. This business became public after Anonymous, the hacker group, published e-mails from Endgame's partner HBGary Federal.

The "new" business of Endgame allowed the expansion of its services to the commercial cyber security market. The company now offers Big Data solutions and sells a "vulnerability intelligence" software that works by pulling together information from the customer's navigation and security systems and pairing it with the company's own research on malware. (GREENBERG, 2014).

Greenberg (2014) argues that, although Endgame no longer sells exploits, the company doesn't deny having businesses with the government and selling the agencies tools that can be used for offensive hacking. Its CEO avoids commenting about government business due to secrecy agreements. It is worth noting, however, that its 'vulnerability intelligence' service can be employed to discover flaws in a surveillance target. And that the company commercializes cyber security solutions that allow for offensive measures to be adopted.

Distinctly from broader commercial defense market, the legal market for zero-days is, on its surface, restricted to governments. The Snowden leaks showed that, in the year of 2012, the NSA contracted a 12-month subscription to VUPEN's exploit service. The CEO and head researcher of VUPEN, Chaouki Bekrar, has argued that the partnership between intelligence agencies and vulnerability sellers is nothing but common sense: "There is no news here, governments need to leverage the most detailed and advanced vulnerability research to protect their infrastructures and citizens against adversaries" (BEKRAR *apud* SCHWARTZ, 2013). The company advertised itself as a leading provider of defensive and offensive cyber security intelligence (see SCHWARTZ, 2013; HARRIS, 2014).

The reasons why VUPEN's business came to a term in 2015 are not clear. But its founders' new company, ZERODIUM, offers a very similar business model. Unlike Endgame, ZERODIUM has not left the zero-day market, but instead, it acquires zero-day discoveries from independent researchers and resells them to its corporate and government clients. In practice, it is hard to see broader changes. ZERODIUM has offered about a US$1 million for an iOS zero-day exploit. To what end is quite unclear.

The table below indicates the dominant approaches to cyber security that IT companies adopt, through the main products and services they advertise.

Table 5: IT companies' dominant approaches to cyber security

	Defensive	Offensive	Active-Defense
FireEye & Mandiant	-	-	Data Center Security
			Enterprise Networks
			Incident Investigation
			Endpoint and Mobility
			Mandiant's consulting services
Hacking Team	-	Remote Control System Galileo	-
Zerodium (former VUPEN)	-	-	-
Endgame	-	-	Endgame Platform
			Endgame Hunting Cycle

FireEye's (and Mandiant's) solutions openly adopt an active-defense approach, which the company names 'adaptive-defense.' The purpose of such approach is to go beyond conventional security, as 'it gives security teams a fragmented, incomplete view into what's going on in their network. It's passive and blind to broader threat trends' (FIREEYE, 2015). The company proposes, instead, an anticipatory, more flexible and integrated framework that incorporates 'internal' (the endpoint's, the customer's) and 'external' intelligence provided by the company's teams or by Mandiant's consulting services. FireEye products also have a focus on investigating the origins and patterns of threats and attacks, in order to provide the customer better risk assessment and incident response.

A distinct pattern can be observed in Hacking Team's Galileo. The company openly advertises[65] for an offensive approach to cyber security. Anchored in the military strategy, the offensive approach is characterized by the adoption of measures such as the conduction of reconnaissance and surveillance, the interception of communications, the denial of access and resources, compromising

[65] The Hacking Team's website announces: "we believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities." (HACKING TEAM, 2016).

systems and undermining its integrity (the so-called ‘hacking back’), and by disabling or destroying assets (ROSENQUIST, 2013).

As Hacking Team announces, its main customers are governments. The threat framework the company emphasizes involves the risks of cybercriminals and terrorists using mobile phones, tablets, laptops and computers equipped with end-to-end encryption. The company’s solution provides law enforcement and intelligence communities a way to bypass this ‘barrier’: Galileo, a hacking suite for government interception.

The “Hunting Cycle” is Endgame’s strategy to counter cyber threats. It has four pillars: to survey, to secure, to detect and to respond. The idea of hunting corresponds to the ‘proactive, surgical, stealthy pursuit and eradication of adversaries to protect enterprise networks’ (ENDGAME, 2016), while the response strategy to be crafted correspond to including options such as killing malicious processes, deleting persistence, blocking traffic or gathering additional forensic data, once the threat is identified.

The case of Endgame is slightly distinct, when compared to the two previous cases. The company does not adopt an openly offensive approach. Its focus is on turning enterprises into ‘hunters,’ proposing that organizations embrace an offensive strategy *within* their networks, instead of waiting for the attack to happen. Thus, despite the possibilities that its platform is being used by its government clients for surveillance purposes (GREENBERG, 2014), the company’s solutions were categorized as ‘active defense.’ This option is justified by a lack of exclusively offensive measures in the company’s advertisements, but not necessarily by the lack of offensive possibilities in the its solutions. Active defense encompasses the possibility of adopting offensive measures in face of an attack, but offense is not the only way to deal with a security threat.

ZERODIUM’s approach to security will remain uncategorized, due to the insufficient data provided by the company. Although the work found indicators that its business remained similar to its antecessor, VUPEN, the actual dynamics of its vulnerability research program could not be properly scrutinized to the point the research could provide a precise characterization about its approach to cyber security. It would be possible to discuss that there is a tendency within the zero-day market that indicates an inclination to an offensive or, at least, active defense bias. It would also be possible to consider that the vulnerabilities that ZERODIUM

acquires and commercializes with other companies and governments are used for offensive measures, such as surveillance, but it is not possible to characterize the company's business as inherently offensive with the little data available about it.

Among the companies involved in the vulnerability and intelligence milieu, there is an attempt to expand business beyond the government sector, but no intention of leaving it. Some businesses rearrangements, like Endgame's and ZERODIUM's, can possibly signal an attempt to look at both market niches. Pressures to secure cyberspace contributed to creating this commercial security market for offensive and defensive cyber security, cyber warfare and surveillance technologies. Thus, despite being relatively small companies, there is a real concern about the implications of the commerce of intelligence solutions and vulnerabilities for security and privacy online. But these 'boutique' companies are far from being alone in the market for offensive and defensive cyber capabilities. Some bigger actors are willing to grab their own parcel of the cyber 'pork', to use Brito and Watkins (2011) term, for themselves.

4.2.3. Defense contractors

As Deibert (2013) notes, this last category is the most secretive among the private actors investigated so far. It is composed by traditional defense contractors whose businesses with the U.S. government dates back to the Cold-War period. Since the late 1990s, in face of restrictions to the defense budget, some of these traditional contractors have oriented themselves to the burgeoning cyber security market (DEIBERT, 2013; HARRIS, 2014; BRITO; WATKINS, 2011).

The secrecy around these companies' businesses makes it more difficult to investigate their strategies with precision. However, some complementary tools, such as the description of the job positions being offered and reports on the acquisitions of technology companies working with cyber security by those defense giants can offer a good reinforcement for the journalistic texts and the information made available both at the websites of these companies and in the WikiLeaks files. The strategy of acquiring minor companies is, in itself, a good thermometer for measuring the kind of business that major defense contractors have with their clients inside the government.

For example, it can show how the current market niche for these defense contractors can be quite confined to the aerospace, defense and intelligence sectors of the government. According to Morgan (2016), these sectors were among the largest contributors to the gross revenue in the cyber security market, in the year of 2015. In the past decade, the sum spent by the U.S. federal government in cyber security was of around US$ 100 billion and the Obama administration has budgeted around US$ 14 million for 2016.

The fact that some defense contractors, such as Boeing and General Dynamics, opted for selling out their cyber security businesses companies with commercial-oriented products may indicate that they are leaving the commercial cyber security market for companies that want to work with corporate customers, and focusing on the government clients instead (MORGAN, 2016). Raytheon Co., one of the biggest defense contractors, has adopted a distinct strategy to conciliate commercial and government demands, leaving for its subsidiary Forcepoint the task of dealing with the commercial market. Another big defense contractor, Northrop Grumman Co., has made a similar move with the creation of its new business unity, Acuity Solutions Corp. Defense contractors have a lot to gain in their business with the government agencies, but the dynamics of working with quite secretive tasks and of working with corporate necessities may be very distinct. This may help to explain why some companies opted for leaving the commercial cyber security sector, while others created separate businesses to answer to the demands of their commercial customers.

All of the major defense companies investigated (Raytheon, Northrop Grumman Corp., Bae Systems, Boeing, General Dynamics, Booz Allen Hamilton and Lockheed Martin) have now entered the cyber security business. They've done so by acquiring smaller several cyber security companies and, at the same time, by developing their own capabilities. Boeing announces it has services on CIP, network surveillance and data analytics, information security, mission assurance and information operations capabilities, whilst Northrop Grumman adds situational awareness, modeling and simulation, cloud security and supply chain to the portfolio. It refers to the work of its cyber security team as being made by "developing systems and solutions that are revamping the entire cyberspace continuum of defense, exploit, and attack."

The involvement of defense contractors in the vulnerability exploit business has recurrently appeared in the media and in the literature on cyber security (SCHNEIER, 2012; 2013; DEIBERT, 2013; BRITO; WATKINS, 2011; HARRIS, 2014), but it is quite difficult to assess, if compared to their smaller and less traditional competitors. Raytheon, for example, announces a series of cyber security solutions for integrated defense systems and intelligence. The list of products (and the forms of cyber security covered by them) that the company offers is the biggest among the contractors investigated. But what calls attention is less the vast cyber capabilities the company has and more the possible functionalities of these capabilities – the "what are they being used for?" question.

The hint may come from quite an unexpected source. Some of the company's jobs announcements call for reverse-engineers and vulnerability researchers to be part of a "highly-skilled and dynamic team that performs vulnerability research and exploit development" in the incorporated Blackbird Technologies, a cyber security company specialized in providing surveillance and secure communications to spy agencies and special operation units. The acquisition of Blackbird by Raytheon has cost about US$ 420 million (REUTERS, 2014). The position for Insider Threat Analyst at the same company requires the candidate to have experience with counter-intelligence and to "collaborate with the intelligence community and Federal Civil partners to share and collect cyber threat data for use in strategic threat assessments, prioritization of resources and development of lead generation." (RAYTHEON, 2016).

In the same vein, General Dynamics requires professionals familiar with zero-day exploits or capable of analyzing unpatched vulnerabilities. The company's cyber security solutions are part of its "Mission Systems", integrating Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems for all domains plus cyber.

Defense contractors got quickly involved in the market for offensive cyber warfare and surveillance technologies. Since the 1990s, the number of cyber-units in these companies has increased. For example, the Booz Allen Hamilton's cyber unit, which focuses on intelligence, was built in the years of 1996 and 1997 by the former NSA's director John M. McConnell. And, like McConnell, many others have employed the knowledge acquired while working for defense and intelligence agencies to create and improve intelligence and cyber security units in private

defense contractors. Taking advantage of the so-called revolving door between government and businesses, government employees head off to the industry after serving intelligence and defense agencies long enough to acquire training, top-secret security clearances and professional contacts and acquaintances. Then, they sell back to government agencies what they've learnt during their stay in the government (HARRIS, 2014).

Table 6 analyzes the defense contractor's main approaches to cyber security, based on a research among the characteristics of the core products and services they advertise in their websites.

Table 6: Defense Contractors' approaches to cyber security.

Company	Defensive	Offensive	Active defense
Bae Systems	-	-	Threat Investigation Solution
			Threat Intelligence Management Plat-form
			Communication and Intelligence technologies
			Automated Threat Detection service
			Cyber Threat Intelligence Team
Boeing	Advanced Malware Assessment Services	-	TAC
			Cyber Analytics Center
Booz Allen Hamilton	Application Security	-	Cyber4Sight
	Information protection		Insider4Sight
	Identity and Access Management		Global4Sight
	Infrastructure and Mobile Security		CyberReady
General Dynamics		-	Security Operations Centers

	Defense and protection capabilities		Critical Incident Response Teams
Lockheed Martin	Industrial Defender Automation Systems Manager	-	Pallisade
			Advanced Threat Monitoring
			LM Wisdom Insider Threat Identification
			Enhanced Threat Protection
			Analysis on Demand
			Security Operations Center
Northrop Grumman	The FAN	Full Spectrum Operations	Cyber Security Operations Center (CSOC)
Raytheon	-	-	Cyber Security Operations Center (CSOC)
			Cyber Range
			Proactive and Dynamic Defense
			Threat Research and Assessment
			Converged Cyber
			Raytheon Riot Tool**

**Unadvertised

The first thing that should be noted is that Table 6 indicates that defensive products are not excluded from the portfolio of defense contractors. It was identified that General Dynamics, Boeing, Booz Allen Hamilton, Lockheed Martin and Northrop Grumman offer at least one openly defensive product/service. General Dynamics defense and protection capabilities include, for example, the deployment of perimeter defenses, protection against zero-days and infrastructure hardening, while Northrop Grumman's "The FAN" is a layered cyber security defensive model to customers building a secure IT architecture.

A second thing that should be noted is that the table indicates that all the actors investigated have a core solution that can be easily characterized as 'active-defense.' What these distinct solutions have in common is the purpose of not only

protecting a machine, a network or the end-user's *online* activities, but also investigating the dynamics of the attack and, in some cases, even punishing the attacker. The basic trait of these products is the fact that the 'defense' is not restricted to the endpoint environment anymore.

Dittrich and Hima (2005) define active defense as constituted by digitally-based, reactive[66] measures that aim at countering an intrusion and serve to investigative, defensive or punitive purposes. These measures are non-cooperative, in the sense that they are implemented without the consent of (at least) one of the parties involved or affected by the intrusion and they tend to impact a remote system (a system that is owned or operated by a third party). According to the authors, "these tactics range from more benign information-gathering measures (e.g., trace-backs) that impact remote systems without impairing their ongoing operations and functions to more aggressive measures (e.g., denial of service counterattacks) expressly intended to inhibit or even stop the operations and functions of remote systems" (DITTRICH; HIMA, 2005:3-4).

A distinction must be made between the offensive and active defense approaches. Offensive security is an independent approach which focuses on using offense to enhance cyber security. Active defense is also an independent approach, which can comprise both non-offensive and offensive measures. In the work, the option was for categorizing as offensive only those products with a manifest offensive purpose (such as conducing cyber operations, or running a platform for government surveillance). The remaining products were considered as active defense because their purposes are not exclusively offensive, although offense can be an option in some cases.

Lockheed Martin's *Pallisade* is an intelligence platform that allows the collection of intelligence about an adversary in order to identify the motives and tactics employed in an attack. It operates under the Cyber Kill Chain framework, a cyber threat model developed to detect a persistent adversary, analyze the attack progress and develop 'actionable intelligence' (LOCKHEED MARTIN, 2016). Bae System's Threat Investigation Solution and Threat Intelligence Management Platform and Booz Allen Hamilton's predictive intelligence solution which include

[66] In the sense that measures are implemented following the detection of an unwanted intrusion and are intended to counter it.

Cyber4Sight, Insider4Sight, Global4Sight and CyberReady solutions, play a similar role as they focus on the detection and investigation of the behavior of the attacker.

If compared to the other companies, Northrop Grumman's website is less specific about the products developed by the it. It is possible to identify the line of security within which the company works, as it advertises having cyber intelligence capabilities "for collecting, fusing and analyzing cyber data to provide actionable information and situational awareness for operators in support or conducting cyber missions," cyber resilience capabilities to serve "as contingencies for compromised networks and platforms to sustain basic functionality and/or restore an optimal state," active cyber defense capabilities to enable defenders to "more readily disrupt, mitigate and neutralize cyberattacks and vulnerabilities through proactive anticipatory actions and/or direct engagement with adversaries in a controlled cyberspace environment;" it is working in the full spectrum of cyber operations, through the integration of cyber and non-kinetic capabilities in order to plan, map, access and maneuver undetected through targeted networks; and it employs "D5 effects[67]" against adversaries, "to shape and prepare the operational environment, and/or work in conjunction with other non-kinetic effects" (NORTHROP GRUMMAN, 2016). These "Full Spectrum Operations" signal that the company engages, with the U.S. government, in real-world, cyber operations, with purportedly offensive ends, as the employment of the D5 effects indicates.

The presence of security operations centers (even if in the form of threat intelligence teams or analytics centers) is a feature that is worth noting. Basically every defense contractor investigated offers a service of this kind, oriented at providing cyber security consulting, training, threat investigation and tracking and incident response. These centers are not always advertised as services in themselves. They can be equally 'implied' in other solutions, as is the case of Lockheed Martin's *Analysis on Demand* service, in which intelligence analysts investigate and analyze threat-related data in order to provide risk-mitigation.

In general, the imperatives of risk-mitigation and prevention underlie most of the advertises of cyber security companies. But regarding active-defense, it

[67] D5 effects refers to the U.S. Air Force "Degrade, Deceive, Destroy Deny, Disrupt" strategy to use the cyberspace domain in its advantage. It represents an open position within the U.S. government regarding the possibility of attacking adversaries through cyberspace.

becomes a part of another imperative, that of prediction. The notion of predictive intelligence is anchored on the attempt to, through the careful tracking and investigation of a threat, predict future risks and adopt measures to anticipate to them.

Booz Allen Hamilton offers a whole line of products under the label of predictive intelligence. According to the company's website, anticipatory, predictive intelligence is fundamental for an effective security posture. In this sense, predictive intelligence involves the anticipation, prevention and response to global threats. This requires not only advanced IT techniques, such as big data analytics, but also a technological savvy workforce.

It should be noted that an exception figures on Table 6. Raytheon Riot Tool escapes the main methodology employed in the work as it was not advertised in the company's official website, once it was secretly developed on the request of the FBI. Raytheon Riot Tool is a social-media, data mining application in which the main function is to analyze whether an individual is to be judged or not a security risk. The existence of this application came to public in a The Guardian's 2013 article, where the company recognized to have developed and shared the application with the U.S. government and the industry, as part of a joint national security research and development effort (GALLAGHER, 2013).

A final, interesting remark, concerning the solutions offered by the selected defense contractors is the fact that, as secretive as these companies might be about some of their solutions, as in the case of Raytheon Riot Tool illustrates, the involvement with the intelligence sector is publicly recognized and advertised as a strategic advantage for both the companies and the national security community. Bae Systems describes itself as a global provider of communications and intelligence technologies. Boeing includes among its offerings critical infrastructure protection, network surveillance and data analytics, information security, mission assurance and information operations capabilities. Northrop Grumman emphasizes its intelligence capabilities. Lockheed Martin offers to its government clients cyber security solutions for intelligence-driven defense. General Dynamics advertises that through its capabilities, it defends the nation's critical cyber resources and networks, and it assists its defense and intelligence customers with the solutions it develops. Raytheon's cyber security products are part of a broader Intelligence, Information and Services business. Lastly, Booz

Allen argues for a collaborative framework with the defense and intelligence community to tackle the challenge of cyber risks.

The products and services on Table 6 are a small parcel of what is offered by defense contractors to governments and commercial customers. Comparing the three categories of cyber security companies studied in the work, the solutions advertised by the last group were the ones that presented the most diversified set of approaches to cyber security. This can be explained by the variety of solutions they offer, if compared to antivirus and IT companies. Considering only the categories investigated (commercial/business, paid and pro/advanced), each company within the antivirus group presented an average of 8,5 main products and services, while in the case of IT companies the average was of 4. In the case of Endgame, ZERODIUM and Hacking Team, the products and services portfolio was relatively small (two main products/services in Endgame's case and one in Hacking Team's and ZERODIUM's).

This may be an indicative that not only are defense contractors investing heavily in the cyber security field: they are also investing in a specific approach to cyber security, one that even in the case when it is not openly offensive, it can be marked by some offensive contours. In general, cyber security companies are not focusing alone on 'hardening the infrastructure' and waiting for it to be capable of blocking an attack anymore. Even manifest defensive products and solutions come with at least a basic risk-management tool. The most recent appeal to active defense, and even openly offensive approaches, should bring some reflections about the concept of security that these companies are producing through their practices.

The next chapter discusses the impacts of active defense and offensive approaches on the concept of security. It discusses the patterns found in this chapter's analysis, analyzes the disputes among companies for a dominant approach to security and develops a reflection about the current dominant paradigm of security and about the place of defensive, active defense and offensive approaches in it.

The problem with a "digital arms trade" (DEIBERT, 2013:348) for products and services involving active is its possible impact over actual security in cyberspace. This trade is part of a market that has been irresponsibly fueled by the competition around the definition of cyber threats and cyber security and by the growing hype around threats coming from cyberspace. As Deibert (2013) observes,

there is a growing legitimacy in the adoption of ‘retaliatory’ measures and the increased intelligence-gathering capabilities of private companies (traditional defense contractors or not) to prevent constant penetrations in their networks. These companies now offer services that allow them to hunt threats, and preventively assess risks, in contrast to companies that offer passive defense solutions.

5. An analysis of cyber security companies' disputes over the production of cyber security

In the previous chapter, it was argued that cyber security companies produce specific conceptions of security through their practices, that is to say, through the advertisement and commercialization of cyber security solutions. Three approaches were identified in each sub-category of company: a defense-oriented approach, predominantly found in the antivirus companies' products; an offensive approach rising in the context of IT companies in the zero-day market; and a mixed approach, named active-defense, mainly adopted by defense contractors. The current chapter discusses the characteristics of each approach and the symbolic disputes happening within the *champ* for the prevalence of a certain category over the others.

The main argument is that the three approaches to cyber security have something in common: to a certain degree, all rely on risk-based practices and on a risk-oriented approach to security. The role of risk varies within each case, as it can be used to justify the development of less-intrusive and more defensive cyber security solutions, or the employment of a more aggressive approach to combating cyber threats. Based on this, it is argued that having 'risk' as a common ground does not equalize the implications, for security, of the three approaches.

The chapter is divided in four moments. Firstly, it discusses the semi-conscious disputes underlying the approaches identified in the research. Disputes are partially unconscious because companies do not always recognize themselves as a part of a dispute for the production of a concept. On the other hand, most companies assume to be in direct competition with their equals, based on the liberal, capitalist assumption of free-competition.

It is argued that there is a prevalence of active-defense, in contrast with an openly offensive or exclusively defensive approach that is strategic to the companies' relations with the State. As is the case with the use of force, in the U.S. (and in most countries in the world), only state-actors and the corporations under contract with them have the legal endorsement to process and collect intelligence and to conduct offensive cyber operations. But as a certain degree of suspicion falls over the idea of a company 'hacking back,' or simply proactively hacking a third party for whatever the purpose, the label of active defense comes as a relief separating the more assertive investigation operations in order to attribute the attack

and the use of ‘security through obscurity’ measures from active hacking activities. In this sense, active-defense may be seen as a viable solution not only for defense contractors, but also for other cyber security companies, among the antivirus industry and IT companies, that commercialize products and services with such approach.

Secondly, the chapter analyzes the predominance of an anticipatory approach to security in most of the solutions analyzed, and the strength it has when active defense is concerned. The argument is that anticipatory cyber security has in the current paradigm of risk a fertile ground. As argued in chapter two, this paradigm is marked by the existence of complementary attitudes towards risk. Active defense invokes a paradigm of prevention: when everyday cyber security is concerned, the adoption of measures to anticipate the risk, relatively known in nature, but far less predictable when it comes to the moment of the attack, is portrayed as the best strategy to combat it. The exception is the precautionary nature residing in the invocation of the ‘digital disaster’ (HANSEN; NISSENBAUM, 2009). Risks to critical infrastructure and the threat of cyber terrorism, when directly addressed by companies, may result in different strategies to deal with risk, but follow a very similar path in regards to the discourse adopted by governmental instances.

Thirdly, the chapter traces a correlation between active defense and the marketization of security, discussed in chapter one. The argument is that the predominance of active defense as a viable solution to fight cyber threats and the appeal that more offensive strategies are slowly conquering within industry are both coherent with the entanglement between states and markets that has accompanied the development of the cyber security *champ*. The growing popularity and acceptability of invasive solutions result from the traditional bridges constructed between the government and industry, through partnerships, contracts and the workforce mobility.

Lastly, the work considers the implications of the preference for active defense for the concept of security. The core of active defense strategies is a process of intelligence-acquisition about the threat in order to trace proper risk-mitigation strategies and to proportionate adequate ‘incident response’, in which the former and latter terms have a wide semantic nature. The information and techniques gathered in the investigative process allow for better prevention, and as cyber threats are said to evolve and improve each day, the cycle of hunting for more

information about them continues. In the midst of this cycle, the temptation of going on the offensive becomes strong. And, in some cases, the imperative of active defense can even conceal more offensive attitudes towards the adversary.

5.1. The symbolic disputes for the production of cyber security

This section continues the analysis started in the previous chapter, expanding the discussion about the characteristics of each approach to cyber security. It considers each approach as a strategy, adopted in the context of the *champ* to proportionate companies a certain advantage when the governmental market is concerned, and analyzes how the disputes among private companies, recognized as part of a liberal-capitalist natural dynamic of free-competition among private entities, produce dominant understandings of security, in general, and of cyber security, in particular.

In economics, competition is a constitutive aspect of the market process. It is believed to be beneficial for economic performance, productivity and innovation (OECD, 2014). Private companies, in general, have in the struggles with other companies for the offer of goods and services in the market a commonsensical, long established, social norm. Less emphasized, however, is the underlying competition for establishing particular understandings about the businesses they're in. Thus, when the work claims that companies engage in symbolic struggles, it stresses that, as with other social universes, the dispute for the production of specific understandings regarding cyber security is not always expressly recognized by private companies as such. Disputes are commonly portrayed as natural outcomes of the market dynamics, inside a context of search for profit and scarcity, and not aiming directly at the production of a specific meaning about something.

The advertisement of products and services is one important strategy in the struggles within the cyber security *champ*. It sets the companies' strategies and perceptions regarding the most pressing risks and comes as a response to pressures within the political and military spheres to make cyberspace more secure to national security ends. These products and services also manifest the companies' distinct perspectives on how cyber-threats are best combated. By posing the advertised solution as *the* solution against a certain security issue, they advocate that the approach they adopt is the most suitable in the context of the selected target audience.

Kaspersky's Anti Targeted Attack may be useful to counter APTs in an organization's network, while Total Security for Business is the most suitable to protect a company's endpoints. These two solutions belong to the same company, but have distinct approaches to security – the first is active defense, the second, defensive. – They tell something about the nature of the dispute at stake: on one side, companies advocate for an exclusive view of security, as is the case of Hacking Team's offensive approach. In most cases, however, the disputes do not involve companies defending a given view instead of another. Different approaches have been observed within the same company's portfolio (see Tables 4, 5 and 6 in topic 4). This indicates that what these disputes are about is the allocation of specific views of security to specific groups of customers.

The defensive approach tends to be associated with the home user and small and mid-sized businesses. Cyber security solutions falling under a defensive view of security all presented an emphasis on hardening the endpoint's infrastructure and combating the threat once it was inside the system, network, or similar. This focus can be related to the security requirements of the targeted groups, which tend to be low if compared to governments, critical infrastructure operators and big corporations or private entities dealing with sensitive information, such as banks. In this perspective, a local store will hardly face the same security threats a big multinational corporation will and even if it does, the risks would be allegedly lower. The antivirus companies that have expressly affirmed to be working with governments, critical infrastructure sectors or larger corporate clients have presented solutions in the active defense spectrum.

In those solutions where defensive cyber security was portrayed as unable to address the dynamics of current cyber-threats, the option was for a distinct approach to security. The inability of exclusively defensive measures to counter current threats is associated with the way that newest IT technological developments, and particularly the IoT, open new avenues to attacks. To address the new security challenges posed by advancements in technology, security would do better if reformulated.

The urge to reformulate the concept of (cyber) security answers to the needs and specificities of two particular groups: government and big corporations. Companies that have in these groups their main target audience have presented more solutions in the offensive and active defense spectrum, if compared to those

with a focus on smaller, commercial customers. Among other things, this suggests that governments and corporations have at their disposal alternatives like using advanced intelligence-gathering techniques to go on the hunt[68] and, in some cases, even retaliating an adversary's attack.

As shown in chapter three, the overtly offensive alternative has been advocated by Hacking Team. Hacking Team publicly announces to commercialize its surveillance solutions only with governments, as it sustains that security produced by law enforcement (and counter terrorism) is a fundamental right of the citizen. Most recently, after researches indicating that the platform has been used by non-democratic governments to surveil citizens (MARQUIS-BOIRE, 2012; MARCZAK et al., 2014), the company has updated its customer's policy to settle that it does not commercialize with countries blacklisted by the U.S., the European Union and NATO.

The offensive alternative is particularly worrisome as it implies that agents actively engage in surveillance-like activities and even in limited, cyber-war like scenarios. And as Rosenquist (2013) indicates, the offensive security approach is driven by the military doctrine of controlling the battlefield and taking the fight to the enemy. It legitimizes a series of controversial measures, from surveillance to hacking another party's system, in the name of security and law enforcement.

Although some people advocate for an increased adoption of overtly offensive measures by private companies – or believe that this is only a matter of time (INFORMATION WEEK, 2013; ROSENQUIST, 2013), the imperative of active defense remains the most adopted by cyber security companies. This solution is most often associated with the challenges faced by big, commercial and government clients, which tend to be equated, if not almost equalized.

In contrast with Hacking Team, for example, Endgame has a more diversified customers base. And with such a wider base, it has adjusted the way it addresses security challenges. It advertises that the experience with the intelligence community and the department of defense is helpful for its commercial customers, as the challenges faced by government actors have eventually become commonplace. Marked by an involvement with the zero-day market, the company

[68] "Going on the hunt" suggests the use of intelligence to gain information about an attack and those behind it. It is a constitutive step of both active defense and offensive products and services.

now uses subtle terms, such as offense within a company's network, and allies the terms 'defense' and 'hunt' to characterize its commercial strategy. It equalizes the security requirements of private actors and governments, and pictures its customers as hunters. As such, Endgame characterizes the security of private companies as marked by an imperative of reacting and gathering intelligence about an attack.

The alternative of active defense is strategic to cyber security companies' relations with their commercial customers, but most fundamentally with state-actors. To big corporate clients, active defense opens up a way in which intelligence-gathering about an attack and the countermeasures it allows can be used to their favor at a payable cost. In what concerns the companies' relations with their government clients, active defense may come as a euphemism to the combined use of intelligence collection and (aggressive) countermeasures. This is because under the U.S. law[69], companies are often discouraged to adopt tactics such as hacking back, except with the government's endorsement.

In the context of the cyber security market,[70] active defense establishes a semantic separation between assertive investigative operations and 'security through obscurity[71]' from offensive activities outside the victim's network, such as hacking back. On the one hand, it addresses the perceived common security challenges faced by the target audience. But it also attends to the expectations of all the parties concerned (vendors and customers alike): active defense becomes a viable solution for those cyber security companies that aim at the strategic, government market. The most sophisticated the capacity of the product/service to 'anticipate' the threat, the bigger is its appeal. At the same time that it rises as a dominant conception of security, it becomes a strategy in the midst of the disputes for this specific piece of the market. In the struggles to delimit which security is the most suitable to whom, cyber security companies compete to define how governments and other relevant, commercial customers should protect themselves.

[69] Criminal offenses under the U.S. Computer Fraud and Abuse Act (18 USC 1030).

[70] The military definition for active defense involves the adoption of measures to both detect, analyze, identify and mitigate threats and offensive capabilities and resources. In the same vein goes the definition proposed by Dewar (2014).

[71] The concept refers to the reliance on the secrecy of the design and/or implementation of a network, endpoint or system as a method to assure its security. See Anderson (2001).

5.1.1. Disputes between openly offensive security, defensive security and active defense

At first sight, openly offensive, defensive and active defense solutions seem to coexist peacefully in the cyber security market, each one specifically aiming at a certain kind of customer. There are, nevertheless, disputes between these competing approaches to security which manifest in studies and texts that make the case for one or other approach. One fundamental issue at stake is the possibility of granting broader, legal authorizations of the use of 'hacking back' by private actors.[72]

There is little disagreement over the importance of defensive measures. Defense is a constitutive part of offense and active defense, and it is an approach in itself. Contestations revolve around the reliance on purely defensive measures, on the option for equating cyber defense solely to the hardening of the infrastructure and of the resilience of the machine and network. Those making the case for active cyber defense or for the adoption of an openly offensive strategy argue that defense alone does not suffice to protect against cybercrime and other cyber threats (DEWAR, 2014; GLOSSON, 2015; STRAND, 2015).

The research has observed that those making the case for active defense seldom conflict with the proponents of an openly offensive approach. In some cases, they establish a distinction between both approaches, considering that offense is a prerogative of governments and their contractors (and of companies that sell these solutions exclusively to governments), whilst active defense may have a broader range. What is often established is that active defense is distinguished from offense because it comprises more than just the possibility of hacking back (DENNING, 2014; DEWAR, 2014; STRAND, 2015).

The active defense approach and the debate concerning its elements derive from the U.S. military doctrine. When discussing a framework for active defense, Denning (2014) argues that this is an approach to cyber defense which is multi-dimensional, with four dimensions: the scope of effects (if they are either internal or external), the degree of cooperation (if it's cooperative or non-cooperative), the type of effects (if it involves collecting, sharing, blocking or adopting preemptive

[72] For a debate on legal interpretations of the hacking back alternative in the U.S. Computer Fraud and Abuse Act, see Steptoe (2012).

measures against an attack), and the degree of automation (if it is automatic or involves human action). The author even considers that, in the case of the "cyber", private entities are expected to provide strong defense and active defense in order to defend their network, and these actors may be authorized, by laws, contracts and policies, to conduct certain active cyber defense measures, but does not delve further into the legal and ethical aspects of the use of active defense by private actors.

The Computer Fraud and Abuse Act is a legal barrier to the full employment of active defense measures, since it requires the private entity to have an authorization before it engages in 'hacking back' or similar activities. There is a debate over how the act is to be interpreted to allow private companies to legally engage in this kind of activity (STEPTOE, 2012) and, having this legal restriction in consideration, some have proposed a legal framework for the use of active defense by private actors (GLOSSON, 2015). As Dittrich and Hima (2005) observe, in some cases, companies adopt active defense measures without involving law enforcement agencies, either due to the pace of cyber-attacks against their networks or due to concerns with the effects of making an attack public to the company's reputation.

The case for the use of active defense by private companies on their own behalf has put some pressure on how the Computer Fraud and Abuse Act is to be interpreted while, at the same time, it has been positive for the commerce of this kind of solution. The pressure that some authors have made to argue that merely defensive measure are not enough, and that defense has to be more reactive (STRAND, 2015) indicates that there is a broader movement, in the U.S., in favor of adopting active defense as the main strategy for commercial and governmental cyber security. By avoiding a direct contestation of the offensive approach, the proponents of active cyber defense save for private actors the possibility of disposing of the full-spectrum of active defense measures for combating cyber threats – hacking back included.

5.1.2. Risk and anticipatory cyber security

A very interesting pattern that has been perceived in the course of the research is the reliance on a risk-oriented approach to security. To a certain extent, defensive, offensive and active-defense products and services have all focused on reducing or

anticipating cyber risks (the end), through either hardening the endpoint infrastructure (defensive measures) or investigating the pattern of behavior of the threat, as a form of anticipating and preventing future attacks from happening (the means).

In the context of the disputes among companies, the imperative of anticipating to risks appeared as a leveler tendency. Thus, to a certain degree, it is possible to affirm that the practices hitherto analyzed all rely on a risk oriented approach to security. They have all focused on solutions to mitigate risk or preventing it from taking place, in the first place. According to Ewald (2002), the preventive attitude relies on the ability of scientific knowledge and technical control to reduce the probability of risk.

The current security paradigm[73] offers anticipatory security a fertile ground to flourish. It is marked by distinct, complementary attitudes towards the possibility and probability of a risk to happen: providence, prevention and precaution[74]. Under the prevailing paradigm, the process of securing an undetermined number of fluxes that compose everyday life comprehends three dimensions in which a body is subject to protection, due the inherent permeability of the flux and the risks it poses; to control, in which the distinction between good and bad fluxes is established through processes of identification, localization and selection; and to regulation, so excesses are to be avoided and a certain equilibrium can be reached (GROS, 2012).

Defensive measures to a certain extent are measures of prevention in that, through protective measures set in face of the inherent permeability of the machine, prevention falls within the walls of the machine's security, with little or no consistent human interaction. The prevention is somewhat anterior and not directly dependent on a specific attack. It presupposes that without the assurance that a machine is properly secured, the risk of a silent, unperceived invasion is high.

Offensive measures seem, at first, at odds with the paradigm of prevention, but within the context of cyber security, they actually presuppose a prior process of identifying, investigating, localizing and selecting the target. Further, these

[73] According to Gros (2012), this paradigm is termed biosecurity and focuses on assuring the normal functioning of any given process or flux. The author considers that within this paradigm, each flux (of information, of people, of markets) arguably deserving protection, control and regulation constitutes a domain of security.

[74] These institutes have been conceptualized previously in the work.

measures can fall in the preventive specter of anticipatory cyber security once they're moved by the desire to attack sooner than later. The perceived risk is that not taking effective providences may encourage attackers to keep digging for more information within critical networks.

The whole notion of anticipatory security presupposes attempting to exert some control on facts that have not happened yet. In some cases, in order for this kind of control to take place, it is necessary to identify and investigate the *modus operandi* of the threat. Anticipatory cyber security rests on the premise that: one should avoid future risks by learning from past events. As already discussed, active defense relies on the adoption of measures to ameliorate the techniques of anticipation of the threat. It invokes the paradigm of prevention and places anticipation as the best strategy. Here, prevention depends on acquiring intelligence about a threat and then turning this intelligence in favor of the victims of a cyber-attack – and, incidentally, of cyber security companies' technical knowledge.

A possible exception to the preventive approach is the precautionary nature of the security concerns motivated by cyber-terrorism and the threat of a catastrophic disruption of critical infrastructure (in place of everyday disruptions). As chapter two has argued, it was the sense of urgency of these 'irreversible,' worst-case-scenario risks that served as core imperatives of securing cyberspace and triggered several calls for public-private partnerships (WHITE HOUSE, 2003; 2011; GAO, 2016).

Although within the anticipatory spectrum of security, in this case, the attitude towards risk is quite distinct. The precautionary principle suggests that the mere possibility of a risk is enough to take precautionary measures, but this risk often has as characteristic the irreversible nature of the damage (EWALD, 2002; GROS, 2012). This paradigm does not rely on the predictive nature of the most common, but not least complex, threats due to the nature of the object of security being threatened. In practice, the adoption of the precautionary paradigm within cyber security adds a degree of urgency to existent attempts to control and secure cyberspace against risks and may authorize dubious actions by companies and governments in alliance.

This is visible in the case of cyber terrorism, where the precautionary imperative has served to justify the adoption of offensive capabilities by companies and governments, and to a certain extent, it has contributed to equalize the attitudes

and measures adopted by both. The scenario is slightly more complex in the case of CIP oriented solutions, as the precautionary attitude has led to the preference for more active defense like products and services.

5.1.3. Active Defense and Marketization

The relations between cyber security companies and the U.S. government are a constitutive aspect of the struggles within the cyber security *champ*. As discussed in chapter one, through the process of marketization, the state authorizes, legitimates and takes part in certain market practices. In the U.S. cyber security *champ*, marketization takes form in the outsourcing of certain governmental functions, such as intelligence and data collection, cyber operations, maintaining the security of its information systems, and so on, and the constitution of public-private partnerships between IT companies and the federal government as a recognition of the power these companies have when it comes to information technologies.

It is possible to establish a logical correlation between the broader process of marketization, that takes place in the cyber security *champ*, and the predominance of active defense as a viable solution to combat cyber-threats – or even the appeal that certain offensive measures are having in the industry. Before being normalized in the practices within the cyber security market, concepts such as active defense and the concurrent adoption of offensive measures to answer cyber-threats were being explored within the U.S. military and policy-making universes (see DEWAR, 2014; NATO CCDCOE, 2013; GAO, 2004; WHITE HOUSE, 2003).

As argued in chapter two, the cyber security *champ*, as well as the formulation of cyber security policies and solutions, has been marked by an entanglement between public and private actors. The sharing of scientific and technical knowledge, new technologies and security concerns by these parties has become both a commonplace and a necessity (WHITE HOUSE, 2003; NORTHROP GRUMMAN, 2015). Public-private partnerships and defense contracts have been working as bridges, where information is exchanged, responses are coordinated and the security concerns of governments and companies become even. But these legal and political instruments are not the only factors that have influenced the equivalence of security concerns: the traditional mobility of IT specialized workforce between the public and private milieus keeps contributing to the 'import' of ideas from one sector to another.

Partnerships such as the Financial Institutions Information Sharing and Analysis Centre's (FI-ISAC) have resulted not only in information sharing, but also in joint actions. Botnet takedown operations were coordinated by the UK National Crime Agency and included the GCHQ, the Europol, the FBI, BAE Systems, Dell and Kaspersky Labs. A similar operation was carried out by the Microsoft's Digital Crimes Unit in conjunction with an ISAC, the FBI, the American Bankers Association and others (see HARRINGTON, 2014).

Actions of this kind, as well as the defense contracts tying corporations and governments together, are slowly contributing to a wider acceptability of more 'invasive' solutions and of the expanded version 'protect, detect and react' paradigm (OVERILL, 2004), which includes active 'threat intelligence' gathering services, through the activities of CSOCs, being offered by private companies.

But in some situations, alliances between governments and corporations can result in the development of invasive surveillance tools, such as Raytheon's Riot Tool, and on the deployment of equally invasive operations as attempts to identify potential threats to national security. It can further result in attempts, by government's agencies and its contractors, to undermine modern Internet architecture's standards, such as cryptography and anonymity, in the name of national security and law enforcement.

As a security paradigm that has traditionally been used by the military, the concept of active (or proactive) defense was gradually imported and adapted by companies within the Defense Industrial Base (DIB). The alternative of active defense, in contrast to offensive measures or purely defensive options, allows for a vast range of actions by the security provider – and, consequentially, it also allows a significant range of solutions to be offered in both the commercial and government markets.

The variability of actions allowed by the label grants it a privileged position in the context of public-private partnerships. Adapted to the reality of commercial cyber security, many active defense measures rest, without any harm, within the realm of legality, as in the case of threat intelligence and services like the CSOCs show, whereas government agencies and companies working for them can set forth the original definition to expand active defense's reach. In other words, governments can 'go on the offensive' without openly doing so. The notion of adapting to each kind of threat, promoted in Endgame's strategy, is a constitutive

aspect of active defense and is consistent with how government and the private sector understand the cyber-threat nowadays.

In sum, there is an involvement of defense and intelligence contractors – or other kinds of private actors – in state-sponsored cyber operations mobilized under a paradigm of active defense. This 'dual-use' paradigm can serve both the commercial and the defense cyber security markets and, in both cases, it raises concerns over the expansion of active defense beyond the limits of legality (see DEIBERT; ROHOZINSKI, 2010; DEWAR, 2014).

5.2. Active defense as a security paradigm

Inquiring about the implications of the paradigm of active defense for broader conceptions of security involves recognizing the relevance of cyber security as a security problem. Between the 1990s and the 2000s, the topic went through a process of securitization, moved by the excessive concerns with the impacts of ITs on national and international security. The topic was then introduced to policy and lawmaking and later recognized as a relevant subject within the countries' security agendas (see HANSEN; NISSENBAUM, 2009)

Active defense directly influences the way that security issues in the virtual domain are managed. Working within a risk anticipation orientation, theoretically, it sets forward preventive measures in order to foresee the possibility of an attack and consequentially act before it happens. In practice, it involves detecting, identifying and reacting to an attack through a series of overlapping and sometimes uncoordinated measures involving the measures to perfect the detection, the collection of intelligence about a threat behavior or the attacker, the use of honeypots,[75] bogus DNS entries[76], identifying the attacker's IP, using geolocation, creating fake websites with malware embedded in them, acquiring remote access to an attacker's system and other forms of hacking back. The data gathered through most of these processes can be used later in attempts to prevent future attacks.

[75] A honeypot is a security mechanism that purportedly simulates a computer, system or network security flaws in order to collect information about an attacker.

[76] Also known as DNS hijacking, it corresponds to the subversion of the resolution of Domain Name System (DNS) queries. Such modifications serve malicious activities, such as phishing, but are used by ISPs to redirect the user's web traffic to its servers in order to collect statistics, serve advertisements and other purposes. It can further be used by DNS service providers to censor the access to a given domain.

Some authors have argued that it is necessary to be careful with the use of active defense as a strategy (OVERILL, 2004; DEWAR, 2014). Dewar (2014) considers that it necessarily includes action beyond the defender's immediate network (through hacking back or surveillance). But even if it does not include such an option, it still involves the use of 'security through obscurity' measures, which, according to Anderson's (2001) may have some serious economic consequences, not only by constituting deliberated means of entrenching monopolies, but also by making it harder to distinguish between good and bad products, due to the little information available about their design.

Dewar (2014) notes that given cyberspace's interconnectedness, problems involving the dubious legality of private companies' and state actors' actions in measures undertaken outside the victim's network may become exacerbated if they occur extra-territorially. He notes that, as a security paradigm, active defense employs two methods: a real-time, identification and mitigation of threats in defenders' networks and a capacity to take external, offensive countermeasures.

The paradigm of active defense authorizes the adoption of security measures as a form of risk anticipation. This happens not only through least invasive methods, like 'security through obscurity,' but also fundamentally through threat intelligence and hack backs. The basic of threat intelligence suggests that operation centers act exclusively within the victim's network and that it happens only in the event of an attack, and involves exclusively threat behavior analysis. This isn't necessarily false. But it can be only a part of the story.

If attackers' means and motivations are so diverse as companies and governments stress, resting within the environment of a potential victim won't suffice to prevent the next attack from happening, nor provide an adequate level of intelligence to cast away the possibility of a new attack. A more invasive investigation will eventually be required.

This leads to a correlated issue to active defense: its use as a veiled justification for offensive measures. In practice, the limit between active defense and offensive approaches is very thin. The work has categorized as offensive only those approaches from companies which openly characterized them as such. In this vein, cyber operations and surveillance platforms were the most common solutions within offensive cyber security.

The paradigm of anticipatory security through active defense seems to be rooted on a utopic dream of operating in a cyberspace free from the risk of physical and digital harms. But, contradictorily, this paradigm has to recognize that cyberspace, computer systems and networks, and everything related are inherently risky, so the best one could do would be to try to anticipate to risks. It is almost as if one could conceive of security while aiming for a social world free of any violence.

This utopic, contradictory paradigm influences the form that security takes. It is not so much an objective condition characterized by the absence of dangers, as it is an attempt to exert control over certain kinds of fluxes. To feed the utopia of a riskless cyberspace, anticipatory security invokes every form of control available, prevention included. It escapes market's and technical considerations to become an end in itself. It urges for total surveillance to keep citizens safe, because cyberspace is inherently dangerous and favors criminals and terrorists. Any attempt to control bad fluxes can be validated, and the reach of 'security' keeps expanding. And it is important to be careful with an uncontrolled expansion of the concept of security, because this powerful concept has been used to justify and suspend civil liberties, authorize war-making and massively reallocate resources to the sector being threatened and to all those actors who profit from it.

6. Concluding thoughts

The cyber security market is a complex arrangement where collectivities, in the form of corporations, interact with governments and individuals. It has existed almost in consonance with the diffusion of ICTs beyond the scope of academic and military research, and gained considerable strength since policy-makers realized the possibilities and risks of ICTs. Part of the literature has turned its attention to the illegal market operating underneath the legitimate cyber security market (ABLON et al., 2014; FIDLER, 2014) and the 'gray' market, characterized by legal business transactions between private companies and governments (FIDLER, 2014). Legal and illegal, legitimate or illegitimate, each specter of the market operates in accordance with its own dynamics, but all are backed by an economic logic and sustained by a necessary technical expertise.

Since the Morris worm[77], much has changed in the universe of computer security. The notion of the virtual space as an intrinsically insecure environment became pervasive in the technical and political accounts of the impacts of ICTs in governments' and private actors' daily lives (CSTB, 1991; CSIS, 2008). And in both the political discourse and on the products and solutions offered by private companies, the term "cyber security" came to replace its old-fashioned, technical, cousin "computer security."

Security in cyberspace has become a profitable business. Struggles in this *champ* fuel a multi-billionaire market by increasing the number of perceived insecurities and generating a demand for the market to supply. The practices of private companies become more present and relevant in this social universe to the point that it becomes difficult to disentangle their effects from those of other practices in the *champ*. In theory, it is not so complicated to identify whether a practice is from a think tank or from a government. A policy brief is, generally, a think tank practice, while an official speech by the President or any given law is a government's practice. In reality, though, a policy brief can be very much influenced by market conditions: to reach the conclusion that a certain system has inherent flaws or that a security solution, the antivirus, for example, is not enough to counter newer cyber security risks, a think tank needs to consider the state of the

[77] The Morris Worm (named after its creator, Robert Morris) was one of the first computer worms distributed through the Internet and the first to gain the media's attention.

art of the cyber security market and consider some of the same economic approaches that market actors make when developing their products.

The range of what constitutes a security risk is significantly expanded, sometimes more at the expense of fear than of actual events (BRITO; WATKINS, 2011). Technical risks are combined with risks to security, as is the case of arguments about the security risks of the theft of intellectual property, that marry economics and national security (CSIS, 2008; DENARDIS, 2014).

Early cyber security companies, mostly antivirus companies, were born to address the risks posed by computer worms and viruses. As a response to this evolving technology, malicious codes became increasingly sophisticated. Additionally, with the expansion of the Internet to far beyond its original capacity[78] and with the expansion of mobile connectivity, new categories of risks began to appear, at the same time that the impacts of previous, existent threats, could have a larger reach. What is elusive in this small story about how companies began to address cyber security problems is the dimension the service has acquired when the debate entered policy circles (see DUNN CAVELTY, 2008).

Anchored on reports such as the CSTB's and others, politicians' and security experts' awareness of cyber risks increased and, thus, they started taking preventive and precautionary measures against real events and events in potential (see CSTB, 1991; ARQUILLA; RONFELDT, 1993). The political hype over cyber security called for increased budgetary investments to improve the resilience of the government and private sector's networks, on the one hand, and for preventive measures, on the other. The discourse of prevention became particularly prominent after the 09/11 attacks, with the enmeshment between counterterrorism and cyber security policies (PALLUAULT, 2011; DEIBERT; ROHOZINSKI, 2010).

The possibilities for the cyber security market became wider: if, initially, specialized companies appeared to address the problems posed by computer worms and viruses, something strongly anchored on technical solutions, the dynamics of virtual risks allowed a broader market to operate, something that included these previous players and new players, such as defense contractors or companies

[78] The adoption of the IPv6 protocol to avoid the exhaustion of the previous IPv4 indicates the extent to which the Internet has been expanded. The new protocol will replace IPv4 and allow for 7.9×10^{28} more internet addresses than its predecessor.

specialized in cyber security solutions other than antivirus. Cyber security became a matter of protecting infrastructure and governments against terrorism, combating foreign espionage and preventing cyber-attacks from happening.

In this context, the rationale of 'security' and the participation of the market in it are correlated. The current paradigm of security invites one to view "security" as a commodity, a merchandise (GROS, 2012). Under this paradigm, security has two senses: one related to a state of protection and absence of peril, and the other designating the "entirety of the means of effective protection for people, the system of active threats that makes it possible to avert potential disturbances in a continuing way" (GROS, 2010:280).

Whilst distinct understandings of security have been formulated through the modern era (see GROS, 2012), the security of the network, which informs cyber security, is about securing fluxes. The permeability of the machine is viewed as a risk. And the generalized interconnection, so constitutive of contemporaneity, fuels the paranoia of a planetary catastrophe, extensive to the universe of the networks in the form of major disruptions (GROS, 2012). The main concern of this conceptualization is with assuring the continuity of processes and preventing interruptions of any kind – or, at least, continuously work to prevent it. As Gros (2012) defines, this understanding of security

> Il s'agit cette fois de désigner la continuité d'un processus. Ce sens de la sécurité alors pourra concerner aussi bien des fluxes matériels (numériques, alimentaires, etc.), qu'il faut accompagner a fin d'empêcher les engorgements soudains ou les interruptions brutales (sécurité énergétique, routière, alimentaire), ou bien qu'il s'agit de trier, sélectionner, filtrer, pour interdire d'accès les éléments nocifs (sécurité informatique, sécurite sanitaire) (GROS, 2012:173).

Under the contemporary dynamics of securitization of the virtual space, imperatives of protection, control and regulation (of the flux) take place. And under the imperative of protection are the principles of prevention and precaution. These principles and the ideal of control pursue a logic of permanent requests, in contrast to the antique ideal of internal stability (GROS, 2012). The constant risk of threats, magnified by the inherent vulnerabilities of cyberspace, makes cyber security the 'good' one requests for, a good that, from the beginning was never truly indivisible nor a monopoly of the State (DUNN CAVELTY, 2015). In this sense, distinctly from the security of the state, for example, cyber security is somewhat strange to

the previous logics of war and peace, as it is a child of the paradigm of security, instead of war (GROS, 2010; 2012).

Commodified, cyber security fuels and is fueled by a logic of supply and demand. As the debate on the IoT highlights, the more people and devices get more connected, new forms of system and network exploitation are believed to have deeper and far reaching damages. And the more diversified and complex the real or perceived threats, the more diverse and complex the security solutions offered. Three consequences arise from this. One is that the strong logic of the market, imbued in the provision of cyber security, helps establishing a 'culture of fear' – particularly among government circles, where the concerns about cyber-threats are the most intense. A second consequence is that it leads to a cost-based differentiation in the provision of security. And the efficacy of such provision is also amenable to the amount of money one can pay to have it (GROS, 2012). The free or the most basic versions of products offer little to truly protect the user or the company against the diversity of security threats out there in the Internet. To keep oneself protected, one has to acquire sophisticated, but often quite specialized, security solutions.

The third consequence has not been envisaged in Gros' (2012) analysis and is a particular outcome of the growing participation of the state in cyber security policy making. Because of the peculiar origins of ICTs, the state's involvement in the *champ* has always required a direct involvement with other powerful agents operating in it, as is the case of private companies. As the work has shown, public-private partnerships have been invoked in order to carry on cyber security policies. The perception, by government circles in the U.S., of the operation of ICTs and the expertise about it as roles that belong mainly to the private sector, and the insistent calls to secure cyberspace, have led to the constitution of a diverse set of public-private arrangements. Some are particularly peaceful. Deibert and Rohozinski (2010) argue that, in some cases, businesses are forced to comply with government's demands. But in some cases, they voluntarily do. And in others, they even seek governments with specific products and services to sell, and vice-versa. With the latter example in mind, it should be noted that a particular security-oriented arrangement involving companies willing to commercialize their technical expertise with the security-seeking government, stands out. It is called the cyber security industrial complex.

6.1. The cyber security industrial complex

One immediate consequence of pressures to secure the virtual space enabled by ICTs has been the constitution of a particular arrangement between public entities and private corporations – either traditionally belonging to the field of defense or those new, security-oriented, companies born with the expansion of information technologies. This arrangement is oriented towards the commercialization of a broad set of products and services required by governments, including active-defense solutions, the commercialization of zero-day vulnerabilities, and internet filtering and surveillance technologies (BRITO; WATKINS, 2011).

The cyber security industrial complex is a far reaching enmeshment between the public and the private spheres. It encompasses not only defense companies that traditionally participated in the previous military-industrial complex, but also includes some of the more recent and specialized IT companies working with quite innovative cyber security solutions. What is commercialized in this burgeoning market are solutions to cope with terrorism, cyberwar, the activities of malicious hackers, possible disruptions in critical infrastructure and cyber-crime.

There is a competition between these distinct groups of firms for security contracts with the government, as both IT firms and defense contractors see opportunities to profit from the cyber business (BRITO; WATKINS, 2011). Large security vendors, for example, tend to use the acquisition of highly specialized start-ups and smaller companies as a strategy to gain significant shares of the market. Not only this allows the acquirer a larger market share; as it also adds to its services portfolio some new, disruptive technologies and renovated engineering talent. In addition, the acquisition of innovative start-ups may expand the ties among the private sector and the government, or even create new ones, as some of the newly incorporated companies eventually come with an extra bonus: existent contracts with government agencies (DEIBERT, 2013).

In the context of the cyber security industrial complex, companies not only serve a market for network attack strategies and surveillance techniques: by marketing cyber security solutions and intelligence services to defense and intelligence agencies, they are also creating a new market and new opportunities (DEIBERT, 2011). The government's interest in spending on computer and cyber security solutions is directly influenced by the way that market actors and the

industry reinforce particular frames of cyber threats (BARNARD-WILLS; ASHENDEN, 2012). One example is the perception of an IT market analyst quoted in Brito and Watkins (2011): "It's a cyber war and we're fighting it. In order to fight it, you need to spend more money, and some of the core beneficiaries of that trend will be the security software companies." (BRITO; WATKINS, 2011:69)

The cyber security industrial complex holds an intimate relation to processes of militarization in the West. As U.S. major corporate giants and dozens of niche firms join forces to serve the cyber security market, a global, cyber-offensive oriented market flourishes: "there are enormous profits to be made in developing capabilities to *deny* access to knowledge, prevent networks from functioning, or subvert them entirely. Fibre-optic surveillance and cyberspace disruption is now big business." (DEIBERT, 2013:398)

Intelligence-gathering capabilities advertised by corporations are as good as, or even better than, the government's. And these actors not only design threat signatures, they are also discovering (and commercializing) zero day vulnerabilities (HARRIS, 2014). Harris (2014) contends that some companies today are in position to compete with governments for the "conduct of hostilities" in cyberspace.

The perverse dynamics of the cyber security industrial complex is that it feeds itself of a fear-based hype and, in turn, sells back to the government some products and services that have been used to surpass existent regulations and violate *online* privacy (BRITO; WATKINS, 2011; DEIBERT, 2012; 2013; HARRIS, 2014). This institutional arrangement possibly jeopardizes existent attempts to make cyberspace a more secure environment by both employing techniques that explore the systems' and networks' vulnerabilities in the same fashion that cyber-criminals do and by creating a defense-budget dependent constituency with a wide influence over policy-making, threat-perceptions and strategic interests (see DEIBERT, 2011; 2013).

The existence of the cyber security industrial complex also affects the dynamics of Internet governance. Currently, there is a consensus that it is distributed among numerous stakeholders, which includes governments, private companies, civil society networks and communities of technical experts from multiple countries (DEIBERT; ROHOZINSKI, 2010; MUELLER et al., 2013; DENARDIS, 2014). Technical arrangements are negotiated and established by private corporations and non-governmental entities; and these arrangements are, in

DeNardis' (2014) words, arrangements of power. This involves disputes and deliberations over how to coordinate, manage and shape the Internet to reflect particular policies. Further, the creation and distribution of power among actors in a network is marked more by the constitution of certain "clubs" of governance than by an egalitarian form of organization (MUELLER et al., 2013). These alliances between stakeholders grant them a better position to influence technical arrangements: "actors positioned more centrally within networks, or who seize a first-mover advantage, may be better able to influence the information flows within it." (MUELLER et al., 2013:90).

Cyber security, as a central component of Internet governance, responds to problems concerning user's authentication, CIP, cyber-terrorism, malicious codes, espionage, denial of service attacks, the theft of identity and intellectual property, as well as data interception and modification (DENARDIS, 2014). By carrying out acts of surveillance and espionage, acquiring zero-days for exploitation purposes, developing "cyber arms" and deploying them against state (and possibly non-state) targets, public and private actors enmeshed in the cyber security industrial complex undermine the central components of Internet governance. And, by patronizing new market solutions to some perceived 'cyber insecurities', the risk is that private companies may be purposely feeding a spiral of loosely grounded fear and insecurity.

In addition, this complex also brings to the surface concerns with the accountability of the parties involved, due to the complicated enmeshment between public and private practices. In this context, it becomes tricky to point whether a practice is accountable to a government or to a contractor. Outsourcing is also an attempt made by governments to mitigate risks, but the arrangements born out of this, particularly when they touch sensitive issues, such as data and cyber security, often lack transparency (DEIBERT; ROHOZINSKI, 2010).

As Deibert (2013) notes, it is possible to picture several good reasons for a burgeoning cyber security market. Among these reasons is the efficiency of the private sector's response to the constant need to fend off malicious software. However, when market dynamics and the desire of defense and intelligence agencies (and some companies) to monitor and "strike back" threats marry, perverse dynamics are created: "Securing cyberspace is only a part of the cyber security market: exploiting it, mining it for intelligence, and even propagating

vulnerabilities that undermine and destabilize it are quickly becoming just as lucrative parts of the game." (DEIBERT, 2013:504)

6.1.1. Cyber insecurity beyond the cyber security industrial complex: dealing with a multiplicity of public-private arrangements

The cyber security industrial complex is a phenomenon that has important implications for the effective 'security' of the Internet. This arrangement is a particular result of struggles between agents in the *champ* of cyber security and, as the last section has shown, its role in increasing the overall perception of security in cyberspace is highly questionable. However, disputes among agents also generate other kinds of public-private arrangements that are not always as peaceful for the government-company relations. The cyber security industrial complex generates patterns of cooperation among government and the private sector at the expense of the competition between companies to grab a parcel of the public-sector market. This competition has led to the adoption by companies of aggressive market strategies to gain more space in it and to commercialize specific security solutions, with the market creating some additional needs to protect oneself.

Other distinct arrangements have generated more conflict in the relationship between government agencies and IT companies than the case of the cyber security industrial complex. They often involve less the companies working with cyber security services and more those companies offering a wider range of services, such as ISPs, OSPs, banks and even companies within the cyber risk assessment business. The companies play a less direct role in shaping cyber security, but this role is nonetheless crucial to understand the dynamics of the production of cyber security contemporarily. Whilst these companies were not the primary object of the research, when investigating the dynamics of the *champ*, it became clear that they also played an important and central role in it.

The distinction of these companies in relation to companies working directly with cyber security is that the impacts of their decisions on cyber security is *a priori* less visible. This is because much of the impact they have in the production of cyber security relates to decisions over the development and adoption of certain technical standards in detriment of others. This process of development and adoption of technical standards takes into consideration the market strategy of each company. Apple, for example, is a corporation that values the security of its products. Thus,

it comes as no surprise that vulnerabilities in the iOS system are the most valuable in the exploit market (GREENBERG, 2012). Social networks, in turn, have a relevant part of their revenue coming from advertising. The policy of providing personalized adds based on user's preferences is behind the practices of data and meta-data collection developed and employed by these companies. The data collected is, in turn, requested by governments in many occasions and, more often than not, the companies are obliged to comply with governments solicitations.

Efforts by the NSA to work with IT companies to make products and services 'surveillance-friendly' also show how much political and economic stakes impact the design and administration of technologies. Documents leaked by Edward Snowden show that the agency has spent about $250 million annually to make products design exploitable. The case of Juniper's network breach has exposed the existence of encryption backdoors authored by government agencies – and the extent of the compliance of some companies with this policy.

As it was observed earlier in the work, the infrastructure of this network is owned and operated primarily by the private sector. Because of their size and of user's dependence on these companies, the decisions and policies adopted by them have consequences for policies of privacy and Internet governance. Google, for example, uses lobbying and advocacy activities to support or repudiate certain legislations in attempts to shape public policy according to its commercial interests (see DEIBERT, 2013).

By establishing technical and architectural standards, social media companies wield a growing political power (DENARDIS, 2014). But, to the same extent, they become increasingly subject to the assertion of state power in the Internet. Within their territorial jurisdictions, governments tend to enlist or compel the private sector to police the data they collect and the networks they control and thus empower companies to monitor, filter and control the user's activities *online.* An immediate consequence of this is allowing the growth of new markets for the commercial exploitation of data (DEIBERT, 2013).

As worrisome as the tendency of downloading policing and monitoring responsibilities to the private sector may be, this is an issue where disagreements between private and public agents are strong. The conflict between Apple and the FBI over the use of backdoors to circumvent encryption is a case in point. Companies actively repudiate the excessive intervention of the State in the

operation of their technologies. The Apple case is particularly illustrative because the strength of its operational system has been an important part of the company's market strategy. Whilst the Apple itself does not deny it has complied with FBI's investigations on several occasions (see COOK, 2016), the FBI's request was viewed as a defiance to the trustfulness of the technology that company sells, on one side, and to user's privacy, on the other. The company's position in face of the request granted it the strong support of other companies and pro-privacy groups, highlighting the conflict of interests that has been constitutive of the U.S. government and Silicon Valley relationship.

Closer to the dynamics of the cyber security industrial complex is the relation between government and telecommunication companies and ISPs. The relation between these agents can be located between the gray area of the cyber security industrial complex (because of much of the shared dynamics between the government and such companies, including cooperation for surveillance purposes) and other arrangements, particularly because they don't commercialize cyber defensive/offensive solutions directly. A router company, like Cisco or Juniper, is an Internet chokepoint, a physical point through where the data flow is transmitted. In other words, these companies control parts of the communication flow in cyberspace, they have the power to allow and constrain communications, as well as to enable or constrain governmental surveillance and filtering, which largely depends on the collaboration of these companies. Filtering and censorship in non-democratic countries is a practice which is also enabled by companies born in consolidated democracies and wanting to expand their businesses elsewhere (DEIBERT, 2012; 2013).

To summarize, it is possible to note that in these arrangements, private companies produce cyber security differently. Cyber security companies actively work with protective and offensive measures in cyberspace, but the social media, internet service providers and telecommunication companies shape cyber security through the technical standards they develop and apply in compliance or in conflict with government requests. The U.S. government has been particularly inclined, through either friendly cooperation or legal compliance, to use the power these companies have to enforce law and security in cyberspace. But the impacts of these arrangements extend well beyond the universe of U.S. Internet users.

6.2. The global impacts of struggles in the U.S. *champ*

Although the work considers the dynamics of the cyber security *champ* in the U.S., it is naïve to believe that the practice of agents, or the effects of these practices, are restricted to the universe of U.S. politics. In fact, this *champ* is particularly relevant because of the direct and indirect implications that struggles in it have for how the Internet is experienced around the world.

Domestic political systems arbitrate international developments differently. The regulations that domestic actors issue have an important role in Internet governance, particularly by allowing or constraining practices of control, filtering and surveillance on the Internet (ERIKSSON; GIACOMELLO, 2009). The desire to expand their business to beyond the U.S. and other occidental markets has led many companies to comply with local regulations in several countries with diverse political systems, as non-democratic as they may be.

The case of Google subjecting to the Chinese government restrictions and filtering is good example, but Google is not alone in this. Companies in the cyber security industrial complex commercialize surveillance technologies with non-democratic government with far less legal restrictions than they do with the U.S. companies (see DEIBERT, 2013). In face of the possibilities granted by less democratic markets worldwide, the struggle for an effective parcel of a local market becomes the struggle for a parcel of the global market of cyber security.

This may as well create some frictions with the domestic markets to where these companies are expanding. In Brazil, for example, it is not unlikely for private Internet companies, such as Google and Facebook, to refuse to cooperate with local law enforcement agencies because of existent contractual and legal obligations in the U.S., where their core services and servers are hosted (DINIZ et al., 2014).

Another aspect of the global effects of the practices in the local, U.S. market, has been publicized by Edward Snowden's revelations about the extensive surveillance practices of the NSA. Underlying the actions of the intelligence agency is a complex set of data collection and monitoring practices favored by the will of some companies to commercialize the solutions required by the U.S. government, on the one hand, and by the known or unknown collection of the data collected and stored by social networks and other online service providers, on the other. These

practices reached public authorities worldwide and the population of several countries as well.

The competition for a parcel of the market has led some companies to expand businesses beyond their birthplace. The U.S. is still a valuable market for cyber security and other IT companies, but the Latin-American, and South Asian markets have been seen as providers of great opportunities as well, according to the Cyber Security Ventures market analysis (MORGAN, 2016). But this expansion has been in part driven by the growth of a cyber security industrial complex, when cyber security companies are concerned, and by either the consolidation of public-private arrangements outside the U.S. or by the expansion of U.S. born public-private arrangements beyond the country's jurisdiction, as in the case of NSA's mass surveillance. Additionally, companies willing to expand businesses that still have to observe U.S. regulations can originate serious concerns about what end they give to user's data outside the country. As Deibert (2013) highlights, much of the data collected abroad by these companies is subject to the U.S. Patriot Act, a controversial antiterrorism legislation.

6.2.1. Power, security and internet governance

In terms of Internet governance, the conflictual nature of a large portion of these arrangements between governments and private actors suggests that, in the long term, none of them will actually control the Internet. A "complex pattern of overlapping governance structures", in Dunn Cavelty's (2009b:214) words, still prevails. These structures stem from diverse actors and their different approaches to the Internet, as well as from the power struggles among them.

Currently, it is agreed that the Internet is best governed through a multi-stake-holder approach[79] (see RENDA, 2013; CONTRERAS et al., 2013; COMNINOS, 2013). Issues about the governance of the Internet go beyond the policies and laws enacted by governments' actors, as they involve concerns with the technical design, corporate policies and the role of global institutions in establishing them (CONTRERAS et al., 2013; DENARDIS, 2014). In this sense, what is said and

[79] The multi-stakeholder model is informed by a consensual, bottom-up, decision making process over the Internet Domain System involving distinct, interested parties, which includes businesses, technical experts, the civil society and governments.

done on behalf of cyber security is relevant for how internet governance is understood and conduced in practice, as cyber security measures are established by both technical specificities and corporate policies. The increased securitization of cyberspace is an important factor shaping today's global communications and it may jeopardize the way the Internet is experienced by distinct stakeholders – the civil society included – as certain issues regarding information security and the governance of the Internet (for example, the debates about encryption and Internet control) are also securitized and transformed into national security concerns (COMNINOS, 2013). The relation between Internet governance and cyber security becomes quite clear in Renda's (2013) question over whether the Internet should remain an end-to-end, neutral environment, or if Internet freedom should be sacrificed in the name of security.

According to Nye (2014), Internet governance faces many areas of public and private decision-making. While technical standards related to the Internet protocol are set by engineers involved in non-governmental and non-profit, private entities, the determination as to which of these standards will be applied "depends upon private corporate decisions about their inclusion in commercial products" (NYE, 2014:5). At the same time, the increased involvement of the state in matters of Internet security and governance is associated with the growing pressures to make cyberspace secure, while cybercrime is believed to encourage the involvement of private companies in cyber security (NYE, 2014; DEIBERT; ROHOZINSKI, 2010).

Because of the complex pattern of governance structures that constitute Internet governance, private companies can be as powerful as governments in this arena. But their power is exercised in distinct ways, through the maintenance of the ownership and operation of material and virtual infrastructures, through the definition of technical standards or through direct commercializing cyber security solutions with governments. As Nye (2011) argues, the power over information flows is distributed and agents have distinct resources of power at their disposal.

On one side, companies themselves produce cyber security. Banks develop complex anti-fraud and anti-theft systems to protect their internal networks and customer's transactions, while telecommunication companies implement their own security measures to protect infrastructure (HARRIS, 2014); software developers invest in technologies that protect the data of their users, social networks establish

their own privacy and user policies while cyber risk assessment companies help in shaping perceptions of security and insecurity in the market by analyzing what constitutes a security threat to their commercial and government clients. These companies may willingly or unwillingly attend a state request for the control and filtering of a content or very much comply with surveillance practices.

On the other side, some companies are willing to offer what the government wants – and create some additional needs. They provide cyber defensive and even cyber offensive solutions for government agencies and other companies anxious to avoid unwanted intrusions, that could possibly culminate in the theft of vital information, in their networks. These companies answer to a growing demand for a "secure" cyberspace at the same time they have the power to indicate, themselves, what can constitute a cyber security threat.

In this way, it is necessary to pay attention to the way the cyber security industrial complex poses specific challenges to the governance of the Internet, as it pulls the balance of power towards a more 'centralized' arrangement between government and private companies. The increased development of surveillance technologies, together with offensive and defensive cyber weapons, means that companies are working on new tools to search and store data, to follow real-time movements through geolocalization features. And, in some countries, the use of these technologies may help introducing, legitimizing and normalizing practices of censorship.

What is elusive in the struggles over cyber security is the very logic of security that is applied to them. To keep questioning if it is the government or other kinds of actors the one who controls the Internet (see ERIKSSON; GIACOMELLO, 2009) may help in understanding to what side of the balance the power struggles for the Internet are pending, but it does little to understand the weight of cyber security for the governance of Internet and how agents shape it with their practices, something that directly influences how users experience it. The prevailing logic of security works on the basis of constructing a division over what is safe and what stays at the margins – the black markets, the criminals, the rogue. This working legitimizes practices of 'legit' agents in the *champ* – the state, private companies – to the detriment of illegitimate practices of the wrongdoers, even when the former practices are similar to the latter. The exploitation of vulnerabilities is illustrative of this argument. According to this logic, security is less about guaranties and more

about the permanent evaluation of what constitutes a threat. The logic of the permanent evaluation, in turn, may cast legal guaranties and rights aside when the imminent and constant threat is concerned.

Further, the role of states and private companies in cyber security indicates that more cyber security does not necessarily equate to a better way to counter cyber threats and surveillance. As Comninos and Seneque (2014) argue, the current cyber security discourse has been dominated by a focus of states and corporations on their own security rather than on the security of Internet users and the civil society. This approach to cyber security may, in turn, cast balance of power and most pressing decisions pertaining Internet governance away from civil society and the Internet users' interests.

Unlike computer security, much of what is understood by cyber security to-day is not (exclusively) about assuring the security and integrity of the system, nor the usability of the Internet, but about what results from its promoted marriage with concerns regarding CIP, espionage and cyber-terrorism. The tension between what is done to assure the uninterrupted flow of information *versus* what is done to filter, control and interrupt it seems to be constitutive of this marriage, and it is carried out in the course of the struggles over cyber security. One must, however, be attentive to the way these struggles and the arrangements born out of them have the potential to either increase or jeopardize the equilibrium between the flow of information and the freedom and liberty of the everyday user, and be particular wary of alliances between governments and corporations acting on their own behalf.

6.3. What form of cyber security is desirable?

In contrast with other forms of security, cyber security is peculiar because of its symbiotic relation with the market, since the inception of early information and communication technologies. With the marketization of the Internet, in the 1990s, the role of private actors in shaping security in cyberspace, from the definition of technical security standards and requirements to advertised cyber security solutions, has become even more fundamental. The close relationship between these actors and governments, in turn, has become pivotal for the establishment of national security policies and guidelines concerning cyber security.

The participation of private companies in the production of security is a constitutive aspect of the predominant neoliberal mode of governance that was already strong in the 1970s. For cyber security, the dynamics could not be much different: if, on the one hand, the *champ* has a strong participation of private actors from the beginning, on the other hand, it does not escape from much of the dilemmas posed by this mode of governance – although these dilemmas may gain a different shape in this realm.

A first dilemma is about the patterns of the distribution of power among a diverse set of private entities. The analysis of the *champ* of cyber security under a Bourdieusian framework that has been carried out in this work has shown that the immediate power over the control of information flows is distributed among a diverse group of profit and non-profit private actors. The first group was a more immediate focus of the research because of the visible economic interests invested by them and because of the extent to which these interests are relevant for how they contribute to the production of security.

A more diffused exercise of power by invested actors implicates in more diffused options to make them accountable for the power they exercise. In most cases, IT companies are best held accountable in face of the government of the country in which their servers are located; and their accountability in places where they commercialize their services without necessarily having a physical infrastructure is at best imperfect, often marked by conflicts between their contractual obligations in the host countries *versus* the legal obligations they should comply with in foreign countries. Accountability becomes even more difficult in cases where private companies orient themselves to serve national security interests, as it happens with the cyber industrial complex alliance. As this chapter has shown, such marriage between economic and security interests can be nothing but worrisome for the way people currently experience the Internet.

Companies act first and foremost in accordance with their economic interests. While it is undeniable that the particular constitution of IT companies by computer experts and engineers grants their structure more flexibility and broader goals in some cases – such as concerns with data privacy, the resilience of systems and so on –, the dynamics of funding and eventual arrangements in the structure of most companies places profit as a first priority. But, as an indissociable part of the private enterprise nature, some economic ends may adjust very awkwardly to actual

security problems. With their risk-oriented mindset, so common under the current paradigm of security (see GROS, 2012), companies define security on the basis of a permanent evaluation rather than in terms of guaranties.

This evaluation takes into account the most immediate (perceived) threats to physical and digital infrastructure that could possibly affect governments and companies – and, by consequence, citizens. The CIP/CIIP arguments, with all the fear of great disruptions by criminals and terrorists, bring biopolitics to the core of cyber security and have played an important role in the legitimation of cyber security policies (including budgets), in the political sphere. As citizens are portrayed as being threatened by the very risks that haunt companies' operations *online*, cyber security becomes an urgent security matter.

The power exerted by private companies becomes particularly dangerous when unchecked and a-problematically submitted to the security interests of governments. If governments are the ones responsible for making companies accountable, one has to wonder what happens when their interests converge at the expense of the legal guaranties of the citizens. As Gros (2012) has argued, security policies are constructed on the basis of a differentiation between what is secure and what remains in the gray area of insecurity, the unsafe. For the most part of the time, this is an arbitrary decision or a result of power struggles and alliances between invested actors.

No wonder why some authors have been emphasizing the importance of adopting a "distributed approach" to cyberspace security (DEIBERT, 2012; 2013). They are worried with the possible implications of the arrangements that have been constituted as a result of the cyber security hype. A distributed approach is anchored on the notion that it is necessary to check the concentration of power domestically, in order to increase the trustfulness of a political entity internationally. It involves the combination of multiple actors with shared governance roles and responsibilities in such a way that none of these actors may effectively control cyberspace without cooperating with the others. This involves the participation not only of private companies and governments, but of citizens and the civil society as well: "Securing cyberspace requires a reinforcement of, rather than relaxation of restraint on power, including checks and balances on governments, law enforcement and intelligence agencies as well as the private sector." (DEIBERT, 2012:273).

Roughly speaking, the participation of citizens in the process of securing cyberspace has been lacking in much of current cyberspace governance. It is almost derisive. The civil society has made itself more present in the virtual universe, but the individual itself is still viewed as a mere user, due to the lack of technical expertise, which has been pointed in chapter one as a *sine qua non* condition to enter disputes in the *champ* of cyber security. This is a barrier that makes cyberspace less democratic and places the burden of cyber insecurity at the shoulders of the end-user, which rests powerless to decide important aspects of security and governance at the same time it is directly affected by the dynamics of struggles in the *champ*.

7. References

ABELE-WIGERT, I.; DUNN, M. **International CIIP Handbook 2006:** an Inventory of 20 National and 6 International Infrastructure Protection Policies. Zurich: Center for Security Studies, v. 1, 2006.

ABLON, L.; LIBICKI, M. C.; GOLAY, A. A. **Markets for Cybercrime Tools and Stolen Data:** Hackers' Bazaar. Santa Monica: RAND Corporation , 2014.

ABRAHANSEM, R.; WILLIAMS, M. Security Beyond the State: Global Security Assemblages in International Politics. **International Political Sociology** , 3, 2009. 7-17.

ABRAHANSEN, R.; LEANDER, A. **Routledge Handbook of Private Security Studies**. Abingdon: Routledge, 2016.

ACKERMAN, S. US tech giants knew of NSA data collection, agency's top lawyer insists. **The Guardian**, 19 March 2014. Access 6 February 2016.

ACKERMAN, S. NSA and FBI fight to retain spy powers as surveillance law nears expiration. **The Guardian**, 15 April 2015. Available at: <http://www.theguardian.com/us-news/2015/apr/15/nsa-fbi-surveillance-patriot-action-section-215-expiration>. Access 5 February 2016.

ADAMS, W. The Military-Industrial Complex and the New Industrial State. **The American Economic Review, Papers and Proceedings of the Eightieth Annual Meeting of the American Economic Association**, 58, n. 2, May 1968. 652-665.

ADLER, E.; POULIOT, V. International practices. **International Theory**, 3, n. 1, 2011. 1-36.

ADLER-NISSEN, R. **Bourdieu in International Relations:** rethinking key concepts in IR. New York: Routledge, 2013.

ALBERTS, D. S.; PAPP, D. S. (Eds.). **The Information Age:** An Anthology on Its Impact and Consequences. Washington DC: CCRP Publication Series, 1997.

ALBERTS, D. S.; PAPP, D. S.; KEMP III, T. W. Historical Impacts of Information Technologies: An Overview. In: ALBERTS, D. S.; PAPP, D. S. **The Information Age:** An Anthology on Its Impact and Consequences. CCRP Publication Series, 1997. p. 13-34.

ANDERSON, R. **Why information security is hard - an economic perspective**. 17th Annual Computer Security Applications Conference (ACSAC'01). IEEE Computer Society. December, 2001.

ANDERSON, R. H. **Risks to the U.S Infrastructure from Cyberspace**. Santa Monica: RAND, 1996.

ANDERSON, R. H. et al. **Securing the U.S. Defense Information Infrastructure:** A Proposed Approach. Santa Monica: RAND, 1999.

ARADAU, C. Security That Matters: Critical Infrastructures and Objects of Protection. **Security Dialogue**, 41, n. 5, October 2010. 491-514.

ARADAU, C.; LOBO-GUERRERO, L.; MUNSTER, R. V. Security, Technologies of Risk, and the Political: Guest Editors' Introduction. **Security Dialogue**, 39, n. 2-3, 2008. 147-154.

ARQUILLA, J.; RONFELDT, D. **Cyberwar Is Coming!** Santa Monica: RAND Corporation, 1993.

ASHLEY, R. Untying the Sovereign State: A Double Reading of the Anarchy Problem. **Millennium - Journal of International Studies**, 17, n. 2, May 1988. 227-262.

AVANT, D. Private security companies. **New Political Economy**, 10, n. 1, 2005. 121-131.

AVAST SOFTWARE INC. **Avast! Download Free Antivirus for PC, Mac & Android**, 2016. Available at: <https://www.avast.com>. Access 20 feb. 2016.

AVIRA. Avira 2016 - Donwload the free antivirus for PC & Mac, 2016. Available at: <https://www.avira.com/>. Access 24 feb. 2016.

BAE SYSTEMS, 2016. Available at: <http://www.baesystems.com/en/home?r=BR>. Access: 20 feb. 2016.

BALL, K.; HAGGERTY, K. D.; LYON, D. **Routledge Handbook of Surveillance Studies**. London: Routledge, 2012.

BALL, K.; SNIDER, L. E. (Eds.). **The surveillance-industrial complex. A political economy of surveillance**. Abington UK/New York: Routledge, 2013.

BALZACQ, T. A theory of securitization: origins, core assumptions, and variants. In: _____ **Securitization theory:** how security problems emerge and dissolve. New York: Routledge, 2011.

BALZACQ, T. et al. Security Practices. In: DENEMARK, R. A. **International Studies Encyclopedia Online**. [S.l.]: Blackwell, 2010. Available at: <http://www.isacompendium.com/subscriber /tocnode?id=g9781444336597_chunk_g978144433659718_ss1-2>. Access: 25 dec. 2015.

BARAJAS, O. How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape. **Security Intelligence**, p. 17, September 2014. Available at: <https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/>. Access: 20 January 2016.

BARNARD-WILLS, D.; ASHENDEN, D. Securing Virtual Space: Cyber War, Cyber Terror and Risk. **Space and Culture**, 15, n. 2, 2012. 110-123.

BARRET, D. FBI Fears Loss of Surveillance Tools in Patriot Act. **The Wall Street Journal**, 4 February 2015. Available at: <http://www.wsj.com/articles/fbi-fears-

loss-of-its-surveillance-tools-in-patriot-act-1423091243>. Access: 4 February 2016.

BAUMAN, Z. et al. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, 8, 2014. 121–144.

BECK, U. **Risk Society:** Towards a New Modernity. London: Sage, 1992.

BELLANOVA, R. Data protection, with love. **International Political Sociology**, 8, n. 1, 2014. 112-115.

BENDRATH, R. The American cyber-angst and the real world - any link? In: LATHAM, R. **Bombs and Bandwidth:** the emerging relationship between information technology. New York: The New Press, 2003. p. 49-73.

BENDRATH, R.; ERIKSSON, J.; GIACOMELLO, G. From 'cyberterrorism' to 'cyberwar', back and forth: How the United States securitized cyberspace. In: ERIKSSON, J.; GIACOMELLO, G. **International Relations and Security in the Digital Age**. New York: Routledge, 2007. p. 57-82.

BERLING, T. V. Bourdieu, International Relations, and European Security. **Theory and Society**, 41, 2012. 451–478.

BERLING, T. V. Knowledges. In: ADLER-NISSEN, R. **Bourdieu in International Relations:** Rethinking Key Concepts in IR. London: Routledge , 2013. p. 59-77.

BERNDTSSON, J.; STERN, M. Private Security and the Public-Private Divide: Contested Lines of Distinction and Modes of Governance in the Stockholm-Arlanda Security Assemblage. **International Political Sociology**, 5, 2011. 408-425.

BETZ, D. J.; STEVENS, T. **Cyberspace and the State:** Toward a Strategy for Cyber-power. New York: Routledge , 2011.

BEVIR, M. **Key Concepts in Governance**. New York: SAGE, 2009. 128-132 p.

BIGO, D. Border Regimes, Police Cooperation and Security in an Enlarged European Union. In: ZIELONKA, J. **Europe Unbound. Enlarging and Reshaping the Boundaries of the European Union**. London: Routledge, 2002. p. 213-239.

BIGO, D. La Mondialisation de la (In)sécurité? **Cultures & Conflits**, 58, 2005. 53-101. Available at: <http://conflits.revues.org/1813>. Access: 20 dec. 2015.

BIGO, D. Security, Surveillance and Democracy. In: BALL, K.; HAGGERTY, K.; LYON, D. E. **The International Handbook of Surveillance Studies**. London: Routledge, 2011a.

BIGO, D. Pierre Bourdieu and International Relations: Power of Practices, Practices of Power. **International Political Sociology**, 5, n. 3, 2011b. 225-258.

BIGO, D. Security: analysing transnational professionals of (in)security in Europe. In: ADLER-NISSEN, R. **Bourdieu in International Relations:** rethinking key concepts of IR. New York: Routledge, 2013. p. 114-130.

BIGO, D. International Political Sociology: Internal security as transnational power fields. In: RHINARD, M.; BOSSONG, R. **Theorising Internal Security Cooperation in the European Union**. Oxford: Oxford University Press, 2015. Forthcoming.

BILGE, L.; DUMITRAS, T. Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World. **Symantec Research Labs**, Raleigh, 2012.

BIPARTISAN POLICY CENTER. **Cyber Security Task Force: Public-Private Information Sharing**. Bipartisan Policy Center Homeland Security Project. Washington DC. 2012.

BITDEFENDER. **Bitdefender Antivirus Software**, 2016. Available at: <http://www.bitdefender.com/?ctrsel=1>. Access: 24 feb. 2016.

BOEING. Cybersecurity & Information Management. **Boeing**, 2016. Available at: <http://www.boeing.com/defense/cybersecurity-information-management/>. Access: 20 feb. 2016.

BOOTH, K. **Theory of world security**. Cambridge: Cambridge University Press, 2007.

BOOTH, K.; WHEELER, N. **The security dilemma:** fear, cooperation and trust in world politics. New York: Palgrave MacMillan, 2008.

BOOZ ALLEN. Strategy and Technology Consulting Firm. **Booz Allen Hamilton**, 2016. Available at: <http://www.boozallen.com/>. Access: 05 feb. 2016.

BOURDIEU, P. Vive la crise! For heterodoxy in social science. **Theory and Society**, 17, 1988. 773-787.

BOURDIEU, P. **In other words:** essays towards a reflexive sociology. Cambridge: Polity Press, 1990.

BOURDIEU, P. **The Field of Cultural Production**. Cambridge: Polity Press, 1993.

BOURDIEU, P. **Practical Reason:** On the Theory of Action. Stanford: Stanford University Press, 1998.

BOURDIEU, P. **Science of science and reflexivity**. Cambridge: Polity Press, 2004.

BOURDIEU, P. **Sobre o Estado**. São Paulo: Companhia das Letras, 2014.

BOURDIEU, P.; WACQUANT, L. **Réponses:** Pour une anthropologie réflexive. Paris: Éditions du Seuil, 1992.

BRITO, J.; WATKINS, T. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. **Harvard National Security Journal**, 3, 2011. 39-84.

BRUNEAU, T. C. The US experience in contracting out security and lessons for other countries. **Revista Brasileira de Política Internacional**, Brasília, 58, n. 1, 2015. 230-248.

BUEGER, C.; GADINGER, F. The Play of International Practice: Minimalism, Pragmatism and Critical Theory. **International Studies Quarterly**, 59, n. 3, 2015. 1-12.

BUZAN, B.; HANSEN, L. **The Evolution of International Security Studies**. Cambrigde: Cambridge University Press, 2009.

BUZAN, B.; WAEVER, O.; WILDE, J. **Security:** a New Framework for Analysis. London: Lynne Rienner Publishers, 1998.

CAMERON, D. Pentagon to Open Silicon Valley Office, Provide Venture Capital. **The Wall Street Journal**, 23 April 2015. Available at: <http://www.wsj.com/articles/pentagon-to-open-silicon-valley-office-provide-venture-capital-1429761603>. Access: 3 February 2016.

CARAFANO, J. The New Arms Race Is About Bytes, Not Bombs. **The Daily Signal**, February 2015. Available at: <http://dailysignal.com//2015/02/08/the-new-arms-race-is-about-bytes-not-bombs/>. Access: 27 dec. 2015.

CASTELLS, M. **A Galáxia da Internet**. Rio de Janeiro: Zahar, 2001.

CASTELLS, M. **The rise of the network society**. 2. ed. Malden: Blackwell, v. 1, 2010.

CASTELLS, M. **The rise of the network society**. Oxford: Wiley-Blackwell, 2010.

CHERNOFF, F. **Theory and metatheory in international relations:** concepts and contending accounts. New York: Palgrave MacMillan , 2007.

CHOMSKY, N. War Crimes and Imperial Fantasies. **International Socialist Review**, v. 37, September–October 2004. Available at: <http://www.isreview.org/issues/37/chomsky.shtml>. Access: 06 jan. 2016.

CLARKE, R. A.; KNAKE, R. **Cyber War:** The Next Threat to National Security and What to Do About It. New York: Ecco, 2010.

COLLIER, S. J.; LAKOFF, A. The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem. In: DUNN, M.; KRISTENSEN; S., K. **The Politics of Securing the Homeland:** Critical Infrastructure, Risk and Securitisation. New York: Routledge, 2008.

COMMISION, E. The Internet of Things. **Digital Single Market: Digital Economy and Society**, 2016. Available at: <https://ec.europa.eu/digital-single-market/en/internet-things>. Access: 05 apr. 2016.

COMNINOS, A. A Cyber Security Agenda For Civil Society: What is at Stake? **APC Issue Papers**, p. 1-12, April 2013.

COMNINOS, A.; SENEQUE, G. Cyber security, civil society and vulnerability in an age of communications surveillance. **Global InformatIon Society Watch 2014: Communications surveillance in the digital age**, p. 32-40, 2014.

COOK, T. A Message to Our Customers. **Apple**, 2016. Available at: <http://www.apple.com/customer-letter/>. Access: 05 mar. 2016.

CONTRERAS, J. L.; DENARDIS, L.; TEPLINSKY, M. Mapping Today's Cybersecurity Landscape. **American University Law Review**, 62, n. 5, 2013. 1113-1130.

CROUCH, C. Markets and States. In: NASH, K.; SCOTT, A. E. **The Blackwell Companion to Political Sociology**. Oxford: Blackwell, 2004. p. 240-249.

CSIS. **Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency**. Center for Strategic and International Studies. Washington DC, p. 90. 2008.

CSIS. **Cybersecurity two years later:** a report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington DC: Center for Strategic and International Studies, 2010.

CSIS. **Cybersecurity Two Years Later:** a Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington DC: Center for Strategic and International Studies, 2011.

CSTB. **Computers at Risk:** Safe Computing in the Information Age. Washington DC: National Academy Press, 1991. System Security Study Committee, Computer Science and Telecommunications Board.

CURRIER, C.; MARQUIS-BOIRE, M. Leaked Documents Show FBI, DEA and U.S. Army Buying Italian Spyware. **The Intercept**, July 2015. Available at: <https://theintercept.com/2015/07/06/hacking-team-spyware-fbi/>. Access: 05 feb. 2016.

CYBERSECURITY VENTURES. Cybersecurity market report. Available at: <http://cybersecurityventures.com/cybersecurity-market-report/>. Access: 2 February 2016.

DAY, R. E. **The Modern Invention of Information:** Discourse, History and Power. Carbondale: Southern Illinois University Press, 2001.

DE GOEDE, M. The Politics of Privacy in the Age of Preemptive Security. **International Political Sociology**, 8, 2014. 100–118.

DEIBERT, R. Ronald Deibert: Tracking the emerging arms race in cyberspace. **Bulletin of the Atomic Scientists**, 67, n. 1, 2011. 1-8.

DEIBERT, R. Tracking the emerging arms race in cyberspace. **Bulletin of the Atomic Scientists**, v. 67, n. 1, p. 1-8, 2011.

DEIBERT, R. The Growing Dark Side of Cyberspace (and What To Do About It). **Penn State Journal of Law & International Affairs**, 1, n. 2, 2012. 260-274.

DEIBERT, R. **Black Code:** inside the battle for cyberspace. Oxford: Signal, 2013.

DEIBERT, R. J.; ROHOZINSKI, R. Risking Security: Policies and Paradoxes of Cyberspace Security. **International Political Sociology**, 4, 2010. 15-32.

DEIBERT, R.; ROHOZINSKI, R. Risking security: Policies and paradoxes of cyberspace security. **International Political Sociology**, 4, n. 1, 2010a. 15-32.

DENARDIS, L. **The Global War for Internet Governance**. New Haven: Yale University Press, 2014.

DENNING, D. E. Cyber-security as an Emergent Infrastructure. In: LATHAM, R. **Bombs and bandwidth:** the emerging relationship between information technology and security. New York: The New Press, 2003. p. 25-48.

DENNING, D. E. Framework and principles for active cyber defense. **Computers & Security**, 40, February 2014. 108-113.

DEVETAK, R. Critical theory. In: BURCHILL, S., et al. **Theories of International Relations**. 3. ed. New York: Palgrave MacMillan, 2005. p. 137-160.

DEWAR, R. S. The "Triptych of Cyber Security": A Classification of Active Cyber Defence. **2014 6th International Conference on Cyber Conflict**, Tallin , 2014. Available at: <https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf>. Access: 01 apr. 2016.

DHS. Cyber Security Overview, 2015. Available at: <https://www.dhs.gov/cybersecurity-overview>. Access: 29 dec. 2015.

DHS. **Homeland Security Budget-in-Brief:** Fiscal Year 2016. [S.l.]: [s.n.], 2015. Available at: <https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf>. Access: 26 feb. 2016.

DHS. Cybersecurity. **Homeland Security**, 2016. Available at: <http://www.dhs.gov/topic/cybersecurity>. Access: 30 January 2016.

DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil: Threats and responses. **Igarapé Institute Strategic Paper 11**, December 2014.

DITTRICH, D.; HIMMA, K. E. Active Response to Computer Intrusions. In: HOSSEIN, B. E. **The Handbook of Information Security**. Hoboken: John Wiley & Sons, 2005.

DOD. The Department of Defense Cyber Strategy. **US Department of Defense**, 2016. Available at: <http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy>. Access: 30 January 2016.

DOHERTY, S. et al. Hidden Lynx – Professional Hackers for Hire. **Security Response**, Symantec, September 2013.

DUNN CAVELTY, M. **Information Age Conflicts:** A Study of the Information Revolution and a Changing Operating Environment. Zürich: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse ETH , 2002.

DUNN CAVELTY, M. The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP). **International Journal for Critical Infrastructure Protection**, 1, n. 2, 2005. 258-268.

DUNN CAVELTY, M. Critical Infrastructures: Vulnerabilities, Threats, Responses. **CSS Analysis in Security Policy**, n. 16, 2007.

DUNN CAVELTY, M. **Cyber-Security and Threat Politics:** US Efforts to Secure the Information Age. London: Routledge, 2008.

DUNN CAVELTY, M. Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory. In: ERIKSSON, J.; GIACOMELLO, G. E. **International Relations and Security in the Digital Age**. New York: Routledge, 2009a. p. 85-105.

DUNN CAVELTY, M. National Security and the Internet: Distributed Security through Distributed Responsibility. **International Studies Review - The Forum**, 11, 2009b. 205–230.

DUNN CAVELTY, M. The Militarisation of Cyberspace: Why Less May Be Better. **4th International Conference on Cyber Conflicts**, 2012. 141-153.

DUNN CAVELTY, M. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber Security Discourse. **International Studies Review**, 15, 2013. 105-122.

DUNN CAVELTY, M. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. **Science and Engineering Ethics**, 20, n. 3, 2014. 701-715.

DUNN CAVELTY, M. The Normalization of Cyber-International Relations. In: THRÄNERT, O.; ZAPFE, M. E. **Strategic Trends 2015:** Key Developments in Global Affairs. [S.l.]: CSS, 2015.

DUNN CAVELTY, M. Cyber-security and private actors. In: ABRAHANSEM; R.; LEANDER, A. E. **Routledge Handbook of Private Security Studies**. New York: Routledge, 2016.

DUNN CAVELTY, M. D. Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate. **Military and Strategic Affairs**, 3, n. 3, dec. 2011.

DUNN CAVELTY, M.; BRUNNER, E. Information, Power, and Security – An Outline of Debates and Implications. In: CAVELTY, D., et al. **Power and Security in the Information Age:** Investigating the Role of the State in Cyberspace. Aldershot: Ashgate, 2007. p. 1-8.

DUNN CAVELTY, M.; JAEGER, M. D. In(Visible) Ghosts in the Machine and the Powers that Bind: The Relational Securitization of ‘Anonymous. **International Political Sociology**, 9, n. 2, June 2015. 176-194.

DUNN CAVELTY, M.; SUTER. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. **International Journal of Critical Infrastructure Protection**, 2, 2009. 179-187.

DUNN, J. E. Antivirus is 'dead' says Symantec security head as firm launches more services and cloud security. **Tech World**, 06 May 2014. Available at: <http://www.techworld.com/news/security/antivirus-is-dead-says-symantec-security-head-as-firm-launches-more-services-cloud-security-3515066/>. Access: 05 jan. 2016.

DUNNE, J. P.; SKÖNS, E. The Changing Military Industrial Complex. **No 1104, Working Papers from Department of Accounting, Economics and Finance**, Bristol, 2011.

EICHLER, M. Private Security and Gender. In: ABRAHANSEN, R.; LEANDER, A. E. **Routledge Handbook of Private Security Studies**. London : Routledge, 2016. p. 158-166.

EISENHOWER, D. D. Military-Industrial Complex Speech, Dwight D. Eisenhower, 1961. **Public Papers of the Presidents**, 1961. Available at: <http://coursesa.matrix.msu.edu/~hst306/documents/indust.html>. Access: 06 jan. 2016.

ELIAS, N. **The Civilizing Process**. Oxford: Blackwell, 2000.

ENDGAME. Endgame, 2016. Available at: <https://www.endgame.com/>. Access: 28 mar. 2016.

ERIKSSON, J.; GIACOMELLO, G. The Information Revolution, Security, and International Relations: (IR)relevant Theory? **International Political Science Review**, 27, n. 3, 2006. 221–244.

ERIKSSON, J.; GIACOMELLO, G. **International Relations and Security in the Digital Age**. New York: Routledge, 2007.

ERIKSSON, J.; GIACOMELLO, G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. **International Studies Review**, 11, 2009. 205-230.

EVANS, D. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. **White Paper. Cisco Internet Business Solutions Group**, 2011.

EWALD, F. The Return of Descastes's Malicious Demon: An Outline of a Philosophy of Precaution. In: BAKER, T.; SIMON, J. E. **Embracing Risk:** The Changing Culture of Insurance and Responsibility. Chicago: Chicago University Press, 2002. p. 273-302.

FBI. FBI - Cyber Crime. **The Federal Bureau of Investigation**, 2016. Available at: <https://www.fbi.gov/about-us/investigate/cyber>. Access: 28 January 2016.

FIDLER, M. **Anarchy or Regulation:** Controlling the Global Trade in Zero-Day Vulnerabilities. [S.l.]: [s.n.], 2014. 195p. p. Thesis (Center for International

Security and Cooperation Freeman Spogli Institute for International Studies, Stanford University.

FINIFTER, M.; AKHAWE, D.; WAGNER, D. An Empirical Study of Vulnerability Rewards Programs. **22nd USENIX Security Symposium** , Berkeley, CA, 2013.

FIRE EYE. Cyber Security & Malware Protection. **FireEye**, 2016. Available at: <https://www.fireeye.com/>. Access: 24 feb. 2016.

FIREEYE. Security Reimagined, Part 1: An Adaptive Approach to Cyber Threats for the Digital Age. **FireEye**, 2015. Available at: <https://www2.fireeye.com/security-reimagined-part1.html>. Access: 01 mar. 2016.

FOUCAULT, M. **Security, territory, population:** lectures at the Collège de France, 1977-78. New York: Palgrave MacMillan, 2007.

FRIEDMAN, J.; BOUCHARD, M. **Definitive Guide to Cyber Threat Intelligence:** Using Knowledge about Adversaries Win the War against Targeted Attacks. Anapolis: CyberEdge Group, LLC, 2015. iSIGHTPartners.

GALLAGHER, R. Software that tracks people on social media created by defence firm. **The Guardian**, 10 February 2013. Available at: <http://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence>. Access: 28 mar. 2016.

GALLAGHER, R.; GREENWALD, G. How the NSA plans to infect 'millions' of computers with malware. **The Intercept**, 12 March 2014. Access: 2 February 2016.

GAO. **Cyber Security for Critical Infrastructure Protection**. Washington DC: [s.n.], 2004. Available at: <http://www.gao.gov/new.items/d04321.pdf>. Access: 01 apr. 2016.

GAO. Key Issues: Cybersecurity, 2016. Available at: <http://www.gao.gov/key_issues/cybersecurity/issue_summary#t=0>. Access: 20 January 2016. US Government Accountability Office.

GARCIA, M.; STEINBACH, T.; KRAMER, L. A Proposed Cyber Initiative: The State of the Field and Hewlett's Potential Impact. **The William and Flora Hewlett Foundation Memorandum**, p. 1-11, March 2014.

GENERAL DYNAMICS. **General Dynamics**, 2016. Available at: <http://www.gd.com/>. Access: 20 feb. 2016.

GLOSSON, A. D. Active Defense: An Overview of the Debate and a Way Forward. **Mercatus Working Paper**, Arlington, August 2015.

GOLDSMITH, J.; WU, T. **Who Controls the Internet? Illusions of a borderless world**. Oxford: Oxford University Press, 2006.

GREENBERG, A. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. **Forbes**, March 2012. Available at:

<http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#31fa26616033>. Access: 20 feb. 2016.

GREENBERG, A. Inside Endgame: A Second Act For The Blackwater Of Hacking. **Forbes**, February 2014. Available at: <http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/#5fcd3e6052d9>. Access: 05 feb. 2016.

GREENBERG, A.; ZETTER, K. How the Internet of Things Got Hacked. **Wired**, 28 December 2015. Available at: <http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/>. Access: 20 January 2016.

GROS, F. **States of Violence:** an essay on the end of war. London: Seagull Books, 2010.

GROS, F. **Le Principe Sécurité**. Paris: Gallimard, 2012.

GRUMMAN, N. Trusted Solutions. **Northrop Grumman**, 2016. Available at: <http://www.northropgrumman.com/Capabilities/Cybersecurity/Pages/default.aspx>. Access: 28 mar. 2016.

GUZZINI, S. **Realism in International Relations and International Political Economy - The Continuing Story of a Death Foretold**. New York: Routledge, 1998.

HACKETT, R. No, NSA Has Not Changed Stance on Encryption. **Fortune**, 23 January 2016. Available at: <http://fortune.com/2016/01/23/nsa-rogers-encryption-stance/>. Access: 2 February 2016.

HACKING TEAM. **HackingTeam**, 2016. Available at: <http://www.hackingteam.it/>. Access: 23 feb. 2016.

HANSEN, L.; NISSENBAUM, H. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, 53, 2009. 1155–1175.

HARRINGTON, S. L. Cyber Security Active Defense: Playing with Fire or Sound Risk Management? **Richmong Journal of Law & Technology**, 12, 2014. Available at: <http://jolt.richmond.edu/v20i4/article12.pdf>. Access: 01 apr. 2016.

HARRIS, S. **@War:** the rise of the military-internet complex. Boston: Houghton Mifflin Harcourt, 2014.

HARTUNG, W. D. **Prophets of War:** Lockheed Martin and the Making of the Military-Industrial Complex. New York: Nation Books, 2011.

HASSAN, Q. F. Demystifying Cloud Computing. **Cross Talk**, p. 16-21, January-February 2011. Available at: <http://static1.1.sqspcdn.com/static/f/702523/10181434/1294788395300/201101-Hassan.pdf?token=c64hDS998vDx7adR2u0yARM3HO4%3D>. Access: 26 January 2016.

HERN, A. Apple's encryption means it can't comply with US court order. **The Guardian**, 8 September 2015. Available at: <http://www.theguardian.com/technology/2015/sep/08/apple-encryption-comply-us-court-order-iphone-imessage-justice>. Access: 2 February 2016.

HERZ, J. Idealist Internationalism and the Security Dilemma. **World Politics**, 2, n. 2, January 1950. 157-180.

HOBSON, J. M. **The State and International Relations**. Cambridge: Cambridge University Press, 2003.

HOVEN, J. V. D.; WECKERT, J. **Information technology and moral philosophy**. Cambridge: Cambridge University Press, 2008.

HUYSMANS, J. Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe. **European Journal of International Relations**, 4, n. 4, 1998. 479-505.

INFORMATION WEEK. Offensive Cybersecurity: Theory And Reality. **Information Week**, 21 January 2013. Available at: <http://www.informationweek.com/government/cybersecurity/offensive-cybersecurity-theory-and-reality/d/d-id/1108269?>. Access: 20 mar. 2016.

INTEL SECURITY. Antivirus, Encryption, Firewall, Email Security, Web Security, Network Security. **Intel Security - McAfee**, 2016. Available at: <http://www.mcafee.com/us/index.html>. Access: 25 feb. 2016.

INTELLIGENCE CAREERS. Jobs in the U.S. intelligence community, 2016. Available at: <https://www.intelligencecareers.gov/>. Access: 15 feb. 2016.

ITU. Overview of Cyber Security. **Recommendation ITU-T X.1205**, 2008.

ITU. **Overview of the Internet of things. Recommendation ITU-T Y.2060**. [S.l.]: [s.n.], 2012. Available at: <http://handle.itu.int/11.1002/1000/11559>. Access: 25 January 2016. International Telecommunications Union.

JACKSON, P. Pierre Bourdieu, the "Cultural Turn" and the practice of international history. **Review of International Studies**, 1, n. 34, 2008. 155-181.

JORDAN, T. **Cyberpower:** the Culture and Politics of Cyberspace and the Internet. New York: Routledge, 1999.

KARATZOGIANNI, A. (Ed.). **Cyber Conflict and Global Politics**. London: Routledge, 2009.

KASPERSKY LAB. Internet security center. **Kaspersky lab**, 2015. Available at: <http://www.kaspersky.com/internet-security-center>. Access: 23 dec. 2015.

KASPERSKY LAB. Antivirus Protection & Internet Security Software. **Kaspersky Lab US**, 2016. Available at: <http://usa.kaspersky.com/>. Access: 25 feb. 2016.

KASSNER, M. Endpoint security: What makes it different from antivirus solutions. **TechRepublic**, March 2012. Available at: <http://www.techrepublic.com/blog/it-

security/endpoint-security-what-makes-it-different-from-antivirus-solutions/>. Access: 10 feb. 2016.

KELLMEREIT, D.; OBODOVSKI, D. **The Silent Intelligence:** the Internet of Things. San Francisco: DND Ventures , 2013.

KEOHANE, R. O.; NYE, J. S. Power and Interdependence in the Information Age. **Foreign Affairs**, September/October 1998. Available at: <https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age>. Access: 30 dec. 2015.

KEOHANE, R.; NYE, J. Power and Interdependence Revisited. **International Organization**, 41, n. 4, 1987. 725-753.

KEOHANE, R.; NYE, J. Power and interdependence in the information age. **Foreign Affairs**, v. 77 , n. 5, September-October 1998.

KEOHANE, R.; NYE, J. Power and Interdependence in the Information Age. **Foreign Affairs**, v. 77, n. 5, p. 81-94, September/October 1998. Available at: <https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age>. Access: 30 dec. 2015.

KITCHIN, R.; DODGE, M. **Code/Space:** software and everyday life. Cambridge MA: The MIT Press, 2011.

KRAUSE, K. Critical theory and security studies: the research programme of 'critical security studies'. **Cooperation and Conflict**, 33, 1998. 298-333.

KRAUSE, K.; WILLIAMS, M. C. **Critical security studies:** concepts and cases. Minneapolis : University of Minnesota Press, 1997.

LATHAM, R. (Ed.). **Bombs and Bandwidth:** the emerging relationship between information technology. New York: The New Press, 2003.

LEANDER, 2. **Chimeras with Obscure Powers:** Hybrid States and the Public-Private Distinction. The Chimerical State and the Public-Private Hybridization of the 21st Century. New York: [s.n.]. 2009c.

LEANDER, A. The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies. **Journal of Peace Research**, 42, n. 5, 2005. 605–622.

LEANDER, A. Securing Sovereignty by Governing Security through Markets. In: ADLER-NISSEN, R.; GAMMELTOFOT-HANSEN, T. **Sovereignty Games:** Instrumentalising State Sovereignty in Europe and Beyond. New York: Palgrave MacMillan, 2008.

LEANDER, A. Thinking tools. In: KLOTZ, A.; PRAKASH, D. **Qualitative methods in international Rrelations:** a pluralist guide. [S.l.]: [s.n.], 2008. p. 11-27.

LEANDER, A. The Privatization of Security. In: DUNN CAVELTY, M.; MAUER, V. **The Routledge Handbook of Security Studies**. New York: Routledge, 2009a.

LEANDER, A. **Security:** a contested commodity. [S.l.]: [s.n.], 2009b. Working Paper.

LEANDER, A. Commercial Security Practices. In: BURGESS, P. J. **Handbook of New Security Studies**. New York: Routledge, 2010.

LEANDER, A. The Promises, Problems, and Potentials of a Bourdieu-Inspired Staging of International Relations. **International Political Sociology**, 5, 2011. 294–313.

LEANDER, A. Understanding US national intelligence: analyzing practices to capture the chimera. In: BEST, J.; GHECIU, A. **The return of the public in global governance**. Cambridge: Cambridge University Press, 2014. p. 197-220.

LIBICKI, M. **Conquest in Cyberspace:** National Security and InformationWarfare. New York: Cambridge University Press, 2007.

LIBICKI, M. C.; SENTY, D.; POLLAK, J. **H4CKER5 Wanter:** An Examination of the Cybersecurity Labor Market. Santa Monica: RAND Corporation, 2014.

LOCKHEED MARTIN. Cyber Security and Defense. **Lockheed Martin Cyber Security**, 2016. Available at: <http://cyber.lockheedmartin.com/>. Access: 14 feb. 2016.

LUHMANN, N. **Risk:** a Sociological Theory. New York: de Grutier, 1993.

MARCZAK, B. et al. **Mapping Hacking Team's "Untraceable" Spyware**. The Citizen Lab Research Brief No.33. 2014.

MARGETTA, R. **'Dramatic' Cyberattacks on Power Grids and More Predicted by NSA Chief**. CQ NEWS: [s.n.], 2014. Available at: <http://intelligence.house.gov/dramatic-cyberattacks-power-grids-and-more-predicted-nsa-chief>. Access: 01 mar. 2016.

MARKET RESEARCH MEDIA. U.S. Federal Cybersecurity Market Forecast 2015-2020. **Market Research Media - Premium market analysis:** taking uncertainty out of decision making, 2015. Available at: <http://www.marketresearchmedia.com/?p=206>. Access: 6 February 2016.

MARQUIS-BOIRE, M. **Backdoors are Forever: Hacking Team and the Targeting of Dissent**. Citizen Lab Research Brief No. 12. 2012.

MARTINEZ, J. A.; KAYSER, M. R. E. Cyber Professionals in the Military and Industry—Partnering in Defense of the Nation. **Air & Space Power Journal**, January/February 2013. 4-20.

MAY, C. **The Information Society:** a Sceptical View. Cambridge: Polity Press, 2002.

MCAFEE, J. The death of antivirus and what comes next. **Silicon Angle**, 22 June 2015. Available at: <http://siliconangle.com/blog/2015/06/22/the-death-of-antivirus-and-what-comes-next/>. Access: 06 jan. 2016.

MCCARTHY, D. R. **Power, Information Technology and International Relations Theory:** The Power and Politics of US Foreign and Internet. New York: Palgrave MacMillan, 2015.

MCDONALD, N. Is Antivirus Obsolete? **Gartner**, September 2012. Available at: <http://blogs.gartner.com/neil_macdonald/2012/09/13/is-antivirus-obsolete/>. Access: 09 feb. 2016.

MCGANN. **2014 Global Go To Think Tank Report**. [S.l.]: University of Pennsylvania, 2015. Available at: <http://repository.upenn.edu/cgi/viewcontent.cgi?article=1008&context=think_tanks>. Access: 02 feb. 2016.

MCLAUGHLIN, J. NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI. **The Intercept**, 21 January 2016. Available at: <https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/>. Access: 10 February 2016.

MEDVETZ, T. **Think Tanks in America**. Chicago: University Of Chicago Press, 2012.

MÉRAND, F. Pierre Bourdieu and the Birth of European Defense. **Security Studies**, 19, n. 2, 2010. 342-374.

METZ, C. Telecoms Look Past Cisco and HP to Open Source Hardware. **Wired**, 27 January 2016. Available at: <http://www.wired.com/2016/01/telecoms-look-past-cisco-and-hp-to-open-source-hardware/>. Access: 30 January 2016.

MORGAN, S. What does federal spending in 2016 mean for the cybersecurity sector? **CSO: Cybersecurity Business Report**, December 2015. Available at: <http://www.csoonline.com/article/3016035/government/what-does-federal-spending-in-2016-mean-for-the-cybersecurity-sector.html>. Access: 4 February 2016.

MORGAN, S. Top five U.S. defense contractors bungle commercial cybersecurity market opportunity. **CSO: Cybersecurity Business Report**, 28 January 2016. Available at: <http://www.csoonline.com/article/3027383/security/top-five-u-s-defense-contractors-bungle-commercial-cybersecurity-market-opportunity.html>. Access: 4 February 2016.

MORGENTHAU, H. **A política entre as nações**. Brasília: UNB, 2002.

MUELLER, M.; SCHMIDT, A.; KUERBIS, B. Internet Security and Networked Governance in International Relations. **International Studies Review**, 15, 2013. 86–104.

NAKASHIMA, E. Google to enlist NSA to help it ward off cyberattacks. **The Washington Post**, 4 February 2010. Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html>. Access: 2 February 2016.

NATO CCDCOE. **The Tallin Manual on International Law Applicable to Cyber Warfare**. Tallin: [s.n.], 2013.

NEGROPONTE, N. **A vida digital**. São Paulo: Companhia das Letras, 1995.

NEUMANN, I. B. Returning practice to the linguistic turn: the case of diplomacy. **Millennium: Journal of International Studies**, 31, n. 3, 2002. 627-651.

NISSENBAUM, H. Where Computer Security Meets National Security. **Ethics and Information Technology**, 7, n. 2, june 2005. 61-73.

NORTHROP GRUMMAN. **Northrop Grumman Corporation**, 2016. Available at: <http://www.northropgrumman.com/Pages/default.aspx>. Access: 15 feb. 2016.

NSA. **National Security Agency - Central Security Service:** Defending our nation. Securing the future, 2016. Available at: <https://www.nsa.gov/ia/index.shtml>. Access: 01 mar. 2016.

NYE JR, J. S. **O Futuro do Poder**. São Paulo: Benvirá, 2011.

NYE, J. **Power in a global information age:** from realism to globalization. New York: Routledge, 2004.

NYE, J. S. **The Regime Complex for Managing Global Cyber Activities**. [S.l.]: Centre for International Governance Innovation and the Royal Institute for International Affairs, 2014.

NYE, J.; OWENS, W. A. America's Information Edge. **Foreign Affairs**, March-April 1996. Available at: <https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge>. Access: 13 January 2016.

OECD. **Factsheet on how competition policy affects macro-economic outcomes**. [S.l.]: [s.n.], 2014. Available at: <https://www.oecd.org/daf/competition/2014-competition-factsheet-iv-en.pdf>. Access: 15 apr. 2016.

OFFICE OF MANAGEMENT AND BUDGET. **Fiscal Year 2016 Budget of the U.S. Government**. Washington DC: U.S. Government Publishing Office, 2015.

OLLMAN, G. The Business Of Commercial Exploit Development. **DarkReading**, 2012. Available at: <http://www.darkreading.com/risk/the-business-of-commercial-exploit-development/d/d-id/1138713>. Access: 15 feb. 2016.

OVERILL, R. E. Reacting to cyber-intrusions: the technical, legal and ethical dilemma. **Journal of Financial Crime**, 11, n. 2, 2004. 163-167.

O'ZINN, J. **Social Theories of Risk and Uncertainty:** An Introduction. Oxford: Blackwell , 2008.

PALLUAULT, O. La Dynamique Contemporaine de Sécurité et le Renuveau de la Défense Civile Américaine sous l'administration Clinton. **Cultures et Conflits**, 84, 2011. 103-129.

PAPP, D. S.; ALBERTS, D. S. National security in the information age: setting the stage. In: ALBERTS, D. S.; PAPP, D. S. **Information Age Anthology (Volume**

II): National Security Implications of the Information Age. Washington DC: CCRP publication series, 2000. p. 1-54.

PAPP, D. S.; ALBERTS, D. S.; TUVAHOV, A. Historical Impacts of Information Technologies: an Overview. In: ALBERTS, D. S.; PAPP, D. S. **The Information Age:** An Anthology on Its Impact and Consequences. Washington DC: CCRP Publication Series, 1997. p. 13-35.

PCCIP. Critical foundations: protecting America's infrastructures (excerpts). In: ALBERTS, D. S.; PAPP, D. S. E. **An Information Age Anthology (volume II):** National Security Implications of the Information Age. Washington DC: CCRP publication series, 2000. p. 225-258.

PETERSEN, K. L. Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility? **Cambridge Review of International Affairs**, 21, n. 3, September 2008a. 403-420.

PETERSEN, K. L. Terrorism: when risk meets security. **Alternatives: Global, Local, Political**, 33, n. 2, 2008b. 173.

PETERSEN, K. L. Risk analysis – A field within Security Studies? **European Journal of International Relations**, 18, n. 4, 2011. 693-717.

PETERSEN, K.; TJALVE, V. S. (Neo) Republican security governance? US homeland security and the politics of "shared responsibility. **International Political Sociology**, 7, n. 1, 2013. 1-18.

POULIOT, V. The Logic of Practicality: A Theory of Practice of Security Communities. **International Organization**, 62, n. 2, April 2008. 257-288.

POULIOT, V.; MÉRAND, F. Bourdieu's concepts: political sociology in international relations. In: ADLER-NISSEN, R. **Bourdieu in International Relations:** rethinking key concepts in IR. New York: Routledge, 2013. p. 24-44.

RAYTHEON. **Technology Today**, n. 1, 2015. Available at: <http://www.raytheon.com/news/technology_today/2015_i1/>. Access: 23 dec. 2015.

RAYTHEON. Raytheon cyber, 2016. Available at: <http://www.raytheoncyber.com/>. Access: 20 feb. 2016.

RECKWITZ, A. Toward a Theory of Social Practices: A Development in Culturalist Theorizing. **European Journal of Social Theory**, 5, n. 2, May 2002. 243-263.

REITMAN, R. Tech Companies and NSA Surveillance: Questions, Contradictions, and Economic Consequences. **Eletronic Frontier Foundation**, 21 March 2014. Available at: <https://www.eff.org/deeplinks/2014/03/tech-companies-and-nsa-surveillance-questions-contradictions-and-economic>. Access: 6 February 2016.

RENDA, A. Cybersecurity and Internet Governance. **Global Memos**, 13 May 2013.

REUTERS. Raytheon acquires cyber firm for $420 million. **Reuters**, 5 November 2014. Available at: <http://www.reuters.com/article/us-blackbird-techonologies-m-a-raytheon-idUSKBN0IP22620141105 >. Access: 20 feb. 2016.

RID, T.; BUCHANAN, B. Attributing Cyber-Attacks. **Journal of Strategic Studies**, 1-2, 2015. 4-37.

ROBINSON, N. et al. **Cyber-security threat characterisation:** A rapid comparative analysis. Santa Monica: RAND Corporation, 2013.

ROGERS, M. **Fordham University's Fifth International Conference on Cyber Security - ICCS 2015**. New York: [s.n.]. 2015. Special Keynote Address.

ROSENQUIST, M. How Offensive Cyber Security is Changing the Industry. **IT Peer Network**, 8 October 2013. Available at: <https://communities.intel.com/community/itpeernetwork/blog/2013/10/08/how-offensive-cyber-security-is-changing-the-industry>. Access: 25 mar. 2016.

ROSZAK, T. **El Culto a la Información:** Tratado sobre alta tecnología, inteligencia artificial y el verdadero arte de pensar. Barcelona: Gedisa, 2005.

SALMI, D. The death of Antivirus has been greatly exaggerated. **Avast!Blog**, 7 May 2014. Available at: <https://blog.avast.com/2014/05/06/the-death-of-antivirus-has-been-greatly-exaggerated/>. Access: 05 feb. 2016.

SCHATZKI, T.; KNORR-CETINA, K.; SAVIGNY, E. **The Practice Turn in Contemporary Theory**. Oxon: Routledge, 2001.

SCHNEIER, B. Who Should Be in Charge of Cybersecurity? **The Wall Street Journal**, 31 March 2009. Available at: <http://www.wsj.com/articles/SB123844579753370907>. Access: 30 January 2016.

SCHNEIER, B. The Vulnerabilities Market and the Future of Security. **Forbes**, 30 May 2012.

SCHNEIER, B. The Battle for Power on the Internet. **The Atlantic**, 24 October 2013. Available at: <http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>. Access: 30 January 2016.

SCHWAB, K. The Fourth Industrial Revolution: What It Means and How to Respond. **Foreign Affairs**, December 2015. Available at: <https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>. Access: 20 January 2016.

SCHWARTZ, M. NSA Contracted With Zero-Day Vendor Vupen. **DarkReading**, September 2013. Available at: <http://www.darkreading.com/risk-management/nsa-contracted-with-zero-day-vendor-vupen/d/d-id/1111564?>. Access: 06 feb. 2016.

SHORROCK, T. **Spies for Hire:** The Secret World of Intelligence Outsourcing. New York: Simon & Schuster, 2008.

SIMMONS, B. A. International Studies in the Global Information Age. **International Studies Quarterly**, 55, 2011. 589–599.

SINGER, P. Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry. **International Security**, 26, n. 3, 2002. 186-220.

STEPTOE. The Hackback Debate. **Steptoe Cyberblog**, November 2012. Available at:<http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/>. Access: 05 apr. 2016.

STERLING, B. **The Epic Struggle of the Internet of Things**. Moscow: Strelka Press , 2014.

STEVENS, T. Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why? **International Political Sociology**, 9, 2015. 230-247.

STEWART, T. A. Welcome to the revolution. In: ALBERTS, D. S.; PAPP, D. S. **The Information Age:** An Anthology on Its Impact and Consequences. [S.l.]: CCRP Publication Series, 1997. p. 5-12.

STRAND, J. How I Learned To Love Active Defense. **DarkReading**, July 2015. Available at: <http://www.darkreading.com/attacks-breaches/how-i-learned-to-love-active-defense/a/d-id/1321361>. Access: 05 abr. 2016.

SWARTZ, D. **Culture & Power:** the sociology of Pierre Bourdieu. Chicago: The University of Chicago Press, 1997.

SYMANTEC. **Symantec - The Global Leader in Next-Generation Cyber**, 2016. Available at: <https://www.symantec.com/>. Access: 25 feb. 2016.

SYMANTEC. **Internet Security Threat Report**. Symantec Corporation. Mountain View , p. 98p. 2014.

THE Spy Files. **WikiLeaks**, 2011. Available at: <https://wikileaks.org/spyfiles/>. Access: 15 jan. 2016.

THIELMAN, S. FBI head: terror fight requires open backdoors to encrypted user data. **The Guardian**, 9 December 2015. Available at: <http://www.theguardian.com/us-news/2015/dec/09/fbi-director-tech-companies-backdoors-user-data-access-counter-terrorism>. Access: 2 February 2016.

U.S. DEPARTMENT OF JUSTICE. FBI's FY 2016 Authorization and Budget Request to Congress, 2015. Available at: <https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/24._federal_bureau_of_investigation_fbi.pdf>. Access: 26 feb. 2016.

ULLMAN, R. H. Redefining Security. **International Security**, 8, n. 1, 1983. 129-153.

USAJOBS - The Federal Government's Official Jobs Site, 2016. Available at: <http://usajobs.gov/>. Access: 15 feb. 2016.

VOLZ, D. National Security Agency merging offensive, defensive hacking operations. **Reuters**, 8 February 2016. Access: 12 February 2016.

WALKER, R. B. J. Lines of Insecurity: International, Imperial , Exceptional. **Security Dialogue**, 37, n. 1, March 2006. 65-82.

WALTZ, K. **Theory of International Politics**. Boston: Addison-Wesley, 1979.

WARE, W. H. **Future Computer Technology and Its Impact**. RAND Corporation. Santa Monica. 1966.

WARE, W. H. **Security and Privacy in Computer Systems**. RAND Corporation. Santa Monica. 1967a.

WARE, W. H. **The Computer in Your Future**. RAND Corporation. Santa Monica. 1967b.

WEBSTER, F. What Information Society? In: ALBERTS, D. S.; PAPP, D. S. **The Information Age:** An Anthology on Its Impact and Consequences. Washington DC: CCRP Publication Series, 1997.

WEISER, M. The Computer for the 21st Century. **Mobile Computing and Communications Review**, v. 3, n. 3, p. 3-11, July 1999.

WHITE HOUSE. **The National Strategy to Secure Cyberspace**. Washington DC: The White House, 2003.

WHITE HOUSE. **Cyberspace Policy Review:** Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington DC: U.S. Government Printing Office, 2009. Available at: <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

WHITE HOUSE. **International Strategy to Secure Cyberspace:** Prosperity, Security and Openness in a Networked World. Washington DC: Government Printing Office, 2011. Available at: <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Access: 20 dec. 2015.

WIENER, N. **The human use of human beings:** cybernetics and society. London: Free Association Books, 1989.

WOODS, D. The Product Management FireEye-Mandiant Deal Logic of the. **Forbes**, January 2014. Available at: <http://www.forbes.com/sites/danwoods/2014/01/03/the-product-management-logic-of-the-fireeye-mandiant-deal/#45dc708d4313>. Access: 10 feb. 2016.

YADRON, D. Symantec Develops New Attack on Cyberhacking. **The Wall Street Journal**, 4 May 2014. Available at: <http://www.wsj.com/articles/SB10001424052702303417104579542140235850578>. Access: 15 feb. 2016.

ZERODIUM. ZERODIUM - The Premium Exploit Acquisition Platform , 2016. Available at: <https://www.zerodium.com/>. Access: 22 feb. 2016.

ZHENG, D. E. **Disrupting the Cyber Status Quo**. Washington DC: Center for Strategic and International Studies, 2015.

ZHENG, D. E.; LEWIS, J. A. **Cyber Threat Information Sharing:** Recommendations for Congress and the Administration. Washington DC: Center for Strategic and International Studies, 2015.