CARTA INTERNACIONAL
ASSOCIAÇÃO BRASILEIRA DE RELAÇÕES INTERNACIONAIS
ISSN 2526-9038

Origin and analysis of Brazilian cybernetic fragility

Origem e análise da fragilidade cibernética brasileira

Origen y análisis de la ciberfragilidad brasileña

DOI: 10.21530/ci.v16n2.2021.1109

Ricardo Camerra[1]
Bruno Lima Rocha Beaklini[2]

Abstract

The former National Security Agency agent Edward Snowden uncovered evidence of US cyber espionage. Thus this study examines the geostrategy of such cyber threats. The methodology adopted entailed a qualitative approach. This way, we are able to understand that a spread of US ICT during the 20th and 21st centuries has created a global dependence on American technologies. Brazil's failure to sufficiently develop its ICT sector could have led it to being vulnerable to cyberattacks. However, one cannot be certain that such a factor was behind the NSA surveillance issue, as evidence does not imply a causal relation.

Keywords: The United States of America, Cyber warfare, Brazil, Geostrategy.

Resumo

O ex-agente da Agência de Segurança Nacional Edward Snowden revelou evidências da espionagem cibernética dos Estados Unidos.

[1] Formado em Relações Internacionais pela Universidade do Vale do Rio dos Sinos (ricardojcamera@gmail.com). **ORCID: https://orcid.org/0000-0003-1165-6470**.

[2] Doutor em ciências políticas pela Universidade Federal do Rio Grande do Sul. (blimarocha@gmail.com). **ORCID: https://orcid.org/0000-0001-9372-112X**.

Artigo submetido em 06/08/2020 e aprovado em 10/05/2021.

Este artigo estuda algumas correlações ligadas a essas ameaças cibernéticas, e a metodologia envolve uma abordagem qualitativa. Dessa forma, entende-se que houve uma disseminação das TIC norte-americanas durante o século 20, o que criou uma dependência global das tecnologias estadunidenses. O fracasso do Brasil em desenvolver suficientemente seu setor de TIC pode tê-lo tornado vulnerável aos ataques cibernéticos. No entanto, não se pode ter certeza de que tais fatores foram os motivos da vigilância eletrônica promovida pela NSA, visto que correlações não implicam em relações causais.

Palavras-chave: Estados Unidos da América, Guerra Cibernética, Brasil, Geoestratégia.

Resumen

El exagente de la Agencia de Seguridad Nacional, Edward Snowden, descubrió pruebas de ciberespionaje estadounidense. Por tanto, este estudio examina la geoestrategia de dichas ciberamenazas. La metodología adoptada implicó un enfoque cualitativo. De esta manera, podemos entender que la expansión de las TIC estadounidenses durante los siglos XX y XXI ha creado una dependencia global de las tecnologías estadounidenses. El hecho de que Brasil no haya desarrollado suficientemente su sector de las TIC podría haberlo llevado a ser vulnerable a los ciberataques. Sin embargo, no se puede estar seguro de que tal factor estuviera detrás del problema de la vigilancia de la NSA, ya que la evidencia no implica una relación causal.

Palabras clave: Estados Unidos de América, Cyber Warfare, Brasil, Geoestrategia.

Introduction

Speculations since the 1970s on electronic surveillance by the United States were confirmed in 2013 when several confidential documents were leaked by former National Security Agency (NSA) agent Edward Snowden—who revealed that the United States and its organic Anglo-Saxon allies had been jointly conducting massive surveillance activities (European Parliament 2001; Clement 2014).

Backed by national security laws, the United States had been intercepting heads of state such as Dilma Rousseff as well as companies and government bodies such as Petrobrás and the Brazilian Ministry of Mines and Energy (Clement 2014). Slides provided by Snowden (2013, 2014) revealed what seemed to be other targets, such as Google's infrastructure, Russian oil and gas company Gazprom, Russian state-owned airline Aeroflot, the French Foreign Ministry, the United

Arab Emirates telecommunications company Warid Telecom, and the SWIFT network of international interbank payments.

Since these revelations, Brazil has been reinforcing its strategies and institutions to face similar cyber war threats. Such improvements have been implemented through new legal frameworks and technologies, such as the Policy of Cybernetic Defense, a Cyber Defence Command, a National College of Cyber Defense, a system of Homologation and Certification of Cyber Defense Products, the Military Doctrine of Cyber Defense, a program of development and innovation in cyber defense, and so on (Vianna 2019).

Despite the Brazilian government's intention to overcome its cyber fragilities, one must consider that sectors of Brazilian critical infrastructure have been intercepted in recent years. Hence, this study intends to project a general conjecture for Brazil according to the following logic: since Brazil has been a target of American intelligence, which uses cyber warfare techniques, and is dependent on foreign information and communications technologies (ICTs) and—mostly US—Internet content providers, there is a possibility that cyber-attacks directed at Brazil could be linked to the country's lack of national technologies[3].

Regarding methodology, this study employed qualitative methods to collect and analyze data. First, document-based research was employed, in which US government files were selected, ranging from top secret files leaked by Snowden to official reports available on government websites. Focus was given on files related to Brazil as well as high-tech policies. The same procedure was used to collect Brazilian documents, in addition to a literature review related to international relations, ICT sectors, and cyber warfare.

Notwithstanding, the exact amount of foreign ICT components that integrate the entire Brazilian society has not been found; hence, in this study, a non-statistical sample was used instead of quantitative methods. Moreover, a timeline with a retrospective logic was chosen for an investigation: starting from the NSA cyberattacks that had been revealed by President Dilma Rousseff's government (2010–2016). Then, certain **specific facts** that occurred during the

[3] This work, however, indicates some important factors: importation of telecommunications equipment, foreign direct investment, and international cooperation with technological superpowers do not necessarily mean that the country importing such services and products makes the country vulnerable to backdoors of embedded systems or external cyber-attacks. In fact, even if Brazil masters all technological layers of the ICT sector, it could still be a target of cyber-attacks. Moreover, mechanisms such as cryptography are currently available for systematic protection. Therefore, it is important to clarify that this research does not intend to exhaust such issues.

Cold War and post-Cold War period were explored. The early 2020s, however, were not explored as data and facts from after 2019 were not examined.

Second, an inductive reasoning line was developed to produce a generalization for our findings, as there is no intention to build a quantitative study with causal inferences. This study explains how the United States managed to spread its ICT technologies in contemporary history, as well as demonstrating the Brazilian fragility regarding its own ICT developments, bringing some general data of the ICT sector to the forefront, as it outlines neither statistical data nor a stratification of the whole high-tech supply chain[4].

The first section of this article defines the post-Cold War scenario and some concepts of geostrategy and cyber warfare. The second section refers to the growth of US ICTs. The third points out the development of the Brazilian ICT sector and its outcomes, and finally, the study's conclusions.

From Geostrategy to Cyber War concepts

In this review, the post-Cold War scenario is analyzed in terms of general geostrategy. It is evident that the North Atlantic Treaty Organization's (NATO) presence—led by the United States—has been increasing in Western Europe, the Middle East, the Caucasus, Central Asia, and the Far East. There have been attempts at undermining Russia's influence, dividing Russia and China, and stopping the anti-US coalition of the Asian *Rimland* States. This is, for example, what Zbigniew Brzezinski (2016) and Henry Kissinger (2015) advocated as a standard strategy (Cohen 2014). Conversely, it should be noted that there is also a reverse movement: the Sino-Russian rapprochement, the construction of the New Silk Road, and China's growing economic presence in all continents, in addition to all the complex inter-Asian relations that have their own dynamics (Agnew 2008; Mearsheimer 2019).

However, such a framework cannot be viewed uniquely in stationary geographic terms because the dimension of geostrategic planning does not depend on territories, boundaries, deserts, seas, mountains, or forests (Cohen 2014; Correia 2012). As Qiao, Santoli, and Wang (1999) assert, the strategic mode in which it works originates new warfare standards.

[4] For example, the industrial sector of submarine cables has not been analyzed, although an overview of satellite manufacturing, parts of the IT sector, as well as the dominance of the telecom companies has been pointed out.

> After a DSP satellite identified a target, an alarm was sent to a ground station in Australia, which was then sent to the central command post in Riyadh through the U.S. Cheyenne Mountain command post, after which the "Patriot" operators were ordered to take their battle stations, all of 12 which took place in the mere 90-second alarm stage, relying on numerous relays and coordination of space-based systems and C3I systems, truly a "shot heard 'round the world." The real-time coordination of numerous weapons over great distances created an unprecedented combat capability, and this was precisely something that was unimaginable prior to the emergence of information technology (Qiao, Santoli, and Wang 1999, 11-12).

The importance given to the informational realm has shifted the focus of armed forces and states to new concepts, such as cyber warfare. It can be explained in varying ways. Nations, UN institutions, and authors may slightly disagree on how cyber warfare is perceived, even though its fundamental meaning remains unchanged. This article chose a general explanation, according to selected authors. However, this work does not include discussions on individual-related subjects, such as cyber criminals and cyber terrorism. Only the state-centric vision of cyber warfare and the way its features work is explored.

New electronic technologies have thus been incorporated into the armed forces in the 1980s and the 1990s, and a new vocabulary emerged. There is no longer a traditional war, although this still exists in parallel (Andress and Winterfeld 2013; Kissinger 2015). In this situation, there is neither a formal declaration of war nor an early warning, implying that cyber-attacks may occur at any time in these scenarios. All means—not only hard power—are used to inflict damage on enemies, such as cultural diffusion through social media to win public opinion (Nye 2011), the use of economic sanctions to isolate and weaken a state, the use of lawfare as a weapon, and cyber-attacks. A strategy of gathering all these options of warfare is called a *hybrid war* (Andress and Winterfeld 2013; Nye 2011; Kissinger 2015).

Consequently, cyber war goals include damaging the critical structures of other countries (for example, the energy sector, water and sewage systems, hospitals, telecommunications, the armed forces, and so on). To clarify, one could "steal information [...] crash airplanes, or cause a missile to detonate in the wrong place [...]; financial systems could collapse, supply chains could halt, satellites could spin out of orbit into space, and airlines could be grounded" (Clarke and Knake 2010, 38).

Brazil's Green Book of National Security—the *Livro Verde de Segurança Nacional*—claims that critical infrastructures[5] are "facilities, services, goods, and systems whose interruption or destruction, totally or partially, produce a serious social, economic, political, environmental, international or security impact on the government and society[6]" (Presidência da República 2010, 19). When it comes to the United States, the NSA, the United States Cyber Command (CYBERCOM), and the Department of Homeland Security constitute the core of US cyber warfare and defense (Andress and Winterfeld 2013; Kissinger 2015), and these institutional branches have been conducting cyber war activities such as **supply chain attacks** to implant **backdoors** into embedded systems, SCADA[7] infrastructure, and commercial devices.

> Hearing McConnell, or his successor, Air Force General Ken Minihan, talk about NSA even on an unclassified basis, you begin to understand why they believe re-creating some of its capabilities elsewhere is folly and perhaps impossible. They both speak with real reverence about the decades of experience and expertise NSA has in "doing the impossible" when it comes to electronic espionage. NSA's involvement in the Internet grew out of its mission to listen to radio signals and telephone calls. The Internet was just another electronic medium. As Internet usage grew, so did intelligence agencies' interest in it. Populated with Ph.D.s and electrical engineers, NSA quietly became the world's leading center of cyberspace expertise. Although not authorized to alter data or engage in disruption and damage, NSA thoroughly infiltrated the Internet infrastructure outside of the U.S. to spy on foreign entities (Clarke and Knake 2010, 23).

Essentially, Richard Clarke and Robert Knake give the meaning of those highlighted concepts as follows: "one former US intelligence officer told us, 'this may mean that no one can hack Windows easily to spy on China. It certainly does not mean that China is less able to hack Windows to spy on others" (Clarke and Knake 2010, 49). In other words, they explain how China has managed to make a deal with Microsoft to allow the use of Microsoft software in their

[5] The Brazilian government approved Act No. 10.222, of February 5, 2020, that is the National Strategy of Cyber Security — E-Ciber. This piece of legislation encompasses similar concepts and provides the main relevant guidelines to all the Brazilian governmental branches. However, this work does not intend to analyze this piece of legislation.

[6] *Por infraestruturas críticas (IEC) entendem-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade* (Presidência da República 2010, 19).

[7] Supervisory control and data acquisition.

country, so as long as the American company relinquished its secret operating system codes to China.

In this way, different versions of Microsoft software are circulated in China: Versions that include Chinese government encryptions. Here, one can observe the problem of backdoors, through which unauthorized software or hardware weaknesses are put in devices to cause damage or assist in digital surveillance (Andress and Winterfeld 2013; Clarke and Knake 2010). As China utilizes different versions of Microsoft's codes, it would be more complex for the United States to spy on the Chinese government and civilians. This also implies that the United States could engage in similar activities with other clients that do not have the aforementioned advantages possessed by China. However, this also infers that China could spy on other countries that utilize such software.

Such a deliberate operation occurs through supply chain attacks, in which intelligence agencies—such as the NSA—secretly work with major high-tech and ICT suppliers—such as Cisco, AT&T, Microsoft, and Verizon—to deploy unauthorized backdoors that weaken devices within the supply chain of certain products, such as aerospace technology and telecommunications (Deibert 2015; Powers and Jablonski 2015). Hence, through these strategies, governments can emulate massive digital surveillance. "As Admiral Mike McConnell has noted, information managed by computer networks—which run our utilities, our transportation, our banking and communications—can be exploited or attacked in seconds from a remote location overseas" (Clarke and Knake 2010, 38).

As pointed out in the introduction of this study, the US government has used the above strategies to access data stored or flowing through telecom networks, to steal other countries' critical information such as energy policies and military secrets—not to mention the possibility of industrial espionage.

American ICT's Origins and Strategy

The first section of this study has set the conceptual scope for analyzing the issues proposed. The second section is essential for understanding American cyber and telecommunications power. It aims to explore how these systems have been structured throughout the 20th century. Historic factors will clarify how US technology and telecoms became global, as if they were a geostrategic cobweb. That is, this section intends to explore a summarized review of the development of the

US ICT industry and its global trajectory. For this reason, data and sources from different years will be discussed. One will notice that the United States has been leading the ICT sector in recent history, despite competition from other nations.

Telecommunications are not a mere byproduct of the United States' military–industrial complex, but its constitutive part, which is why Schiller (1992) defines it as the military–industrial–communications complex. The US government had provided a strategic direction to this sector in the 1930s and the 1940s. Young students and engineers and their small companies, such as Hewlett-Packard (HP), had been connected to large academic laboratories, such as the Massachusetts Institute of Technology (MIT); the University of California, Los Angeles (UCLA); the University of Southern California (USC); Stanford; Berkeley; and Harvard, and these research centers have been interacting with corporations, such as RCA, Hughes Aircraft, AT&T, General Electric, Westinghouse, Boeing, and their private laboratories (the well-known Bell Labs is an example). All these research centers have been linked by the federal government in a government–university–market arrangement, which means that they have received government subsidies (Bingham 2016; Loveluck 2015; Mazzucato 2014; Schiller 1992).

World War II and the Cold War were the main reasons for the national structure of innovation. This context set the modern industry–military and communications complex, giving rise to modern electronics and microelectronics (Bingham 2016; Cassiolato et al. 2013). Such an institutional architecture produces a multitude of products through the so-called spillover effect, such as satellites, the Internet, micro-waves, new materials, and electronic devices. It is not by chance that more than 90% of the demand for semiconductors from Silicon Valley comes from defense procurement. Sun Microsystems, Apple, Silicon Graphics, Cisco System, Fore, IBM, Compaq, NCR, Cray Research, Intel, Motorola, Bay Networks, and HP are examples of Silicon Valley companies originating directly or indirectly from DARPA[8] projects, which demanded new semiconductors, electronic devices, and software for the US Department of Defense (Bingham 2016; Cassiolato et al. 2013; Loveluck 2015; Mazzucato 2014; Schiller 1992). Whalen (2014) and Chomsky (1993) have called this the *Camelot complex* of private contractors, universities, and government relations.

The American government managed to improve the internationalization of its ICT sector after a series of events that occurred after World War II, such

[8] Defense Advanced Research Projects Agency.

as the consolidation of the American ICT market and the mastering mode in which President John F. Kennedy's government conducted and gathered interest among the military, the National Aeronautics and Space Administration (NASA), and private industry, such as AT&T and Hughes Aircraft. These actions brought about a global telecommunication system through technical cooperation among nations, in which the American government maintained its involvement through joint ventures, exportation, and foreign direct investments—That is, the Intelsat Consortium was created in the 1960s. In the 1970s, President Richard Nixon's administration introduced the Open Sky and Open Door policies, through which institutional and political frameworks were designed for the projection of the US high-tech industry abroad. Meanwhile, President Ronald Reagan's administration and its "Star Wars program" during the 1980s perfected innovation and technology, despite disputes with the Soviet Union (The United States Office of Technology Assessment 1985; Pelton 2017; Whalen 2002, 2014).

The United States, however, had understood that other nations would not accept the predominance of American technology and political influence. For example, France and West Germany had diplomatically pressured the United States to obtain space and ICT technologies. However, technical cooperation was not requested by only first-level allies, such as Western Europe countries. Japan, South Korea, China, Indonesia, Australia, and India also requested agreements. Brazil and most southern underdeveloped countries had been willing to cooperate to improve economic standards as well (Cervo and Bueno 2002; Pelton 2017; The United States Office of Technology Assessment 1985; Whalen 2014).

The United States thus understood the scenario as an opportunity to be linked to other countries' development. This happened mostly during the 1960s and 1970s, which made the United States foster its policy of going global. Hence, agreements between Japan and the United States in 1969, 1975, and 1980 are exemplary in the realm of technological transference and cooperation, whereby American enterprises would disclose space and electronics-related information to Japanese companies and their government. This shows that American corporations have played a major role in Japanese high-tech development (Borrus, Ernst, and Haggard 2003; National Research Council 1996; The United States Office of Technology Assessment 1985).

> For example, a number of Japanese technology development programs envisage an important international component. Several large U.S. firms such as Motorola, IBM, United Technologies, General Electric, and the Stanford

> Research Institute, have participated in joint research and development programs designed to pursue Japanese national research objectives. These projects, which range from micromachine technology to supersonic propulsion systems, to new models for software architecture, offer opportunities for foreign companies to participate in significant development programs (National Research Council 1996, 44).

Most importantly, this strategy supported the origins of a new supply chain and entrepreneurship, the so-called *Wintelism*. Some of the characteristics and features of Wintelism are innovation and disintegration, although they helped the continuous process of internationalization of ICTs during the 1990s (Borrus, Ernst, and Haggard 2003; Hart and Kim 2002). Wintelism—Windows + Intel—refers primarily to the worldwide monopoly on computer models, processors, and operational systems, which are maintained by the symbiotic relationship of IBM—Microsoft—Intel. The IBM—Microsoft—Intel system was widespread internationally through dumping, maintaining monopoly status, and institutional support from the US government in World Trade Organization intellectual property TRIPs (Trade-Related Aspects of Intellectual Property) in a way that the European and Japanese industries could not compete (Borrus, Ernst, and Haggard 2003; National Research Council 1996; Hart and Kim 2002).

Another example is the semiconductor and microprocessor sectors. Updated data demonstrate American Intel and South Korean Samsung to be world leaders in the microprocessor and semiconductor markets (Grimes and Du 2020). "With US companies dominating semiconductor design and South Korea dominating memory chip production" (Grimes and Du 2020, 5).

> The electronics industry of the late 1990s bears only a passing resemblance to that of a decade earlier. Some of the names are the same—IBM, NEC, Toshiba, Digital Equipment Corporation (DEC), Matsushita, Siemens—but those big, vertically integrated assemblers of electronic systems no longer control the industry. In their stead, a new generation of firms has arisen, mostly but not exclusively American owned, who exercise the kind of market power (and have attained the market capitalization) that is but a passing memory for more traditional firms: Microsoft, Intel, Cisco, Oracle, Netscape, Cadence, Dell, Applied Materials, 3COM, SAP, Sun, Qualcomm, Octel. The new firms look nothing like the old leaders (Borrus, Ernst, and Haggard 2003, 56).

Grimes and Du (2020) have reviewed the macrodata of the semiconductor sector and found a leading position in the US high-tech industry:

> Having already identified the key companies in the different semiconductor segments, it's not surprising to discover that the US accounts for 51% of the IDM sector (51% of the total GVC revenue), with 28% from South Korea, 11% from Japan, and 7.0% from Europe. The US is also the dominant headquarter location for the fabless sector (23% of GVC revenue), accounting for 62% of the total, with 18% headquartered in Taiwan and 10% in China. Taiwan has the greatest concentration of foundry companies (11% of GVC revenue), accounting for 73% of the total, with the US having 10% and China 7%. In fact, Taiwan's TSMC alone accounts for 56% of global foundry revenue. Again, the OSAT segment of assembly and testing (6.0% of the GVC revenue) is dominated by Taiwan with 54% of the total revenue, the US with 17%, and China and Singapore both at 12%. In addition to the dominant role of companies from the US and South Korea in the semiconductor GVC, Taiwanese companies clearly play an important role in both the foundry and OSAT segments, while China is also growing in importance in both the fabless and foundry segments (Grimes and Du 2020, 6).

Bearing in mind the perspective presented thus far, the United States has a capacity over ICT networks that no other country seems to have[9]. "The United States has 25 of the top 100 Internet access infrastructure providers, and 55.43% of total Internet single-address traffic; thus, more than half of total Internet access goes through 25 US companies" (Pinto 2015, 69). These data also resemble the research of Ruiz and Barnett, with regards to the topic of "who owns the internet." One has observed the tendency of telecommunication frameworks and concluded that there is an increasing concentration, centrality, and integration of information among developed countries. Furthermore, the data indicate that the United States continues to be the leader in terms of data traffic. This is where geopolitics matters (DeNardis 2015; Ruiz and Barnett 2015).

> At the center of the network of ownership are ten companies: Level 3 (USA), CenturyLink (USA), Telia Sonera (Sweden), AT&T (USA), Cogent Communications (USA), Verizon Business (USA), XO Communications (USA), Hurricane Electric (USA), Tata Communications (India), and NTT Communications (Japan). The most central company is Level 3, with a 22.3% share of the network, followed by Century Link 8.7%, Telia Sonera 8.5%, AT&T 7.8%, and Cogent with 6.7% of the network. The top five companies hold 54% of the network share, the top ten share 77.1% of the network, and the top 18 companies share 92.8% of the network (Ruiz and Barnett 2015, 44).

[9] It is important, however, to remember that the United States does not have total control of the whole telecommunication and online networks. Otherwise, it could remotely activate the detonation diapositives of the Chinese and Russian nuclear warheads, which is a real concern in Russia (Van Putte 2016).

This concentration of data implies what Deibert (2015) states with regards to the organic relations between the private sector and government in the United States. In other words, in addition to Facebook, Google, and Microsoft, major data, service, and technology companies—such as Yahoo, PalTalk, Skype, AOL, Apple, AT&T, Verizon, BT, Vodafone, Cisco, and Level 3—were involved in the cooperation scandal of data collection for the United Kingdom–United States axis intelligence, according to Edward Snowden's revelations (Powers and Jablonski 2015).

> This manner of government pressure on the private sector illustrates the importance of the physical geography of cyberspace. Of course, many of the corporations that own and operate the infrastructure—companies like Facebook, Microsoft, Twitter, Apple, and Google—are headquartered in the United States. They are subject to US national security law and, as a consequence, allow the government to benefit from a distinct homefield advantage in its attempt to "collect it all." And that it does—a staggering volume, as it turns out. One top-secret NSA slide from the Snowden disclosures reveals that by 2011, the United States (with the cooperation of the private sector) was collecting and archiving about 15 billion Internet metadata records every single day. Contrary to the expectations of early Internet enthusiasts, the US government's approach to cyberspace—and by extension that of many other governments as well—has been anything but laissez-faire in the post-9/11 era. While cyberspace may have been born largely in the absence of states, as it has matured, states have become an inescapable and dominant presence (Deibert 2015, 11).

Nonetheless, the federal government of the United States has a legal framework that allows cyber operations to continue. For instance, there is the Foreign Intelligence Surveillance Act of 1978 (FISA), the Communication Act of 1934, and the Patriot Act of 2001. As the main structures and institutions that manage the world Internet are located in the US territory, these pieces of legislation embody the legal framework of the American government when it comes to the strategic use of information—that is, ICANN[10], 10 Internet root-servers out of 13, including the root-server 'A' controlled by Verisign, and the biggest ICT corporations (Andress and Winterfeld 2013; Bradshaw and DeNardis 2018; DeNardis 2015; Deibert 2015; Powers and Jablonski 2015; Ruiz and Barnett 2015).

Oher countries, including Brazil, have proposed the transfer of Internet root-server management to the International Union of Telecommunications, a

[10] Internet Corporation for Assigned Names and Numbers.

United Nations institution based in Geneva, Switzerland. If such a proposal were to be applied, the Internet would therefore not be centralized by one country. However, the United States has not yet accepted this proposal. The *American telecom empire* (Schiller 1992) does not want to give up its power (Andress and Winterfeld 2013; Bradshaw and DeNardis 2018; DeNardis 2015; Deibert 2015; Powers and Jablonski 2015; Ruiz and Barnett 2015).

Therefore, following the concepts highlighted in the first section, information can be gathered and organized based on the logic that this article has been indicating so far. In other words, the so-called *going global* of US ICT seems to favor the American capabilities of cyber warfare (DeNardis 2015; Powers and Jablonski 2015; Ruiz and Barnett 2015). The United States may have repeated the alliance mechanisms between governments and companies, which has been remarkably similar to the so-called *seven oil sisters* strategy[11] (The United States Senate Committee on Foreign Relations, Subcommittee on Multinational Corporations 1975). Instead of *big oil,* telecoms have played an important role in geostrategic terms and cyber wars.

Brazilian Issue

How the United States built its geostrategy on the expansion of ICTs and its outcomes has been previously explained; should this scenario worry Brazilian authorities in terms of sovereignty? This section summarizes the history of the Brazilian technological and telecom sector and presents a discussion on cyber vulnerabilities. This work, however, does not aim to reproduce all the historical factors and interpretations involved in such an issue.

Telecommunications arrived in Brazil at the end of the 19th century, and most companies at the time were American, Canadian, and German. Expansion of the Brazilian communication infrastructure during the 19th century and the first half of the 20th century was slow and troubled (Lins 2017; Pereira Filho 2002; Telebrasil 2004; Kubota and Sousa 2012). In the early 1960s, "80% of Brazil's communications were under the control of a Canadian company called Companhia Telefonica Brasileira (CTB), working in the states of Rio de Janeiro, Sao Paulo, Espirito Santo, and Minas Gerais. Meanwhile, the US company Cia.

[11] In 1975, the US Congress produced a report in which the United States admitted that its geopolitical strategies directly involved giant private national oil companies during the 20th century.

Telefonica Nacional (ITT) connected the states of Paraná and Rio Grande do Sul (Telebrasil 2004, 13)[12]." However, the Brazilian market has approximately 800 telegraph and telephone companies (Pereira Filho 2002).

The 1950s and the 1960s, however, were flourishing years for a nationalist and anti-imperialist mindset, which had grown since the Vargas regime (1930–1945). Even conservatives—but mostly left-wing and nationalist *establishments*—were willing to negotiate a new pattern of national development (Cervo and Bueno 2002). These individuals claimed that foreign private companies were not investing in either the expansion or unification of infrastructure, nor in research and development (R&D). Thus, to create a national telecommunications system that would be centralized and follow the strategic goals of development, Brazil initiated a massive process of nationalization without paying compensations (Lins 2017; Pereira Filho 2002; Telebrasil 2004; Kubota and Sousa 2012). "The creation of a national systems of telecommunication ended activities of foreign enterprises, such as Western Cables & Wireless (Telex), Radiobras (RCA), Italcable (ITT) (Pereira Filho 2002, 38)." Leonel Brizola is an exemplary case. He was the governor of the southern state of Rio Grande do Sul when he nationalized the local ITT branch: an action that was completely against the policy that the United States had been promoting (Cervo and Bueno 2002).

In 1963, the Brazilian Telecommunications Act was enacted, and in 1965, the military regime centralized telecommunications policy and established Embratel—a year prior to Brazil joining the international satellite communications Intelsat consortium. The Ministry of Communications was created in 1967, and in 1976, the Center for Telecommunications Research and Development was established in the city of Campinas as a center for the development of national ICT technologies. The creation of the holding Telebrás in 1972 established a national system that intended to be universal and interconnected. Telebrás and the infant technological industry have been backed by government procurement in an attempt to emulate the American *Camelot* experience (Lins 2017; Pereira Filho 2002; Telebrasil 2004; Kubota and Sousa 2012).

Along with communications policies, scientific and aerospace R&D institutions were established between the 1940s and the 1980s, such as the National Institute

[12] *No início da década de 60, 80% das comunicações do País estavam com a canadense Companhia Telefônica Brasileira — CTB — (Rio, São Paulo, Espírito Santo e Minas Gerais) e com a norte-americana Cia. Telefônica Nacional, da ITT (Paraná e Rio Grande do Sul* (Telebrasil 2004, 13).

for Space Research (INPE), the Instituto da Aeronáutica (ITA), the CAPES-CNPq system (for perfecting and coordinating R&D), the Ministry of Science and Technology, the state-owned Embraer, and so on (Câmara dos Deputados 2010; Santos and Neto 2005; Medeiros and Perilo 1990).

This period marked the attempt of Brazilian authorities to structure an industrial–military and ICT complex to master foreign technologies. The process was characterized by the installation of factories of large US and European manufacturers in Brazil. However, these factories were branches responsible for the decentralized production of some low and medium technological components. There was no *big science* at work, near the scenario in Silicon Valley (Lins 2017; Pereira Filho 2002; Telebrasil 2004; Kubota and Sousa 2012).

US technical cooperation has been quite limited in peripheral countries. As noted in studies by Hagedoorn (2002), most R&D cooperation has been among the Organisation for Economic Co-operation and Development (OECD) nations—although there have been limitations even with regards to these nations. Neither the world powers nor the United States simply desire to empower potential foes or competitors. It has been a logic of deterrence in terms of technology and intellectual property protection.

In this way, the growth of the country's industrial capacity increased the outflow of foreign currencies to pay royalties and inputs. Moreover, technology faced challenges in Brazil due to the lack of other necessary production factors (Santos and Neto 2005). South Korea overcame similar challenges because of Korean educational and institutional measures to develop high-tech industrialization, as well as the support given by the United States. In contrast, Brazil has relied too much on foreign technology in the ICT and aerospace sectors[13], particularly the United States' embedded technology, whereas Brazilians have not received such support that South Korea has had (Teixeira 2005; Kubota and Sousa 2012). Brazilian reliance on these sectors is critical regarding cyber vulnerabilities (Fernandes 2015; Vianna 2019).

> According to (Negri 2007), the Brazilian FDI attraction policies had no requirements related to domestic technology development by multinationals. On the contrary, Brazil adopted the understanding that the mere foreign

[13] Regarding avionics and aerospace sectors, "How much share did the North America aerospace avionics market accounted for in 2018? North America with over 30% share dominates the market due to presence of major aerospace avionics system providers and major full cost carriers" (Bhutani and Wadhwani 2019, n.p).

> presence would be able to boost the national productive structure and contribute to the local production of technology, using an ‘open doors’ policy (Chiarini 2016, 294)[14].

From this perspective, as presented by Chiarini, Brazil had not managed to develop national technology up to the 1970s. There was an astonishing lack of R&D in the educational system and private sector, in addition to institutional–political problems, lack of foreign cooperation, and the debt crisis during the 1980s. According to Herrera (1995), after World War II, Latin America received considerable foreign support for the development of science and industry. Although financial and technical support was nothing like what Europe and Japan received, it was enough to start a technical basis. However, all efforts failed. Extensive poverty, persistent social inequality, low standards of education, institutional, bureaucracy, and political conundrum are cited by [15] Herrera (1995).

In this way, Gutierrez and Leal assert that these issues continue to be important factors during the 21st century, given the fact that Brazil still has not created a high-tech industrial complex, such as those created by developed or developing countries, just like South Korea and China.

> Brazil is one of the few countries among the largest economies in the world that does not have an electronic complex that manufactures integrated circuits. In addition, the manufacture of electronic goods in Brazil is limited, with exceptions, to pure and simple assembly from a total set of imported components (kits), which adds little value to the products. The creation of an integrated industry will be a game change in this situation, strengthening the electronic chain, as link dependence will be reduced (Gutierrez and Leal 2004, 6)[16].

[14] *De acordo com Negri (2007) as políticas brasileiras de atração do IDE não tiveram requisitos relacionados ao desenvolvimento doméstico de tecnologia por parte das multinacionais. Ao contrário, o Brasil adotou o entendimento que a simples presença estrangeira seria capaz de dinamizar a estrutura produtiva nacional e contribuir para a produção local de tecnologia, utilizando-se de uma política do tipo ‘portas abertas’* (Chiarini 2016, 294).

[15] These arguments remind us of the studies of the economist Albert Hirschman. However, as already mentioned, it is not the intention of this article to reproduce all the interpretations and theories of Latin American development.

[16] *O Brasil é um dos poucos países, entre as maiores economias mundiais, a não possuir um complexo eletrônico que contemple a manufatura de circuitos integrados. Além disso, a fabricação de bens eletrônicos no país restringe-se, com exceções, à montagem pura e simples a partir de um conjunto total de componentes importados (kits), o que agrega pouco valor aos produtos. A criação de uma indústria de circuitos integrados propiciará uma reversão dessa situação, fortalecendo a cadeia eletrônica na medida em que será reduzida a dependência de elos* (Gutierrez and Leal 2004, 6)

The value added locally by electronic companies has fallen, as corporations focus on importing ready-made kits, and the knowledge of integrating technology and engineering is getting lost. There are few sectors in which Brazil still has the capacity to develop competitive technologies, such as optical communication, banking automation, and commercial automation. However, the national software industry is obtaining good results (Lima and Moreira 2014).

Some examples of Brazil's technological dependence are mentioned below in terms of how much the US ICT industry has penetrated Brazil's critical infrastructures. The following arguments are illustrations of segments of the current infrastructure, given the knowledge gaps mentioned in the introduction. As the methodology of this study warned, one did not find any aggregate data available.

Brazilian civil, military, and government satellite communications depend on satellites built, owned, and managed by foreign companies: For example, the Embratel Star One series: Brasilsat A1 and A2: Spar Aerospace (Canada) built in partnership with Hughes Aircraft (United States); Brasilsat B1, B2, B3, and B4: Hughes Aircraft (United States); Star One C1 and C2: Alcatel Space (current Thales Alenia Space) (France); Star One C3: Orbital Sciences (United States); and Star One C4, D1, and D2 (in development) Space Systems Loral (United States) (Câmara dos Deputados 2010). Annual satellite services for monitoring and imaging, data, and telecommunications of Embrapa, INMET, Ibama, Caixa Econômica Federal, Casa Civil, the Institutional Security Office, the Ministry of Communications, the Ministry of Defense, and Petrobras are mostly provided by companies from the American military industrial complex and National Oceanic and Atmospheric Administration (Câmara dos Deputados 2010). The new Brazilian defense satellite (SGDC-1) was built by the French Thales Alenia Space (Fernandes 2015).

In terms of website servers, according to data from Telegeography only around 20% of Brazilian websites or websites accessed in Brazil are hosted in Brazil. Most data are hosted by US servers. These data are similar to the information presented as part of the Brazilian Digital Transformation Strategy. "Brazil represents 2.5% of the world's Internet traffic, 40% of IP traffic in Latin America, and is the Latin-American country with the biggest concentration of installed submarine cables. However, it is home of only 0.9% of all datacenters in the world" (Ministry of Science, Technology, Innovation, and Communications 2018, 67).

Airspace Control: The CINDACTA system (Integrated Center for Air Defense and Air Traffic Control) controls the Brazilian airspace. The system was built in the 1970s and developed by the French company Thomson, which is known today as Thales (Sousa and Sousa 2016). Meanwhile, the SIVAM system for monitoring Amazon was developed by Raytheon, an important American weapon company. This foreign technological dependence is well perceived by the Brazilian Air Force document *Plano Estratégico Militar da Aeronáutia 2010-2031:*

> The pursuit of national self-sufficiency in aeronautics, space, and military applications should be prioritized in order to reverse the current undesirable situation of heavy dependence of the Brazilian Air Force on foreign suppliers (especially for materials involving crucial technologies and export restrictions, according to the political criteria of their governments (Ministério da Defesa 2010, 85)[17].

According to sectorial research by Gomes and Fonseca (2014), our index of nationalization of technology in the aerospace sector is around 15% to 35% because most technological and extremely sensitive inputs come from international sources (Gomes and Fonseca 2014). For mobile phones and other similar ICT technologies, Brazil lacks a national company that has managed to master sensitive telecom segments. Companies operating in the domestic market are merely service providers and communications operators (Kubota and Sousa 2012). Furthermore, the domestic industry only assembles components of the mobile phone industry, such as Positivo Informatica (Lima and Moreira 2014; Fernandes 2015). Approximately 80% of network services in Brazil are private and international subsidiaries (Presidência da República 2010), and this situation remains unaltered (ANATEL 2019).

According to Jorge Henrique Cabral Fernandes—a professor at the Department of Computer Science of the Universidade de Brasilia—as long as the Brazilian critical and military infrastructures depend on foreign-made sensitive telecom components, Brazil will not have total defense capacity.

> Without semiconductors for data processing, telecommunications, consumer electronics, automotive production, and industrial automation (Ballhaus et al. 2012), Brazil's sovereignty is severely compromised. Although there are

[17] *A busca da auto-suficiência nacional em materiais aeronáuticos, espaciais e nos bélicos de emprego aeronáutico deve ser priorizada, de modo a reverter a indesejável situação atual, de forte dependência da Força Aérea Brasileira dos fornecedores estrangeiros (especialmente para materiais que envolvem tecnologias sensíveis e sofrem restrições para exportação, por critérios políticos dos governos dos seus fabricantes* (Ministério da Defesa 2010, 85).

> national computer and hardware industries, such as Positivo Informática, which is among the ten largest computer "manufacturers" in the world, all the chips used in the production line are produced outside the country. The design and technological development of these systems are not in the national domain (Fernandes 2015, 594)[18].

Through an IPEA's publication named *Amazônia e Atlântico Sul: desafios e perspectivas para a defesa no Brasil*, Fernandes (2015) asserts that Brazil needs to master the following high-tech segments to perfect its cyber defense and achieve a level of national cyber sovereignty: autonomous electrical energy systems, nanomaterials, high purity silicon wafers, semiconductors, microprocessor chips, controllers and data entry and exit devices, firmware and device drivers, operational systems and their utilities, programming language platforms, libraries of reusable software components, computational applications of all types and for all purposes, human-machine interfaces suitable for Brazilian culture and language, means of wired transmission in optical fiber and coaxial cables, means of wireless terrestrial transmission, means of satellite transmission of geostationary communication and low orbit; modems, gateways, switches and routers technologies, autonomous name service integrated to Iana, national symmetric and asymmetric cryptographic ciphers[19], semi-autonomous and decentralized public key infrastructures, and doctrines and exercises of joint action (Fernandes 2015, 623).

From the above, one cannot deny that Brazil has not mastered the high-tech layers of ICT chains. Thus, it has to import sensitive inputs for its critical infrastructure. As the *Plano Estratégico Militar da Aeronáutia* shows, such a dependence[20] on foreign high-tech sector has worried officials of the armed forces (Ministério da Defesa 2010, 85). The relations between the military–industrial

[18] *Sem semicondutores, seja para fins de processamento de dados, telecomunicações, eletrônica de consumo, produção automotiva e automação industrial (Ballhaus et al., 2012), o Brasil continua a ter sua liberdade de ação severamente comprometida, inclusive militar. Embora se tenha no país indústrias intituladas de informática e hardware, como a montadora Positivo Informática, que se encontra entre as dez maiores "fabricantes" de computadores do mundo,19 todos os chips empregados na linha de produção são produzidos fora do país. O projeto e avanço tecnológico desses sistemas também não são de domínio nacional* (Fernandes 2015, 594).

[19] To master cryptography, technics are important if one points out the fact an important Swiss cryptography company (Crypto AG), which has sold cryptography software to more than 120 governments worldwide, was in the middle of an international scandal, in which Crypto AG was actually controlled by the American Central Intelligence Agency. This way, US intelligence would have the source codes to break through the cryptography that was sold.

[20] It is not by chance that Russia and China have been managing to structure their own ICT and informational complex. International powers usually avoid being dependent on other nations when it comes to strategic sectors, even though nowadays it is not always viable due to the so-called complex interdependence and outsourcing economy.

complex and telecoms were clearly observed in the episode where Edward Snowden leaked Anglo-Saxon secret files in 2013. Snowden's (2013, 2014) materials suggest that digital surveillance, backdoors, and supply chain attacks have hit Brazil's federal government, although the details of these attacks are not completely clear. Some parts of the NSA slides were censured, which means that these materials were only available for a few groups in the NSA.

Should this episode confirm the concerns of the Brazilian military? According to Fernandes (2015), Brazil should avoid foreign ICT dependence due to cyber vulnerabilities. However, one cannot be completely sure that such a correlation exists. A significant amount of the available software and hardware segments, devices, and telecom infrastructure of the country should be checked to verify the quantitative data.

Conclusion

In short, by gathering theoretical concepts of international relations and cyber warfare, in addition to concrete evidence revealed by Snowden, it is possible to provide a general understanding of such an intricate hybrid war scenario. Although this study may help academics fill gaps in knowledge, it admits that such a qualitative approach is not sufficient to give an ultimate outcome.

Bearing in mind such methodological concerns, one claims that the United States has managed to foster its key companies, which had the state of the art of technology. They penetrate other nations' development projects and markets. This strategy has not only brought great economic benefits to the United States, but also astonishing international influence and cyber advantages in terms of cyber war apparatuses.

On the contrary, the integrity and sovereignty of Brazilian telecommunications have been attacked by US cyber war structures. Considering that Brazil is deeply dependent on the foreign ICT industry, particularly that of the United States, there might be a chance that such high-tech dependence is linked to cyber threats, such as those that Snowden has brought to light. This scenario implies that Brazilian authorities should invest in ICT and cyber defense strategies to strengthen cyber security. Further multidimensional studies are required from fields such as IT, cyber security, national defense, telecommunication engineering, and econometric studies to clarify quantitative data.

References

Agnew, John. 2008. "A Nova Configuração do Poder Global." Caderno CRH 21, no. 53 (August): 207-218. https://doi.org/10.1590/s0103-49792008000200002

ANATEL. 2019. "Panorama Setorial de Telecomunicações Dezembro / 2019." ANATEL. Accessed 23 July 2020. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4qMf2onqXJ2IxZmvnFSVufgZbJbUdg7uAnVfgtRoImouKz9k3MxWrrFBuu2W-up3_xD3pLjFvIEQGMca9Ll69I.

Andress, Jason, and Steve Winterfeld. 2013. Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners. Vol. 1. Boston, MA: Elsevier.

Bhutani, Ankita, and Preeti Wadhwani. "Aerospace Avionics Market Size by System (Flight Management System, Communication System, Navigation System, Surveillance System, Electric System, Emergency System, Collision Avoidance System, Weather System, Health Monitoring System, Tactical System, In-Flight Entertainment), by Application (Commercial Aviation, Military Aviation, Business Jet & General Aviation, Helicopters), by End Use (OEM, Aftermarket). Industry analysis report, regional outlook, growth potential, competitive market share, and forecast, 2019–2025." Global Market Insights 2019. Accessed on July 25, 2020. https://www.gminsights.com/industry-analysis/aerospace-avionics-market.

Bingham, Richard D. 2016. Industrial Policy American-style: From Hamilton to HDTV: From Hamilton to HDTV. New York, NY: Routledge.

Borrus, Michael, Dieter Ernst, and Stephan Haggard, eds. 2003. International Production Networks in Asia: Rivalry or Riches? London: Routledge.

Bradshaw, Samantha, and Laura DeNardis. 2018. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." New Media & Society 20, no. 1: 332-350.

Brzeziński, Zbigniew. 2016. The Grand Chessboard: American Primacy and its Geostrategic Imperatives. New York, NY: Basic Books.

Câmara dos Deputados. 2010. A Política Espacial Brasileira. Brasília: Centro de Documentação e Informação, Edições Câmara.

Cassiolato, José Eduardo, Marina Szapiro, Eduardo Maxnuck, Gabriela von Bochkor, Podcameni, João Marcos Hausmann, Marcelo Gerson Pessoa de Matos, and Patrick Fontaine. 2013. "Fronteiras Tecnológicas Subordinadas às Estratégias Nacionais de Desenvolvimento: As Experiências dos Estados Unidos da América, da China, do Japão e da Alemanha." In Dimensões Estratégicas do Desenvolvimento Brasileiro, edited by Maisa Cardoso, v. 2. Brasília: Centro de Gestão e Estudos Estratégicos.

Cervo, Amado Luiz, and Clodoaldo Bueno. 2002. História da Política Exterior do Brasil. Brasília: Instituto Brasileiro de Relações Internacionais/Editora da Universidade de Brasília.

Chiarini, Tulio. 2016. "A Inércia Estrutural da Base Produtiva Brasileira: O IDE e a Transferência Internacional de Tecnologia." Brazilian Journal of Political Economy 36, no. 2: 286-308.

Chomsky, Noam. 1993. Rethinking Camelot: JFK, Vietnam War, and US Political Culture. Montreal: Black Rose Books.

Clement, Andrew. "NSA Surveillance: Exploring the Geography of Internet Interception." In iConference 2014 Proceedings, 412-425. http://hdl.handle.net/2142/47305.

Cohen, Saul Bernard. 2014. Geopolitics: Geography of International Relations. Lanham, MD: Rowman & Littlefield.

Correia, Pedro de Pezarat. "Geopolítica e Geoestratégica." In Carriço, A., Coord, 2012. Nação e Defesa Segurança em África. Lisboa: Instituto de Defesa Nacional, no. 131, 229-246.

Clarke, Richard A., and Robert K. Knake. 2010. Cyber War. Old Saybrook, CT: Tantor Media.

Deibert, Ron. 2015. Geopolitics of Cyberspace after Snowden. Current History 114, no. 768: 9-15. https://doi.org/10.1525/curh.2015.114.768.9.

DeNardis, L. 2015. Global War for Internet Governance. 1st ed. New Haven, CT: Yale University Press.

European Parliament. 2001. Draft Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System). Brussels: European Parliament.

Fernandes, Jorge Henrique Cabral. 2015. "A Perniciosa Armadilha Cibernética e uma Proposta de Mobilização Nacional." In Amazônia e Atlântico Sul: Desafios e Perspectivas para a Defesa no Brasil, organized by Gilberto Fernando Gheller, Selma Lúcia de Moura Gonzales, and Laerte Peotta de Melo. Brasília: Instituto de Pesquisa Econômica Aplicada.

Grimes, Seamus, and Debin Du. 2020. "China's Emerging Role in the Global Semiconductor Value Chain." Telecommunications Policy, (April): 101959. https://doi.org/10.1016/j.telpol.2020.101959.

Gutierrez, Regina Maria Vinhais, and Cláudio Figueiredo Coelho Leal. 2004. Estratégias para uma Indústria de Circuitos Integrados no Brasil. 1st ed. Rio de Janeiro: Banco Nacional de Desenvolvimento Econômico e Social.

Gomes, Sergio B. Varella, and Paulus Vinicius da Rocha Fonseca. 2014. Aeroespacial. In Perspectivas do Investimento 2015-2018 e Panoramas Setoriais. Rio de Janeiro: Banco Nacional de Desenvolvimento Econômico e Social.

Hagedoorn, John. 2002. "Inter-firm R&D Partnerships: An Overview of Major Trends and Patterns Since 1960." Research Policy 31, no. 4: 477-492. https://ideas.repec.org/a/eee/respol/v31y2002i4p477-492.html.

Hart, Jeffrey A., and Sangbae Kim. 2002. "Explaining the Resurgence of US Competitiveness: The Rise of Wintelism." The Information Society 18, no. 1: 1-12.

Herrera, Amílcar O. 1995. "Los Determinantes Sociales de la Política Científica en América Latina. Política Científica Explícita y Política Científica Implícita." Redes 2, no. 5: 117-131.

Kissinger, Henry. 2015. World Order. New York, NY: Penguin Books.

Kubota, Luis Claudio, and Rodrigo Abdalla Filgueiras de Sousa. 2012. "Tecnologias da Informação e Comunicação: Competição, Políticas e Tendências." In Tecnologias da Informação e Comunicação: Competição, Políticas e Tendências, organized by Luis Claudio Kubota, Rodrigo Abdalla Filgueiras de Sousa, Marcio Wohlers de Almeida, and Fernanda DeNegri. Brasília: Instituto de Pesquisa Econômica Aplicada.

Lima, Ricardo Rivera de Sousa, and Diego Moreira. 2014. "Telecomunicações." In Perspectivas do Investimento 2015-2018 e Panoramas Setoriais. Rio de Janeiro: Banco Nacional de Desenvolvimento Econômico e Social.

Loveluck, Benjamin. 2015. Réseaux, Libertés et Contrôle: Une Généalogie Politique d' Internet. Paris: Armand Colin.

Lins, Bernardo Felipe Estellita. 2017. Histórico da Legislação de Telecomunicações no Brasil. Estudo Técnico da Consultoria Legislativa. 1st ed. Vol. 1. Brasília: Camera dos Deputados.

Mazzucato, Mariana. 2014. Entrepreneurial State: Debunking Public vs. Private Sector Myths. 1st ed. London: Penguin Books,.

Mearsheimer, John J. 2019. "Bound to Fail: The Rise and Fall of the Liberal International Order." International Security 43, no. 4: 7-50.

Medeiros, José Adelino de, and Sérgio Alves Perilo. 1990. "Implantação e Consolidação de um Pólo Tecnológico: O Caso de São José dos Campos." Revista de Administração de Empresas 30, no. 2: 35-45.

Ministério da Defesa. 2010. PEMAER — Plano Estratégico Militar da Aeronáutia 2010–2031. Brasília: Ministério da Defesa.

Ministry of Science, Technology, Innovation, and Communications. 2018. Brazilian Digital Transformation Strategy (E-digital). Brasília: Ministry of Science, Technology, Innovation, and Communications.

National Research Council. 1996. Conflict and Cooperation in National Competition for High-technology Industry: A Cooperative Project of the Hamburg Institute for Economic Research, Kiel Institute for World Economics, and National Research Council on "Sources of International Friction and Cooperation in High-technology Development and Trade." Washington, D.C.: National Academy Press.

Nye, Joseph S. 2011. The Future of Power. New York, NY: Public Affairs.

Pelton, Joseph N., Scott Madry, and Sergio Camacho-Lara, eds. 2017. Handbook of Satellite Applications. New York, NY: Springer.

Pereira Filho, José Eduardo. 2002. "A Embratel: da Era da Intervenção Ao Tempo da Competição." Revista de Sociologia e Política, no. 18: 33-47.

Pinto, Marcel Arins. 2015. A Estrutura da Liderança Norte-Americana no Espaço Digital e na Internet. master's diss. Universidade Federal de Santa Catarina. https://repositorio.ufsc.br/handle/123456789/156746

Powers, Shawn M., and Michael Jablonski. 2015. The Real Cyber War: The Political Economy of Internet Freedom. University of Illinois Press.

Presidência da República. 2010. Livro Verde de Segurança Nacional. Brasília: Presidência da República.

Qiao, Liang, Al Santoli, and Xiangsui Wang. 2015. Unrestricted Warfare. Brattleboro, VT: Echo Point Books & Media.

Ruiz, Jeanette B., and George A. Barnett. 2015. "Who Owns the International Internet Networks?" Journal of International Communication 21, no. 1: 38-57.

Santos, Isabel Cristina dos, and João Amato Neto. 2005. "Estratégias para Criação da Indústria Aeroespacial Brasileira." Revista Brasileira de Gestão e Desenvolvimento Regional 1, no. 2. https://www.rbgdr.net/revista/index.php/rbgdr/article/view/69.

Schiller, Herbert I. 1992. Mass Communications and American Empire. Boulder, Oxford: Westview Press.

Snowden, Edward. 2013. Intelligently Filtering Your Data: Brazil and Mexico Case Studies. Snowden Doc Search. Accessed January 5, 2020. https://search.edwardsnowden.com/docs/IntelligentlyfilteringyourdataBrazilandMexicocasestudies2013-12-02_nsadocs_snowden_doc.

Snowden, Edward. 2014. Private Networks are Important. Snowden Doc Search. Accessed January 5, 2020. https://search.edwardsnowden.com/docs/PrivateNetworksareImportant2014-05-13_nsadocs_snowden_doc.

Sousa, Francisco Fabrício Ribeiro de, and Sérgio Barros de Sousa. 2016. "Análise dos Sistemas Computacionais Críticos Utilizados no Controle de Tráfego Aéreo Brasileiro." Revista Brasileira de Computação Aplicada 8, no. 3: 66-84. https://doi.org/10.5335/rbca.v8i3.6018.

Teixeira, Francisco Lima Cruz. 2005. "Desenvolvimento Industrial e Tecnologia: Revisão da Literatura e uma Proposta de Abordagem." Cadernos EBAPE.BR 3, spe: 1-16.

Telebrasil. 2004. Telebrasil: 30 Anos de Sucesso e Realizações. Rio de Janeiro: Telebrasil.

The United States Office of Technology Assessment. 1985. International Cooperation and Competition in Civilian Space Activities. Washington, D.C.: U.S. Congress, Office of Technology Assessment.

The United States Senate Committee on Foreign Relations, Subcommittee on Multinational Corporations. 1975. Multinational Oil Corporations and U.S. Foreign Policy; Report Together with Individual Views. Washington: U.S. G.P.O.

Van Putte, Michael A. 2016. Walking Wounded: Inside the US Cyberwar Machine. CreateSpace Independent Publishing Platform.

Vianna, Eduardo W. 2019. "Segurança da Informação Digital: Proposta de Modelo para a Ciber Proteção Nacional." PhD diss. Universidade de Brasília.

Whalen, David J. 2002. Origins of Satellite Communications, 1945–1965. Washington D.C.: Smithsonian Institution Press.

Whalen, David J. 2014. The Rise and Fall of COMSAT: Technology, Business, and Government in Satellite Communications. Houndmills, Basingstoke, Hampshire; New York, NY: Palgrave Macmillan.