Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil

Análise Comparativa das Regulações para Segurança e Defesa Cibernética nos Estados Unidos e no Brasil

Rev. Bras. Est. Def. v. 6, nº 2, jul./dez. 2019, p. 93–123
DOI: 10.26792/RBED.v6n2.2019.75149
ISSN 2358-3932

VITELIO BRUSTOLIN

INTRODUCTION: DIFFERENCES AND INTERSECTIONS BETWEEN CYBERSECURITY AND CYBER DEFENCE

Cybersecurity is "the governance, development, management and use of information security, OT security,[1] and IT security[2] tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries" (Walls 2003). Cyber defence, on the other hand, is "a computer network defence mechanism which includes response to actions and critical infrastructure protection and information assurance for organisations, government entities and other possible networks" (Galinec, Možnik, and Guberina 2017).

Therefore, cyber defence is a level above cybersecurity, ensuring the execution of processes and activities, free of threats. Cyber defence also helps to improve the capabilities and uses of the security strategy (Galinec, Možnik, and Guberina 2017). Cybersecurity and cyber defence work together (or should work), as will be discussed throughout this article.

Considering that Brazil is part of the comparison here presented, it is important to clarify the definition of "cyber defence" that guides the Brazilian Army:

Vitelio Brustolin – Research Scientist at Harvard Law School, Postdoctoral Researcher in the Harvard Department of the History of Science, Adjunct Professor at Columbia University in the School of International and Public Affairs, and University Professor at Institute of Strategic Studies and International Relations (INEST) of the Fluminense Federal University (UFF). Cambridge, Massachusetts, USA.

> The set of defensive, exploratory and offensive actions in the context of a military planning carried out in the cyberspace, with the purpose of protecting our information systems, obtaining data for the production of intelligence and causing damage to information systems of the opponent (Ministry of Defence of Brazil 2014, 18).

The Institutional Security Office of the Presidency of Brazil (GSI)[3] makes the following distinction between these concepts: "the scope of cybersecurity action comprises aspects and attitudes of both prevention and repression. For cyber defence it is understood that it comprises operational actions of offensive combat" (Institutional Security Office of the Presidency of Brazil 2010: 19).

It should be noted that Cybernetics is one of the areas listed as a priority by the National Defence Strategy of Brazil (END),[4] alongside Nuclear and Spatial. The END guidelines have a clear motivation: cyber-attacks are a threat, either because of their harmful effects on information stored in databases, or for potential damage in the concrete world — the interconnection of which goes from financial institutions to hospitals, through complex government systems.

Because of this, governments and business organisations around the world have been scrambling to protect their systems. To do so, some cyber defence tools and techniques are used, while hackers try to break through security systems, sending malicious software such as botnets, viruses and trojans viruses, among others, to access valuable data. Despite these efforts, the situation is progressively worsening due to new types of malware developed (Al-Mohannadi et al. 2016). In this scenario, it is important to understand the public initiatives employed in different countries aimed at circumventing these attacks, in order to extract lessons that can be adapted and used in different contexts.

It should be noted that the Internet originated as a military enterprise in the United States (USA or US), where the international providers and the largest companies in the area are also concentrated. It is therefore crucial to analyse the policies adopted by the USA in the fight against cyber-attacks. Table 1 presents the key milestones in the creation of the Internet:

Table 1
Key Milestones in the Development of the Internet

1946	The first electronic computer, called "Eniac", is created for the purpose of performing calculations for the US Army laboratory.
1950	The "Rand Project", which started connecting computers, is developed.
1958	The "ARPA"[5] is founded to foster US technology within the Department of Defence during the Cold War.
1968	The first demonstration of "ARPANET" is made, creating a network of computers.
1973	A Norwegian government agency, Norsar, is the first European institution to connect to ARPANET.
1977	The TCP/IP protocol is created (*Transmission Control Protocol/Internet Protocol*).
1983	The ARPANET is demilitarized and the military part forms MILNET.

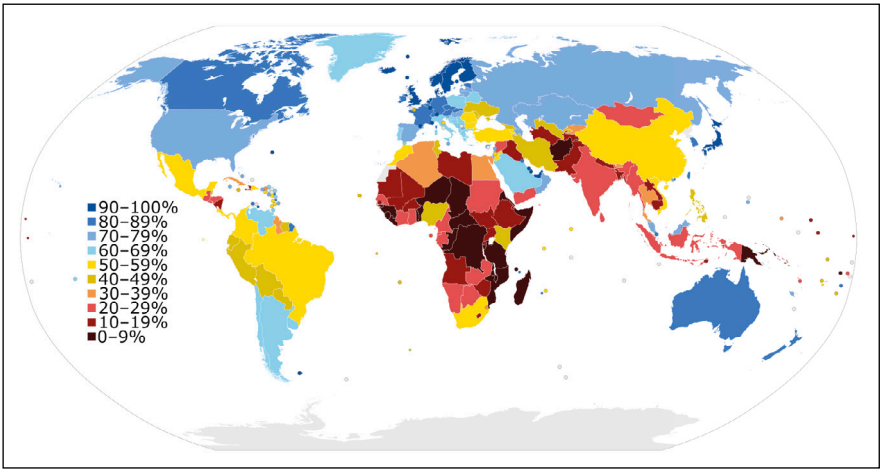
Source: Own elaboration based on bibliographical research (Abbate 1999; Ruthfield 1995: 2-4; Brustolin 2014: 29).

That being said, it is a common practice, both in scientific research and in the governmental sphere, to analyse regulations of other nations and evaluate if they are successful and if some of their aspects are adaptable to their own needs. In this sense, studying US regulations for cybersecurity and cyber defence, in addition to being in accordance with the basic premises of science and with the precepts of efficiency in public administration, can contribute to prevent cyber-crimes in Brazil.

CYBER-ATTACKS

Cyber-attacks are a real risk to the interconnected global infrastructure from hospital care to the functioning of banking and government systems. These attacks have increased over the years and have recently become larger and more dangerous, crippling both public and private systems worldwide (Presse 2017).

The International Telecommunication Union (ITU), an agency of the United Nations (UN), created in 1957 and covering all 193-member countries of the UN, estimates that more than 3 billion people are direct Internet users in the world. Map 1 (below) outlines this number, as a percentage of the population in each country (International Telecommunication Union (International Telecommunication Union 2016, 8).



Map 1 – Percentage of Internet Users by Country.
Source: International Telecommunication Union (2016: 13).

It should be noted that Brazil and the United States are listed in Map 1 as having, respectively, 50-59% (BR) and 70-79% (USA) of their populations as Internet users. This data was published in 2016. Since 2016 the number of Internet users in Brazil has continued to grow, as can be seen in the following 2018 data from the ITU below:

Telecommunications Indicators in Brazil and the United States

Table 2

Key indicators for Brazil (2017)		The Americas	World
Fixed-telephone sub. per 100 inhab.	19.5	23.9	13.0
Mobile-cellular sub. per 100 inhab.	113.0	111.8	103.6
Active mobile-broadband sub. per 100 inhab.	90.2	89.5	61.9
3G coverage (% of population)	95.5	93.9	87.9
LTE/WiMAX coverage (% of population)	83.1	84.3	76.3
Individuals using the Internet (%)	67.5	67.5	48.6
Households with a computer (%)	46.3	64.8	47.1
Households with Internet access (%)	60.8	68.3	54.7
International bandwidth per Internet user (kbit/s)	*29.0*	77.1	76.6
Fixed-broadband sub. per 100 inhab.	13.7	19.9	13.6
Fixed-broadband sub. by speed tiers, % distribution			
-256 kbit/s to 2 Mbit/s	*23.4*	6.6	4.2
-2 to 10 Mbit/s	*34.5*	23.1	13.2
-equal to or above 10 Mbit/s	*42.1*	70.3	82.6

Note: Data in italics are ITU estimates. Source: ITU (as of June 2018).

Table 3

Key indicators for United States (2017)		The Americas	World
Fixed-telephone sub. per 100 inhab.	37.0	23.9	13.0
Mobile-cellular sub. per 100 inhab.	123.3	111.8	103.6
Active mobile-broadband sub. per 100 inhab.	132.9	89.5	61.9
3G coverage (% of population)	99.9	93.9	87.9
LTE/WiMAX coverage (% of population)	99.8	84.3	76.3
Individuals using the Internet (%)	*75.2*	67.5	48.6
Households with a computer (%)	*88.8*	64.8	47.1
Households with Internet access (%)	*87.0*	68.3	54.7
International bandwidth per Internet user (kbit/s)	*125.4*	77.1	76.6
Fixed-broadband sub. per 100 inhab.	33.9	19.9	13.6
Fixed-broadband sub. by speed tiers, % distribution			
-256 kbit/s to 2 Mbit/s	0.9	6.6	4.2
-2 to 10 Mbit/s	13.5	23.1	13.2
-equal to or above 10 Mbit/s	85.6	70.3	82.6

Note: Data in italics are ITU estimates. Source: ITU (as of June 2018).

Source: International Telecommunication Union (2018: 26 and 191).

Table 2 shows that for every 100 people in Brazil, 67.5 are direct Internet users, the same average in the Americas and above the world average, which is 48.6%. The numbers are slightly higher in the United States (Table 3), where for every 100 individuals, 75.2 are direct users of the Internet.

In addition to direct Internet users, there are those who are indirectly affected by the Internet. In other words, companies and governments rely on cyberspace for a variety of activities, from financial transactions to the movement of military forces. Electric power companies, for example, depend on industrial control systems connected to the Internet to provide power to the grid. In addition, shipmasters use satellites and the Internet to monitor freighters while navigating the global sea lanes, while the military rely on secure networks and data to accomplish their missions (Department of Defence USA 2015, 1).[6]

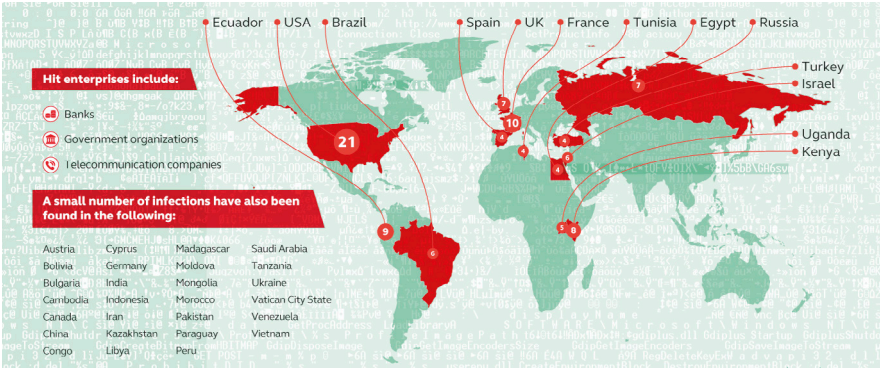
The updated versions of Brazil's National Defence Policy (PND),[7] as well as its National Defence Strategy (END)[8] and its White Paper on National Defence,[9] attribute the responsibility of cyber defence in the country to the Brazilian Army (Ministry of Defence of Brazil 2012, 200). The cybernetics area is also listed as one of the three priorities for the country (Brazil 2012, 36).

As mentioned in the introduction of this article, considering that the Internet originated from a military enterprise in the United States and has the largest concentration of Internet providers and companies, it is important to analyse what initiatives have been employed by the US government to combat cyber-attacks (Brustolin 2014, 29).

This necessity is based on concrete facts: unprecedented and worldwide cyber-attacks have also affected Brazil. In 2017 several companies and public agencies had to shut down their computers, interrupt their services and/or suffered from malfunctioning websites, among them:

- Petrobras.[10]
- National Social Security Institute (INSS)[11] throughout Brazil.
- Courts of Justice in several Brazilian states: São Paulo, Sergipe, Roraima, Amapá, Rio Grande do Sul, Mato Grosso do Sul, Minas Gerais, Rio Grande do Norte, Piauí, Bahia and Santa Catarina.
- São Paulo Public Prosecutor's Office.
- Itamaraty (Ministry of Foreign Affairs).
- Brazilian Institute of Geography and Statistics[12] (IBGE), (Presse 2017).

Worldwide cyberattacks in 2017 in government agencies and companies are displayed in Map 2 (below).

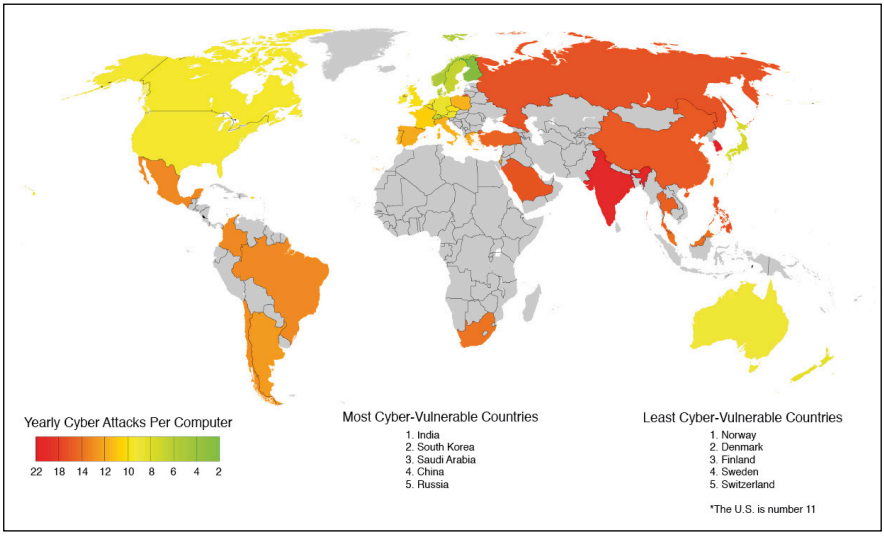


Map 2 – Worldwide Cyber-attack Targets.
Source: AO Kaspersky Lab (2017).

This survey covers 140 organisations in 40 countries, but does not include the more than 300 million personal computers that were infected — in at least 170 countries. In May 2017 alone, in the largest global cyber-attack ever recorded was the result of the release of a ransomware virus called WannaCry (Quesada and Cano 2017). It would be anticipated that by preventing or minimising cyber-attacks, by improving technology and policy, would also have protect personal computer users.

In 2018, the Centre for Studies, Response and Treatment of Internet Incidents in Brazil (Cert.br)[13] accounted for 678 thousand incidents in the country. The figures, which are only those reported to Cert.br, are lower than those for 2017, but almost doubled compared with five years earlier (Benevides 2019).

Map 3 shows the average of the cyber-attacks suffered annually by different countries. While the United States has an average of 11 attacks per computer per year, the numbers in Brazil are slightly higher, with about 12 to 14 attacks per computer per year:



Map 3 – Average of the Cyber-attacks Suffered Annually by Different Countries. Source: The Global Cyber-Vulnerability Report (2015).

Map 3 was created based on data provided by Symantec security company to track the frequency with which individual hosts, or computers, are targeted in several countries. The authors of the map analysed over 20 billion reports generated by more than 4 million computers (mostly personal and business machines) protected by Symantec products in 44 countries over a 2-year period. The data were published in December 2015 (Subrahmanian et al 2015).

SECURITY AND CYBER DEFENCE REGULATIONS IN THE UNITED STATES

The main regulations for security and cyber defence in the United States are presented below. This compilation does not aim to be exhaustive, giving priority to the most significant documents.

Federal Government (USA)

There are few federal regulations for cybersecurity in the United States and those that exist focus on specific industries (Kiyuna and Conyers 2015, 76). The three main regulations are:

1. The 1996 Health Insurance Portability and Accountability Act (HIPAA).[14]

2. The 1999 Gramm-Leach-Bliley Act.[15]
3. The 2002 Homeland Security Act.[16]

These regulations dictate that healthcare organisations, financial institutions, and federal agencies must protect their own systems and information (Schooner and Berteau 2014).

Department of Defence (USA)

The United States Department of Defence (DoD) released in 2011 an orientation called "Department of Defence Strategy for Operating in Cyberspace".[17] The main initiatives of the document are:

1. Create partnerships with other agencies and the private sector in the pursuit of a "Whole-of-government cybersecurity Strategy".
2. Work with international partners in support of collective cybersecurity.
3. Support the development of a cybernetic workforce capable of rapid technological innovation.

Two years later, in November 2013, DoD introduced a new cybersecurity rule to its contractors, in which it demanded:[18]

- Compliance with safety standards of the National Institute of Standards and Technology (NIST).
- Mandatory reports of cybersecurity incidents to DoD.
- A clause that applies the same requirements to subcontractors.

Government System (USA)

On 16 November 2018, President Donald Trump sanctioned the "Cybersecurity and Infrastructure Security Agency Act of 2018" (The United States of America 2018a). The Act transforms the National Protection and Programs Directorate (NPPD),[19] into the Cybersecurity and Infrastructure Security Agency (CISA), with increased assignments. The focus of this Agency is the protection of government networks, with the extension ".gov", but it also monitors the private sector, as publicised: "Federal government; state, local, tribal and territorial governments; the private sector and international partners" (Department of Homeland Security USA 2018a). Although it is unclear which companies are protected and who are the international partners, it is evident that protection does not extend to the rest of the Internet in the country (Department of Homeland Security USA 2018b).

It is important to note that the counterintelligence operations of the National Security Agency (NSA) and the Department of Homeland Security (DHS) have intersections in their work. While the NSA is responsible for national security information systems, the DHS seeks to protect all US government data and respond quickly to any cyber threat (The National Security Agency 2019).

In addition, the United States makes "defensive cyber operations" with the participation of the DoD. For this there is the so-called "Active Cyber Defence" (ACD), which unites DoD resources to those of US intelligence agencies. The ACD focus, however, is not on the Internet in general in the US, but rather on "government agencies and organisations, defence contractors, critical infrastructure segments, and industry" (The National Security Agency 2019).

BEYOND THE REGULATIONS

The US federal government has also been allocating resources for research and collaboration with the private sector for cyber defence and cybersecurity. (Kiyuna and Conyers 2015, 77). This initiative is justified in public documents such as the "National Cyber Strategy of the United States of America". In the September 2018 edition the countries that are currently considered threats to the United States in the area are cited:

> Russia, Iran, and North Korea conducted reckless cyber-attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors — including terrorists and criminals — exploited cyber-space to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states (The United States of America 2018b, 1-2).

In addition, the DoD Cyberstrategy of 2018 complements the above statement:

> We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long term strategic risk to the Nation as well as to our allies and partners (Department of Defence of the United States of America 2018, 1).

The United States will spend US$ 15 billion on cybersecurity in 2019 (US$ 583.4 million more than in 2018). Spending in the area has been in-

creasing steadily every year. This, however, is not yet the total expenditure. According to the government, "due to the sensitive nature of some activities, this amount does not represent the entire cyber budget" (The White House 2018, 273). The Department of Defence will receive most of the resources, reaching almost US$ 8.5 billion. Second comes the Department of Homeland Security, with US$ 1.7 billion (The White House 2018, 273).

By 2020, the budget for cybersecurity will be US$ 17.4 billion. Again, this should not be the total expense, but the other expenses in the area are classified. By 2020, the DoD should receive US$ 9.6 billion and the DHS US$ 1.91 billion (The White House 2019, 305).

THE CYBERSECURITY ACT OF 2012 AND OTHER REGULATORY ATTEMPTS

A bipartisan bill, the Cybersecurity Act of 2012 (S.2105) was proposed by two senators Joseph Lieberman (Democrat) and Susan Collins (Republican), in July of that year (Kiyuna and Conyers 2015, 77–78). Barack Obama, who was president at the time, openly expressed his support for the initiative (Fitzpatrick 2012). In debate in the Senate, the bill was opposed by many Republican Senators, including John McCain, who had been a candidate for the presidency of the United States. McCain said he was concerned about the introduction of regulation that, in his words, "would not be effective and could be a 'burden' for businesses" (Kiyuna and Conyers 2015, 78).

The Democrats lead by Obama were a minority in the Senate at the time, and although the votes did not strictly follow partisan lines, the bill was defeated (Fitzpatrick 2012). Experts warned that failure to approve the bill "could leave the nation vulnerable to widespread hacking or a serious cyberattack" (O'Keefe and Nakashima 2012). This vulnerability would, ironically, be observed in the 2016 Presidential Election, as will be discussed in the next sections.

In the years that followed, President Obama tried three more times to change regulations and policies for cybersecurity in the country (Kiyuna and Conyers 2015, 78). No proposal, however, would have the same scope and level of protection as the Cybersecurity Act of 2012:

– February 2013: "The Executive Order Improving Critical Infrastructure Cybersecurity". One of the highlights of the Order would be the deepening of public-private partnerships, as well as the exchange of information between the Department of Homeland Security and critical infrastructure companies (Office of the Press Secretary, The White House 2013).

– January 2015: a new "Cybersecurity Legislative Proposal". One of the main points of the Proposal would be to provide tools and training for law enforcement authorities to deal more effectively with cybercrime (Office of the Press Secretary, The White House 2015).
– February 2016: "Cybersecurity National Security Action Plan". Among the proposals, we highlight the creation of a "Commission on Enhancing National Cybersecurity". This would be composed of a group of analysts with varied perspectives to make diversified recommendations in the area (Office of the Press Secretary, The White House 2016).

All three of the proposals listed above would need to be approved by the Legislative to become laws. Given the election of Donald Trump in 2016, this is unlikely to happen.

MAIN INITIATIVES ENVISAGED IN THE CYBERSECURITY ACT OF 2012

The Cybersecurity Act of 2012 envisaged public-private partnerships and a co-ordinated framework to protect critical infrastructures in the United States. These would be its main initiatives:

Table 4
The Cybersecurity Act of 2012 (S.2105) — Planned Major Initiatives[20]

1. "**Determine the Greatest Cyber Vulnerabilities**. The bill would require the Secretary of Homeland Security, in consultation with the private sector, the Intelligence Community, and others, to conduct risk assessments to determine which sectors are subject to the greatest and most immediate cyber risks.
2. **Protect Our Most Critical Infrastructure**. The bill would authorise the Secretary of Homeland Security, with the private sector, to determine cybersecurity performance requirements based upon the risk assessments. The performance requirements would cover critical infrastructure systems and assets whose disruption could result in severe degradation of national security, catastrophic economic damage, or the interruption of life-sustaining services sufficient to cause mass casualties or mass evacuations. The bill would only cover the most critical systems and assets in a given sector, and only if they are not already being appropriately secured.
3. **Protect and Promote Innovation**. Owners of "covered critical infrastructure" would have the flexibility to meet the cybersecurity performance requirements in the manner they deem appropriate. The private sector also would have the opportunity to develop and propose performance requirements for "covered critical infrastructure." The bill would prohibit the government from regulating the design or development of information technology products.

(*Continue*)

(*Continuation*)

4. **Improve Information Sharing While Protecting Privacy and Civil Liberties**. As the sophistication of cyber threats and attacks has grown, it is increasingly clear that improved information sharing is a vital tool to combat cybercrime and espionage, and to alert owners of our nation's most critical infrastructure of cyber threats to their systems and assets. Both the government and the private sector collect valuable cyber threat information. This bill would provide a responsible framework for the sharing of cyber threat information between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties.
5. **Improve the Security of the Federal Government's Networks**. To strengthen the security and resilience of federal government systems, the bill would amend the Federal Information Security Management Act (FISMA) and require the federal government to develop a comprehensive acquisition risk management strategy. The amendments to FISMA would move agencies away from a culture of compliance to a culture of security by giving the Department of Homeland Security authority to streamline agency reporting requirements and reduce paperwork through continuous monitoring and risk assessment. The bill would emphasise "red team" exercises and operational testing to ensure federal agencies are aware of their networks' vulnerabilities. By directing OMB to develop security requirements and best practices for federal IT contracts, the bill would also ensure agencies make informed decisions when purchasing IT products and services.
6. **Clarify the Roles of Federal Agencies**. The bill would clarify and improve federal efforts to address cyber threats. The bill would strengthen the critical partnership between the Department of Defence and the Department of Homeland Security. It would consolidate existing cyber offices at the Department of Homeland Security into a unified National Centre for Cybersecurity and Communications to carry out the Department's current responsibilities for protecting the networks of federal civilian agencies and critical infrastructure. Existing relationships between infrastructure owners and government agencies, as well as existing oversight frameworks, would remain intact, wherever possible, to avoid duplication.
7. **Strengthen the Cybersecurity Workforce**. The bill would reform the way cybersecurity personnel are recruited, hired, and trained to ensure that the federal government has the necessary talent to lead and manage the protection of its own networks.
8. **Co-ordinate Cybersecurity Research and Development**. The bill would provide for a co-ordinated cybersecurity R&D program to advance the development of new technologies to secure our nation from ever-evolving cyber threats".[21]

The effects of not implementing some of these initiatives planned in the Cybersecurity Act of 2012 will be discussed in the next section.

FAILURES IN US CYBERSECURITY AND CYBER DEFENCE IN 2016 PRESIDENTIAL ELECTION

As many experts had predicted, the fact that the 2012 Cybersecurity Act was not enacted left the US "vulnerable to widespread hacking or a serious cyberattack" (O'Keefe and Nakashima 2012). This vulnerability was noted in the Presidential Election 2016, which suffered interference from the Russian government as officially verified by multiple Law Enforcement and Intelligence Agencies (Office of the Director of National Intelligence 2017). This interference hampered Hillary Clinton's campaign, increasing the odds of a Donald Trump presidency and growing political and social discord in the United States. The conclusions are presented in the Mueller Report, officially called "Report on the Investigation into Russian Interference in the 2016 Presidential Election" (Mueller 2019).

The Mueller Report concluded that Russian interference violated US criminal law. As a result, 26 Russian nationals and three Russian organisations were indicted. According to the report, at least two methods were employed by the Russian government:

1. The of use profiles on social media, with "Internet trolls" and spreading fake news

2. The hacking by the Russian Intelligence Service (GRU) into email accounts of volunteers and employees of the Hillary Clinton presidential campaign, as well as the hacking of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC).

The stolen documents were released in stages to influence public opinion during the three months prior to the 2016 election. Hackers released the leaked documents to the websites WikiLeaks, DCLeaks, and Guccifer 2.0. (Meyer, Moe, and Connor 2016).

If the Cybersecurity Act of 2012 had been enacted and was enforced in 2016, at least three US cybersecurity and cyber defence vulnerabilities could have been mitigated:

1. DHS, in consultation with the Intelligence Community and the private sector (especially social media companies) could have acted to reduce fake profiles and fake news.

2. Public-private partnerships could have prevented the cyber hacking of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC).

3. Civilian talent recruited to work in cybersecurity could have acted proactively and detected that two of the leak platforms belonged to the Russian Intelligence: DCLeaks and Guccifer 2.0. This was established by

the Mueller Report in 2019 and was released very late by the CIA in 2016. It should be noted that alerting citizens about the Russian interference in the election could have directly influenced public opinion.

4. Finally, a "responsible framework for the sharing of cyber threat information between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties",[22] could have prevented most of the threats during the 2016 Presidential Election.

REGULATIONS FOR SECURITY AND CYBER DEFENCE IN BRAZIL

As well as the previous listing of the main regulations for cybersecurity and cyber defence of the United States, below is presented a listing of the main regulations produced by Brazil. Again, these listings are not intended to be exhaustive, prioritising the most expressive regulations.

Federal Government (Brazil)

Decree 5.484/2005:[23] approves the "Policy of National Defence" (PDN),[24] the document was updated in 2012, when it came to be called the "National Defence Policy" (PND).[25] The last update (from 2016) was legislatively enacted in 2018.[26] The cybernetic area was directly mentioned in only two points of the original Policy. On the other hand, the original Policy anticipated the improvement of "security devices and procedures that reduce the vulnerability of systems related to National Defence against cyber-attacks".[27] The importance of the cybernetic area grew with the prioritisation "of the three sectors", made by the National Defence Strategy (below). The next versions of the Policy would give an increasing importance and space to the cyber sector.

Decree 6.703/2008: approves the National Defence Strategy. The Strategy prioritises Brazilian national autonomy, emphasising autonomous technological empowerment and focusing on the "spatial, cybernetics and nuclear" sectors.[28] It is from this document that cybernetics officially has a prominent role for the Armed Forces of Brazil, being assigned as a priority to the Army. The spatial sector is fundamentally delegated to the Air Force and the nuclear sector to the Navy. The Strategy is periodically updated every four years. The last update, of 2016, was legislatively enacted in 2018.[29]

Law 12.737/2012: typifies crimes related to cybersecurity. This Law is known as "Carolina Dieckmann Law," in reference to the leak of photos by the homonymous actress in 2012.[30] The penalty for those who illegally

access a cell phone or computer account is short: from three months to a year in detention, "which in practice means that it is very difficult for someone to be arrested in Brazil for attacking and stealing information from a third-party device" (Amorim 2019). There is also a statute of limitation of four years.

Law 12.965/2014: known as the "Civil Internet Framework".[31] This Law was elaborated through public consultation.[32] Subsequently, the regulation was replicated by other countries, such as Italy (Canabarro 2014). This Law devotes a section to the protection of records, personal data and private communications between people.[33] In that Section, preserves the content of communications between people if at least one of the terminals is located in Brazil, or if the economic group that is offering the communication service has a branch in Brazil.[34] While creating legal mechanisms to ensure Internet security, the Law does not directly address cyber defence.

Decree 8.491/2015: assigns to the "Centre for Cyber Defence" (CDCiber), competence to:[35]

- Advise the Army Commander and the Defence Minister on the activities of the cyber sector.
- Formulate doctrine.
- Obtain and employ technologies.
- Plan, guide and control operational activities.
- Plan, guide and control the doctrinal activities and development of cybernetic capabilities.[36]

Law 13.709/2018, with adjustments of Law 13.853/2019:[37] "General Law of Personal Data Protection"[38] (fully effective from 2020). This Law protects the data of individuals and companies. The Law helps cybersecurity, but is not applied to:

1. Public safety data.
2. National defence data.
3. State safety data.
4. Investigation and prosecution of criminal offenses.[39]

Decree 9.637/2018: creates the National Information Security Policy. It outlines the principles, objectives, instruments, attributions and powers of information security for federal agencies in Brazil. It also foresees the elaboration of the National Cybersecurity Strategy.[40]

Decree 10.222/2020: approves the National Cybersecurity Strategy of Brazil (called "E-Ciber"). The Strategy is valid from 2020 to 2023. One of the highlights of the document is section 2.2, which outlines its objectives:

1. Make Brazil more prosperous and reliable in the digital environment.
2. Increase Brazilian resilience to cyber threats.
3. Strengthen Brazilian cybersecurity operations on the international stage.

One of the actions foreseen in the Strategy is the creation of "a centralized model of cyber governance in Brazil" (section 2.3.2). Despite this centralization, the Strategy also advocates the creation of "a participatory, collaborative and secure environment, between public organizations, private institutions, academia and society" (section 2.3.3).

In addition, the Strategy establishes the expansion of Brazil's international cooperation in cybersecurity, "with as many countries as possible" (section 2.3.8).[41]

Institutional Security Office (Brazil)

In 2010 the Institutional Security Office published the "Green Paper: Cybersecurity in Brazil".[42] The book is a public document, that presents as "fundamental to develop a set of collaborative actions among government, private sector, academia, third sector, and society, to deal with the mosaic of aspects that cross cybersecurity" (Institutional Security Office 2010, 14).[43] The document distinguishes between the concepts "cybersecurity" and "cyber defence" as presented in the Introduction of this article (Institutional Security Office 2010, 19).[44]

Ministry of Defence (Brazil)

Ordinance 666/2010: creates the Centre for Cyber Defence, attached to the Army Command.[45]

Ordinance 3.389/2012: approves the "Cyber Defence Policy".[46] Among the highlights of the document, we emphasise:[47]

1. "The effectiveness of Cyber Defence actions in the MD depends directly on the degree of awareness reached among organisations and individuals about the value of the information they hold or process".[48] That is, the Ministry of Defence makes clear that joint action is needed with organisations and citizens so that the cyber defence of the country can be effective. This point is reinforced in the following item:

2. "Information and Communications Security (SIC)[49] is the basis of cyber defence and depends directly on individual actions; there is no cyber defence without SIC actions". This text could not be clearer: without individual actions — of all people — there is no cyber defence. This is the limit of action established by the Ministry of Defence itself:

3. "Cybernetic actions in the context of MD are aimed at ensuring the use of cyberspace, preventing or hindering its use against the interests of the country and thus guaranteeing freedom of action".[50]

Another point that stands out is the possibility of recruiting personnel to act in cyber defence. The Cyber Defence Policy makes room for talents outside the Armed Forces, although it is unclear whether they could be civilians in general or just civil public servants. In addition, it is not outlined how, in practise, such recruitment would be carried out: "identify, register and select personnel with skills or abilities, existing in the internal and external environments of the FA".[51]

Ordinance 3.405/2012: it assigns to the Centre for Cyber Defence the responsibility for the coordination and integration of the activities of cyber defence within the scope of the Ministry of Defence, according to the provisions of the National Defence Strategy.[52]

White Paper on National Defence: it was released in 2012. Although cyber defence has a prominent role in the document, it is clear that a low investment is expected in the area. For the period from 2011 to 2035 (that is, 24 years) are expected to be R$ 839.90 million. The budget is not mentioned in the 2016 White Paper update, which was legislatively enacted in 2018.[53]

Normative Ordinance of the Ministry of Defence 3.010/2014: This regulation approves the Military Doctrine of Cyber Defence of Brazil. The document — already mentioned earlier in this article — presents concepts, limitations and forms of cyber defence operations in the country.[54]

CYBERSECURITY AND CYBER DEFENCE ISSUES IN BRAZIL

It is important to note that this study focuses on cyber-attacks. However, cases of external interference in elections through fake news are considered national security issues in any country. That being said, in a similar way to the United States, Brazil had cases of fake profiles in social media and fake news, targeting the 2018 Presidential Election. In the Brazilian case, however, there is no evidence of interference from other countries. In order to determine what had happened, in 2019 the National Congress established a Parliamentary Inquiry Commission[55] — CPI — (Federal Senate of Brazil 2019).

In addition, the Superior Electoral Court (TSE)[56] had to restrict services provided via the Internet in an attempt to reduce cyber-attacks (Superior Electoral Court of Brazil 2019). Four years earlier, on the weekend of the first round of general elections in 2014, the TSE had received 200 thousand cyber-attacks per second (Superior Electoral Court of Brazil 2019).

In another case that became famous, in June 2019, The Intercept website began publishing alleged conversations by Brazilian authorities. The conversations would have been obtained in the Telegram application, illegally, by an anonymous source (Greenwald and Pougy 2019).

These are just a few of the many cases that show how government, companies and citizens are exposed to cybercrime and cyber-attacks in Brazil. To these facts are added others, already mentioned throughout this article, in the section "Cyber-attacks".

As in the US case, regulations such as the Cybersecurity Act of 2012 would have substantially reduced these problems. Similar to the US proposal, the form of confrontation could also be:

1. Determine the greatest cyber vulnerabilities. Clearly Brazil was not prepared for fake social media profiles or the spread of fake news that occurred during the 2018 Presidential Election, despite the events two years earlier in the United States. At the same time, no government action was taken to counteract these efforts this was partially due to the lack of regulation.

2. Protect and promote innovation. Hacking of communication between senior officials shows that the country needs to better safeguard critical information shared in messaging apps. There are safer forms of communication and when it comes to public officials and more advanced technology should be to prevent the exposure of the country to external interference.

3. Improve information sharing while protecting privacy and civil liberties. Information sharing should aim to protect the population, not the exposure of individuals or sale of their data by criminals.

4. Public-private partnerships. Cybersecurity and cyber defence cannot be provided only by the State. The collaboration of the private sector is necessary. At the same time, a legal and institutional arrangement is necessary to make this possible.

5. Civilian talent recruited to act proactively. Among the three areas prioritised in Brazil's National Defence Strategy (cybernetics, nuclear and spatial), cybernetics is the one that most needs the collaboration of civilians. The Brazilian Army does not have enough structure to provide cyber defence for the whole country. This is expressly stated in the Ordinance 3.389/2012.

6. To organise the activities of the Centre for Cyber Defence of the Brazilian Army, the Institutional Security Office, the Brazilian Intelligence Agency (ABIN)[57] and the Federal Police (PF), would be useful to Brazil. The integration between cybersecurity and cyber defence is essential, because without it, it is not possible for institutions to act effectively. This

integration is pursued by the Cybersecurity Act of 2012: "The bill would clarify and improve federal efforts to address cyber threats... Existing relationships between infrastructure owners and government agencies, as well as existing oversight frameworks, would remain intact, wherever possible, to avoid duplication".[58]

FINAL CONSIDERATIONS

There are clear differences between the approaches proposed by the Obama administration and the Trump administration in cybersecurity and cyber defence regulations in the United States. Obama sought formation of councils, commissions, and partnerships with private initiative, as well as the recruitment of civilian talent. On the other hand, Trump is pursuing a more centralised approach, in which cyber defence is provided by the government. As Obama's proposals failed to pass Congress, the centralising paradigm has prevailed.

The main justification for the Cybersecurity Act of 2012 not passing Congress is that the Act would be invasive. That is, the government would have too much power over the privacy of people. However, there was no parliamentary discussion on accountability, which could hold public agents accountable for the misuse of information.

At the same time, the public debate over the regulation of the Internet in the United States has certainly been influenced by the publication of leaked documents by the Wikileaks platform. These leaks reveal the actions of governments and public agents, including espionage (Bridge 2018). The leaks have been published, in a continuous stream since December 2006. Certainly, the leaks also influenced the discourse on Internet regulation and public policy in the rest of the world, including Brazil.

Although the Cybersecurity Act of 2012 failed to pass Congress in advance of the leak of classified information by Edward Snowden, such leaks are certainly having influence on public discussion of governments actions on cybersecurity and cyber defence. In 2013, Snowden was hired by the NSA, after working at Dell and the CIA. In May of 2013, Snowden left the job in the NSA and also left the USA (Burrough, Ellison, and Andrews 2014). In June, he revealed thousands of confidential NSA documents to journalists from The Guardian, the Washington Post, Der Spiegel and The New York Times (Gellman and Soltani 2013). On 5 June 2013, media reports documenting the existence and functions of classified surveillance programs and their scope began and continued throughout the year (Greenwald and MacAskill 2013).

Given these facts, a current discussion on Internet regulation should include accountability mechanisms for public agents.

In fact, because of scandals and leaks like those reported above, people do not trust the government to protect their privacy. However, the government already has the most information on individuals, since identifiable data are used in the issuance of documents such as certificates, passports, driver's licenses, or in income tax returns, for example. On the other hand, some Internet companies, such as social media platforms, hold large amounts of personal information of other types, such as political preferences, product searches, contracting services, etc. It is now impractical to ensure that such information will not be misused, sold, invaded or leaked if there is no regulation — as has already happened with Facebook (Tynan 2018). Even with regulation it would already be difficult to protect the data, with regulation, at least there would be legal instruments that could be used by government agents.

In parallel, most people trust the State to provide them with public safety, or for the Army to defend the country in the case of war. Why the mistrust when it comes to cybersecurity? The misuse of information by governments, evidenced by confidential documents made public by websites such as Wikileaks, for example, makes people less confident in the State when it comes to their privacy. In addition, the feeling of being constantly watched over by a "Big Brother" as described in George Orwell's famous "1984" book[59] compels people to distrust the government in this "trade off" between cyber defence and privacy.

Trust, in this case, can only be established with the perception that the rules serve both individuals in general and public agents. That is, public agents should be held liable if there is an abuse of power or inappropriate use of private information. To this end, it is necessary to create supervisory and control mechanisms that are also applied to government agents. Given the large number of citizens, the overwhelming majority of data will be analysed by cyber threat software, not by people. This software is programmable and verifiable.

Certain data that some people fear to be analysed by governments, are shared openly on social media platforms, since not all individuals care about protecting their information. It is important to raise awareness about what the Internet is and how information is distributed and recorded on the Internet.

There is a price to pay for security, and most of the time this price is a reduction of privacy. In times of over-connectivity, it is the lack of regulation that encourages invasion of privacy and not the existence of reg-

ulation. The rules, as described above, should equally apply to individuals and public agents responsible for their cyber safety.

That being said, from the comparison between the main regulations employed by the United States and Brazil for their respective cybersecurity and cyber defence, we produced four main conclusions:

1. The absence of an effective public policy for cybersecurity and cyber defence in the United States left the country vulnerable to Russian cyber-attacks that influenced the course of the 2016 Presidential Election.

2. The Cybersecurity Act of 2012 would have increased US protection against cyber-attacks. However, the bill was defeated in the Senate of the country.

3. If Brazil had a regulation similar to the Cybersecurity Act of 2012, the country would have prevented most of the fake news and cyber-attacks that occurred in its own 2018 Presidential Election.

4. As demonstrated throughout this article, among all the proposed cybersecurity and cyber defence regulations made so far in both the United States and Brazil, the Cybersecurity Act of 2012 is the most comprehensive. The main initiatives foreseen in the bill can still be implemented by both countries. Such implementation would depend on extensive public debate, but the results would bring potential benefits to both countries.

This work was supported by CAPES [Funding Number 23069.041588/2018-08, Finance Code 001].

Acknowledgments: I am grateful to Alex Csiszar and Peter Louis Galison (Department of the History of Science, Harvard University); Roberto Mangabeira Unger (Harvard Law School); Eurico de Lima Figueiredo (Institute of Strategic Studies and International Relations of the Fluminense Federal University); Alice Ma; Sarah Block; CAPES and Lemann Foundation.

REFERENCES

Abbate, Janet. 1999. *Inventing the Internet*. Cambridge: MIT Press.

Al-Mohannadi, Hamad et al. 2016. "Cyber-Attack Modeling Analysis Techniques: An Overview". Paper delivered at 4th International Conference on Future Internet of Things and Cloud Workshops. Vienna, Austria 22-24 Aug. https://ieeexplore.ieee.org/abstract/document/7592703.

Amorim, Silvia. 2019. "Lei brasileira ainda é insuficiente para punir hackers". *O Globo*, 7 July.

AO Kaspersky Lab. 2017. *APT Trends report, Q1 2017. An Expert Take on Targeted Attack Operations*. Russian Federation, Moscow. https://securelist.com/analysis/quarterly-malware-reports/78169/apt-trends-report-q1-2017.

Benevides, Bruno. 2019. "Brasil entra na mira de hackers e vira alvo de ciberataques do exterior". *Folha de S. Paulo*, 6 July.

Brazil. 2005. *Decree 5.484, of 30 June 2005*. Brasília, Presidency of the Federative Republic of Brazil.

Brazil. 2008. *Decree 6.703, of 18 December 2008*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2018. *Decree 9.637 of 26 December 2018*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2020. *Decree 10.222 of 5 February 2020*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2012. *Law 12.737, of 30 November 2012*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2012 [2005, 2016]. *National Defence Policy*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2012 [2008, 2016]. *National Defence Strategy*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2014. *Law 12.965, of 23 April 2014*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2015. *Decree 8.491, of 13 July 2015*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2018. *Law 13.709, of 14 August 2018*. Brasília, Presidency of the Federative Republic of Brazil.

_____. 2019. *Law 13.853, of 8 July 2019*. Brasília, Presidency of the Federative Republic of Brazil.

Bridge, Mark. 2018. "Loss of internet forces Assange to step down from Wikileaks editor role". *The Times*, 27 September.

Brustolin, Vitelio. 2014. "Innovation and Development through National Defence in the USA and Brazil". PhD Thesis, Universidade Federal do Rio de Janeiro & Harvard University.

Burrough, Bryan, Sarah Ellison, and Suzanna Andrews. 2014. "The Snowden Saga: A Shadowland of Secrets and Light". *Vanity Fair*, 23 April.

Canabarro, Diego. 2014. "A contribuição do Brasil para o Marco Civil da Internet na Itália". *Observatório da Internet no Brasil* [online]. 23 October. https://observatoriodainternet.br/post/a-contribuicao-do-brasil-para-o-marco-civil-da-internet-na-italia.

Department of Defence of the United States of America. 2011. *Department of Defence Strategy for Operating in Cyberspace*. Washington DC, USA: DoD.

_____. 2013. *78 FR 23601*. Federal Register 78, no. 76, 19 April. Washington DC, USA: Government Publishing Office.

_____. 2015. *The Department of Defence Cyberstrategy*. Washington DC, USA: DoD.

_____. 2018. *Department of Defence Strategy for Operating in Cyberspace*. Washington DC, USA: DoD.

Department of Homeland Security of the United States of America. 2018a. *What Does CISA Do?* Washington DC, USA: DHS. www.dhs.gov/CISA.

_____. 2018b. *Cybersecurity*. Washington DC, USA: DHS. www.dhs.gov/topic/cybersecurity.

Federal Senate of Brazil. 2018. *Legislative Decree 179, of 14 December 2018*. Brasília: Brazil.

_____. 2019. "Congresso cria CPI Mista para investigar fake News". Senado Notícias, 3 July. www12.senado.leg.br/noticias/audios/2019/07/congresso-cria-cpi-mista-para-investigar-fake-news.

Fitzpatrick, Alex. 2012. "Cybersecurity Bill Stalls in the Senate". *Mashable*, 2 August.

_____. 2012. "Obama Gives Thumbs-Up to New Cybersecurity Bill". *Mashable*, 20 July.

Galinec, Darko, Darko Možnik, and Boris Guberina. 2017. *Cybersecurity and cyber defence: national level strategic approach*. Automatika 58, no. 3, 273–286, DOI: 10.1080/00051144.2017.1407022.

Gellman, Barton, and Ashkan Soltani. 2013. "NSA infiltrates links to Yahoo, Google data centres worldwide, Snowden documents say". *The Washington Post*, 1 November.

Greenwald, Glenn, and Ewen MacAskill. 2013. "Boundless Informant: the NSA's secret tool to track global surveillance data". *The Guardian*, 8 June.

Greenwald, Glenn, and Victor Pougy. 2019. "As mensagens secretas da Lava Jato". *The Intercept*, 9 June.

Institutional Security Office of the Presidency of Brazil. 2010. *Green Paper: Cybersecurity in Brazil*. Brasília: Presidency of the Republic of Brazil.

International Telecommunication Union. 2016. *Measuring the Information Society Report 2016*. Geneva Switzerland: United Nations.

_____. 2018. *Measuring the Information Society Report 2018: Volume 2*. Geneva, Switzerland: United Nations.

Kiyuna, A., and L. Conyers. 2015. *Cyberwarfare Sourcebook*. Morrisville, USA: Lulu.

Meyer, Josh, Alex Moe, and Tracy Connor. 2016. "Hack of Democratic Congressional Campaign Committee 'Similar' to DNC Breach". *NBC News*, 29 July.

Ministry of Defence of Brazil. 2010. *Bulletin of the Army: 31/2010*. Brasília, Brazil: Command of the Army, 6 August.

_____. 2010. *Ordinance 3.389, of 21 December 2012*. Brasília, Brazil: MD.

_____. 2012. *Bulletin of the Army: Number 52/2012*. Brasília, Brazil: Command of the Army, 28 December.

_____. 2012 [2016]. *White Paper on National Defence*. Brasília, Brazil: MD.

_____. 2014. *Military Doctrine of Cyber Defence*. Brasília, Brazil: Command of the Army.

Mueller, Robert. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington DC: US Department of Justice. https://www.justice.gov/storage/report.pdf.

North American Energy Standards Board. 2017. *The Cybersecurity Act of 2012*. Houston, USA: naesb.org.

O'Keefe, Ed, and Ellen Nakashima. 2012. "Cybersecurity bill fails in Senate". *Washington Post*, 2 August.

Office of the Director of National Intelligence (USA). 2017. *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Washington DC, USA: DNI. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the Press Secretary, The White House (USA). 2013. *Executive Order: Improving Critical Infrastructure Cybersecurity.* Washington DC, USA: White House, 12 February. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

_____. 2015. *President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts.* Washington DC, USA: White House, 13 January. https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

_____. 2016. *Cybersecurity National Action Plan.* Washington DC, USA: White House, 9 February. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Orwell, George. 1949. *1984.* Boston/New York, USA: Houghton Mifflin Harcourt.

Presse, France. 2017. "Ataque de hackers sem precedentes provoca alerta no mundo". *O Globo*, 13 May.

Quesada, Juan, and Rosa Cano. 2017. "O ciberataque: apertar um botão e desligar o mundo". *El País*, 21 May.

Ruthfield, Scott. 1995. "The Internet's History and Development from Wartime Tool to the Fish-Cam". *Crossroads Magazine* 2 no. 1 (September).

Schooner, Steven, and David Berteau. 2014. "Emerging Policy and Practice Issues". Washington DC, USA: GW Law Faculty Publications. https://scholarship.law.gwu.edu/faculty_publications/1056.

Senate of the United States of America. 2012. *S.2105 — Cybersecurity Act of 2012.* Washington DC, USA: Congress.gov. www.congress.gov/bill/112th-congress/senate-bill/2105/text.

Subrahmanian, V. et al. 2015. *The Global Cyber-Vulnerability Report.* Springer International Publishing.

Superior Electoral Court of Brazil. 2019. "Portal do TSE restringe serviços para prevenir ataques cibernéticos". *TSE Communication Advisory*, 27 October. www.tse.jus.br/imprensa/noticias-tse/2018/Outubro/portal-do-tse-restringe-servicos-para-prevenir-ataques-ciberneticos.

The National Security Agency. 2019. *Active Cyber Defence*. Washington DC, USA: NSA. https://apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defence.cfm.

_____. 2019. *What is NSA's role in U.S. cybersecurity?* Washington DC, USA: NSA. www.nsa.gov/What-We-Do/Cybersecurity.

The United States of America. 1996. *Public Law 104-191*. Washington DC, USA: Government Publishing Office.

_____. 1999. *Public Law 106-102*. Washington DC, USA: Government Publishing Office.

_____. 2002. *Public Law 107-296*. Washington DC, USA: Government Publishing Office.

_____. 2018a. *Cybersecurity and Infrastructure Security Agency Act of 2018*. Congress Bills. Washington DC, USA: Govtrack. www.govtrack.us/congress/bills/115/hr3359.

_____. 2018b. *National Cyber Strategy of the United States of America*. Washington DC, USA: Government Publishing Office.

The White House, United States of America. 2018. *Cybersecurity Funding*. Washington DC, USA: White House.

_____. 2018. *Cybersecurity Funding*. Washington DC, USA: White House.

_____. 2019. *Cybersecurity Funding*. Washington DC, USA: White House.

Tynan, Dan. 2018. "Facebook says 14m accounts had personal data stolen in recent breach". *The Guardian*, 12 October.

Walls, Andrew, Earl Perkins, and Juergen Weiss. 2013. *Definition: Cybersecurity*. Stamford, USA: Gartner Inc.

NOTAS

1. "Operational Technology".
2. "Information Technology Security".
3. "Gabinente de Segurança Institucional", in Portuguese.
4. "Estratégia Nacional de Defesa", in Portuguese.
5. "ARPA" (Advanced Research Projects Agency) would later be renamed to "DARPA" (Defence Advanced Research Projects Agency).
6. This Cyberstrategy was updated in 2018, as quoted in other parts of this article.
7. "Política Nacional de Defesa", in Portuguese.
8. The aforementioned "Estratégia Nacional de Defesa".
9. "Livro Branco de Defesa Nacional", in Portuguese.
10. Abbreviation of "Petróleo Brasileiro S.A.", a Brazilian oil and gas company.
11. "Instituto Nacional do Seguro Social", in Portuguese.
12. "Brazilian Institute of Geography and Statistics", in Portuguese.
13. "Centro de Estudos, Resposta e Tratamento de Incidentes de Internet no Brasil", in Portuguese.
14. The United States of America. 1996. *Public Law 104-191*. Washington DC, USA: Government Publishing Office.
15. The United States of America. 1999. *Public Law 106-102*. Washington DC, USA: Government Publishing Office.
16. The United States of America. 2002. *Public Law 107-296*. Washington DC, USA: Government Publishing Office.
17. Department of Defence of the United States of America. 2011. *Department of Defence Strategy for Operating in Cyberspace*. Washington DC, USA: DoD.
18. Department of Defence of the United States of America. 2013. *78 FR 23601*. Federal Register Volume 78, Issue 76, April 19. Washington DC, USA: Government Publishing Office.
19. NPPD is a Directorate of the Department of Homeland Security.
20. Senate of the United States of America. 2012. *S.2105 — Cybersecurity Act of 2012*. Washington DC, USA: Congress.gov.
21. North American Energy Standards Board. 2017. *The Cybersecurity Act of 2012*. Houston, USA: naesb.org.
22. As transcribed in Table 4.
23. Brazil. 2005. *Decree 5.484, of 30 June 2005*. Brasília: Presidency of the Federative Republic of Brazil.
24. "Política de Defesa Nacional", in Portuguese.
25. "Política Nacional de Defesa", in Portuguese.

26. Federal Senate of Brazil. 2018. *Legislative Decree 179, of 14 December 2018*. Brasília: Brazil.
27. Brazil. 2005. *Decree 5.484, of 30 June 2005*. Brasília, Presidency of the Federative Republic of Brazil. [Section 7.1, XII; and 6.19].
28. Brazil. 2008. *Decree 6.703, of 18 December 2008*. Brasília, Presidency of the Federative Republic of Brazil.
29. Federal Senate of Brazil. 2018. *Legislative Decree 179, of 14 December 2018*. Brasília, Brazil.
30. Brazil. 2012. *Law 12.737, of 30 November 2012*. Brasília, Presidency of the Federative Republic of Brazil.
31. "Marco Civil da Internet", in Portuguese.
32. Brazil. 2014. *Law 12.965, of 23 April 2014*. Brasília, Presidency of the Federative Republic of Brazil.
33. Brazil. 2014. *Law 12.965, of 23 April 2014*. Brasília, Presidency of the Federative Republic of Brazil. [Section II].
34. Brazil. 2014. *Law 12.965, of 23 April 2014*. Brasília, Presidency of the Federative Republic of Brazil. [Art. 11, § 2º].
35. Brazil. 2015. *Decree 8.491, of 13 July 2015*. Brasília, Presidency of the Federative Republic of Brazil.
36. Art. 11-B of Decree 5.751/2006, amended by the above-mentioned Decree 8.491/2015.
37. Brazil. 2019. *Law 13.853, of 8 July 2019*. Brasília, Presidency of the Federative Republic of Brazil.
38. "Lei Geral de Proteção de Dados Pessoais (LGPD)", in Portuguese.
39. Brazil. 2018. *Law 13.709, of 14 August 2018*. Brasília, Presidency of the Federative Republic of Brazil. [Art. 4, III: a, b, c, d].
40. Brazil. 2018. Decree 9.637 of 26 December 2018. Brasília, Presidency of the Federative Republic of Brazil.
41. Brazil. 2020. Decree 10.222 of 5 February 2020. Brasília, Presidency of the Federative Republic of Brazil.
42. Institutional Security Office of the Presidency of Brazil. 2010. *Green Paper: Cybersecurity in Brazil*. Brasília: Presidency of the Republic of Brazil.
43. Institutional Security Office of the Presidency of Brazil. 2010. *Green Paper: Cybersecurity in Brazil*. Brasília: Presidency of the Republic of Brazil. p. 14.
44. Institutional Security Office of the Presidency of Brazil. 2010. *Green Paper: Cybersecurity in Brazil*. Brasília: Presidency of the Republic of Brazil. p. 19.
45. Ministry of Defence of Brazil. 2010. *Bulletin of the Army: Number 31/2010*. Brasília, Brazil: Command of the Army, 6 August.

46. "Política Cibernética de Defesa", in Portuguese.
47. Ministry of Defence of Brazil. 2010. *Ordinance 3.389, of 21 December 2012*. Brasília, Brazil: MD.
48. Ministry of Defence of Brazil. 2010. *Ordinance 3.389, of 21 December 2012*. Brasília, Brazil: MD. [Section 1.3, e].
49. "Segurança da Informação e Comunicações", in Portuguese.
50. Ministry of Defence of Brazil. 2010. *Ordinance 3.389, of 21 December 2012*. Brasília, Brazil: MD. [Section 1.3, g].
51. Ministry of Defence of Brazil. 2010. *Ordinance 3.389, of 21 December 2012*. Brasília, Brazil: MD. [Section 3.2.2, d].
52. Ministry of Defence of Brazil. 2012. *Bulletin of the Army: Number 52/2012*. Brasília, Brazil: Command of the Army, 28 December.
53. Federal Senate of Brazil. 2018. *Legislative Decree 179, of 14 December 2018*. Brasília: Brazil.
54. Ministry of Defence of Brazil. 2014. *Military Doctrine of Cyber Defence*. Brasília, Brazil: Command of the Army.
55. "Comissão Parlamentar de Inquérito", in Portuguese.
56. "Tribunal Superior Eleitoral", in Portuguese.
57. "Agência Brasileira de Inteligência", in Portuguese.
58. As transcribed in Table 4.
59. Orwell, George. 1949. *1984*. Boston/New York, USA: Houghton Mifflin Harcourt.

COMPARATIVE ANALYSIS OF REGULATIONS FOR CYBERSECURITY AND CYBER DEFENCE IN THE UNITED STATES AND BRAZIL

ABSTRACT

In this article we compare the main regulations employed by the United States and Brazil for their respective cybersecurity and cyber defence. From this comparison we produced four main conclusions. First, the absence of an effective public policy for cybersecurity and cyber defence in the United States left the country vulnerable to Russian cyber-attacks that influenced the course of the 2016 Presidential Election. Second, the Cybersecurity Act of 2012, which was supported by Barack Obama, who was President at the time, would have increased US protection against cyber-attacks. However, the bill did not become law because it was defeated in the US Senate. Third, if Brazil had enacted legislation similar to the Cybersecurity Act of 2012, the country would have prevented most of the fake news and cyber-attacks that occurred in its own 2018 Presidential Election. Fourth, the main initiatives of the Cybersecurity Act of 2012 can still be implemented by both the United States and Brazil. To reach these conclusions, we compared intended purpose of the Cybersecurity Act of 2012, with facts that highlight the consequent failures in cybersecurity and cyber defence in the United States and Brazil.

Keywords: Cybersecurity; Cyber Defence; Cyber-attacks; Cybersecurity Act of 2012; Internet Regulation; Cyber Safety in the United States; Cyber Safety in Brazil.

RESUMO

Neste artigo são comparadas as principais regulamentações empregadas pelos Estados Unidos e pelo Brasil para as suas respectivas segurança e defesa cibernéticas. A partir dessa comparação, são produzidas quatro conclusões principais. Primeira: a ausência de uma política pública eficaz de segurança e defesa cibernética nos Estados Unidos deixou o país vulnerável aos ciberataques russos que influenciaram o resultado da Eleição Presidencial de 2016. Segunda: a Proposta de Lei de Segurança Cibernética de 2012, que foi apoiada pelo então presidente Barack Obama, teria aumentado a proteção dos EUA contra ataques cibernéticos. No entanto, a Proposta foi derrotada no Senado dos EUA. Terceira: se o Brasil tivesse promulgado uma regulamentação semelhante à Lei de Segurança Cibernética de 2012, o país teria bloqueado a maioria das notícias falsas e dos ataques cibernéti-

cos que ocorreram em sua própria Eleição Presidencial de 2018. Quarta: as principais iniciativas da Proposta de Lei de Segurança Cibernética de 2012 ainda podem ser implementadas — tanto pelos Estados Unidos quanto pelo Brasil. Para se chegar a essas conclusões, foram comparadas as principais iniciativas propostas pela Lei de Segurança Cibernética de 2012 com fatos que demonstram falhas na segurança e defesa cibernética dos Estados Unidos e do Brasil.

Palavras-chave: Segurança Cibernética; Defesa Cibernética; Ataques Cibernéticos; Projeto de Lei de Segurança Cibernética de 2012; Regulação da Internet; Cibersegurança nos Estados Unidos; Cibersegurança no Brasil.

Recebido em 18/10/2019. Aceito para publicação em 03/03/2020.