Notes on the militarization of Brazilian cybersecurity: current state of affairs and perspectives on the near future

Raquel Jorge de Oliveira

Abstract: In this work, I reflect on the state of Brazilian cybersecurity practices, and how they have been conceptualized in laws and in official documents, such as national strategies. Based on literature review, I argue that this is a militarized domain, which could have not only political consequences, but also societal ones. I conclude by arguing for the need for involving other sectors of society in order to deal with cybersecurity challenges in a more effective and adequate manner. I conclude that, by making a partial diagnosis of what cyber threats are and not implementing effective coordination measures, even at the governmental level, Brazil puts itself in a vulnerable position when it comes to a challenge that will stretch well into the next decades by militarizing its handling of the issue.

As is commonly the case in research endeavours, what is found is not necessarily what was initially expected. This study began as a research proposal of a comparative analysis between the cyber strategies implemented by Nordic countries, Estonia and Brazil. The principal objective was to find if there were any similarities between the approaches these actors adopted, and what the differences between their outlooks and proposed solutions were. The study seemed to be justified in its contribution to the understanding of how present and future cyber challenges could be faced given the theme's growing relevance.

Throughout the research, it became progressively clear that Brazil concentrated a significant portion of its cybersecurity capabilities in the military domain. More importantly, this concentration stemmed not only from the vague prescriptions established in the country's main strategic documents - the National Defense Strategy, the National Defense Policy, and the National Cybersecurity Strategy (E-Ciber) -, but from practice, that is, the way in which cybersecurity was actually handled institutionally.

This is significant not only because it puts into question the efficiency of the Brazilian approach, but also, and perhaps mainly, because it highlights the consequences such military prominence may have over civilian affairs. Even if the cyber domain plays a fundamental role in current military innovation trends, and nobody disputes that it does, its innovation locus is not nested within military structures, not even within the government, but in universities and in private businesses. Similarly, the brunt of Information Communication Technology (ICT) users, for example, is not made of government officials or armed forces officers, but of civilians.

There are two main issues to take into consideration when talking about cyber strategies. The first one is correctly diagnosing the problem at hand, thus building a comprehensive understanding of its nature. The second issue is crafting an action protocol which addresses the problem and lists practical steps to solve it. The large scope of actors involved in the cyber domain alone means at the very least that a policy-building coalition which does not take this into consideration will not be effective in responding to challenges. Additionally, partial understandings of what actually can be done through cyber jeopardize security initiatives.

In this scenario, would a military-centric approach be appropriate? I argue in this work that it would not. Mainly because the cybersecurity problem is not principally a military problem, but a common one also involving civilians. Unnecessarily militarizing issues that should be dealt with in the public policy sphere means lending armed officers overarching prominence over matters that do not quite concern the realm of armed conflicts (Strachan, 2014).

If only one piece of information is remembered from this work, let it be that cyber threats are eminently hybrid and have challenged the distinction between times of conflict and times of peace.

We live in the grey zone (Braw, 2021). This means that cyber crosses several domains of knowledge and society, so approaches that do not recognize this fundamental fact will not be complete (Bressan and Sulg, 2020). The internet is everywhere, so in contemporary life we are deeply dependent on electronic communication devices for a wide range of activities, from the most commonplace to the most strategic. Thus, cyber increased the possible surface of attack for malicious actors that take advantage of these weaknesses to not only undertake attacks on critical infrastructure, but also, and mainly, on the resilience of a given population (Pauwels, 2019; Wigell, 2019; Bradshaw, Bailey and Howard, 2021). Modern conflicts have gone through changes that point towards the use of the civilian contingent to destabilize adversaries. Disinformation campaigns are an instrument that serve this purpose, for example, by taking advantage of existing weaknesses. It should be noted that not only foreign actors can make use of this technique (Hanson et al., 2019).

One should also take into consideration human rights, particularly in regards to privacy in the digital age (Mendes, 2008; Mendes and Fonseca, 2020; Bioni, 2021). Enormous amounts of personal information about citizens are available because of their intensive use of ICTs. Should the military have unfettered access to and authority over that source, under the auspices of a cybersecurity strategy? Human rights can be affected in securitization processes related to migration crisis, terrorism, global health crises or other complex themes (Office of the United Nations High Commissioner for Human Rights, 2008; Lamer, 2017; Lopez, 2017; Nuñez-Mietz, 2019; Eck and Hatz, 2020), opening the way to legally sanctioned surveillance. A particularly troublesome prospect, especially in a country with a contentious past of democratic diastoles and systoles.

This is, therefore, a topic which merits further consideration by scholars interested in cybersecurity writ large, particularly when applied to the Brazilian context. This paper builds on the conclusions made by Diniz et al. (2014) and pushes the subject forward by discussing the implications the discernible militarization of Brazilian cybersecurity has for the country. The subject has been framed by Brazilian authorities in war-adjacent terms, which, at best, is a disputed possibility among scholars (Hansen and Nissenbaum, 2009; Rid, 2012; Valeriano and Maness, 2014, 2016, 2018). Apocalyptic attacks on critical infrastructures are possible, but rare and unlikely, since most cyber attacks are of low intensity. I argue that the biggest challenge brought about by the cyber issue is not a hypothetical war fought in cyberspace, but the erosion of the social fabric through hybrid attacks.This paper's objective, then, is to draw attention to Brazil's cybersecurity practices, thus encouraging debates about them.

The article is divided as follows. In the first section, I will comment on Brazil's main laws and strategies pertaining to cybersecurity and cyber defense, outlining, therefore, the structure they lay out. In the second section, my focus will be the country's institutional practices and arrangements. The third and fourth sections will be dedicated to a discussion on the literature

produced on militarization and the implications of this state of affairs, respectively. Perspectives on the near future and likely research avenues will be addressed in the conclusion.

The laws, the strategies and the regulations

The Constitution of the Federative Republic of Brazil (Brazil, 1988) only superficially deals with security-related themes, focusing on more practical provisions such as conditions for declaring state of defense and siege. It does establish the moral principles that guide the Republic in general and in its foreign relations, of which prevalence of human rights, political pluralism and peaceful solution of conflicts stand out. The National Defense Strategy, the National Defense Policy (Brazil, 2020d) - edited in a single document - and the National Cybersecurity Strategy (Brazil, 2020b) are, therefore, the most important documents providing strategic guidance in this domain.

It is important to note that the National Defense Strategy and the National Defense Policy, henceforth the NDS and the NDP, do mandate articulation with initiatives led by other government branches in order to consolidate what it calls "national power" (Brazil, 2020d, p. 11), a grandiose way of referring to capacity to achieve and maintain national goals as defined by the government. The NDS and the NDP's definition of security and defense is standard, and does not deviate from what is generally discussed in the literature. What may be an exception is the weight given to the country's economic development as fundamental for the "maintenance of national potentials", (2020d, p. 11).

Cybersecurity and cyber defense are mentioned expressly in the NDS and the NDP, albeit briefly. They are seen as essential for guaranteeing the integrity of information, management and communication systems of national interest, with particular emphasis on the latter. Thus, the paralysis of activities vital for the functioning of the country's institutions is a major preoccupation. Another particular concern is the accentuation of asymmetries in the defense technology area, which would, in the NDS and the NDP's assessment, influence regional and global balances of power and subvert traditional geopolitical logic. No other elaborations were made on this particular point.

The Brazilian society's involvement in national defense matters is seen as an objective. This seems like an innovative proposition. Further elaboration, however, puts such notions to rest, as "involvement" is defined as merely raising awareness on the importance of matters related to the country's defense and increasing participation in discussions related to the theme.

This involvement's endgame would be generating a "defense culture", a concept not actually defined by the NDS and the NDP. This is a topic raised again a few pages ahead, when it comes to talking about interaction - precisely the word employed - with Brazilian society and articulation with the government on a federal level. The spike in the number of civilian defense specialists is a

goal clearly outlined in the document, as well as engagement with academic communities overseas, though no measures to achieve these are laid out.

It is not unexpected, then, that the prioritization of the governmental, academic and industrial sectors is framed exclusively in regards to science, technology and innovation (CT&I), the so-called hard sciences. The mobilization and development of defense and information management is considered part of the national defense capability. This is the frame through which cyber is seen. Granted, it is noted that the cyber sector "transcends the division between development and defense and between the civil and military domains" (Brazil, 2020d, p. 59), meaning the country as a whole should be empowered to navigate these waters - an idea also mentioned in the National Defense White Book (Brazil, 2020c). The nuclear, cyber and space sectors are under the responsibility of the Navy, the Army and the Air Force, respectively.

Critical infrastructure is the focus when it comes to cyber, as stated in the NDS and the NDP. The understanding is repeated in the National Cybersecurity Strategy, henceforth E-ciber. In fact, information security, specifically, is its principal concern, because, as stated in the document, cyber threats arise in the same proportion and intensity with which cyberspace is used, putting the public administration and society at risk (Brazil, 2020b, p. 2).

In this sense, it is admitted that Brazilian governmental initiatives on cybersecurity are fragmented and inconsistent. In sum, there is no normative, strategic and operational alignment. Society's maturity level when it comes to cyber issues is varied, meaning perceptions on the importance of the theme are not balanced. Education is seen in E-ciber as a relevant axis to address this diagnosis - digital literacy is mentioned - and build a cybersecurity industry, but, much like with other points raised throughout the document, no detailed provisions are given to counter the problem, only general goals.

On a diplomatic note, the Ministry of Foreign Affairs (MRE or Itamaraty) is sidelined in favor of the Institutional Security Office (GSI). This is noteworthy because the Brazilian diplomatic corps is regarded as highly professional and competent in dealing with a wide array of foreign policy themes, though coordination on defense themes is not without challenges (Coutinho, 2018). By assigning the responsibility to manage international acts and cooperation in cyber issues to the GSI, E-ciber essentially puts the MRE in an auxiliary position.

Granted, the Ministry of Foreign Affairs does not have autonomy to design foreign policy, but to advise the President on such matters and implement the leader's guidelines. Still, one cannot help but reflect on this point raised by E-ciber and ponder on its meaning for the relations between the Institutional Security Office, the Ministry of Foreign Affairs and the Ministry of Defense, especially considering the trend since Michel Temer's term as president (2016-2018) to appoint

military officers to lead the GSI and the Ministry of Defense. Since Fernando Henrique Cardoso's presidency (1995-2003), it had been a custom to appoint civilians for these offices, thus building on the civilian oversight of security and defense issues. If this practice is no longer in place, and these organs are granted such importance in cybersecurity matters, what precisely is the impact this will have? At a minimum, it could be expected that civilians could conceivably be sidelined from positions with decision-making power in matters of cybersecurity.

The National Cybersecurity Strategy also mentions the need to create specific normative instruments for the Brazilian context, making a nod to the Digital Governance Policy, the Brazilian Strategy for Digital Transformation (Brazil, 2020a) and the Governance in Data Sharing (Brazil, 2019b). Though not mentioned by E-ciber, the Marco Civil da Internet (Brazil, 2014a), a bill focusing on regulating matters related to the medium, should also be considered an important legal evolution, particularly in regards to article 3 - which establishes the principles governing internet use in the country, especially the protection of privacy and personal data, in addition to the preservation and guarantee of net neutrality - and to article 7 - which considers access to the internet fundamental for exercising citizenship. The General Data Protection Law (Brazil, 2019c) is also important, as it regulates the processing of personal data in digital or non-digital media.

It is interesting that E-ciber makes the federal government's preference for a centralized cybersecurity management model clear. The preference is justified based on the report produced by the Parliamentary Inquiry Commission on Espionage, held in 2014, according to which "the distribution and handling of issues related to cybersecurity in the country has not contributed to the government having an overview of the subject, which hinders the execution of more effective actions in this domain", (Brazil, 2014).

This is the claim used to justify the creation of a single system that brings together state and non-state actors involved in cybersecurity, in order to align themselves strategically, doctrinally and operationally. It is stated that the responsibility of the federal government - particularly the GSI - is discussing options for institutionally strengthening Brazilian cybersecurity, given that authorities do not see the need to create new government agencies. Resizing the current GSI structure is understood to be enough. The report goes on to say that a law that regulates cybersecurity actions is needed. The instrument should specify attributions, point out mechanisms for a dialogue with society and grant to the Institutional Security Office the role of strategic coordinator in cybersecurity actions - with the participation of representatives of all national entities.

Finally, attention should be paid to the Brazilian Strategy for Artificial Intelligence's (Brazil, 2021b) launch in April 2021. It is reasonable to assume that the government has invested energy in the topic, given that the strategy is an extensive and interesting document whose central point is the

concept of axes: three horizontals, which cut across the six verticals. The horizontal axes are legislation, regulation and ethical use; artificial intelligence governance; international aspects. Verticals, in turn, are education; workforce and training; research, development, investment and entrepreneurship; application in the productive sectors; application in public power; and public safety.

It is a well-structured plan that already has implementation initiatives within the scope of the Ministry of Science, Technology and Innovation and Embrapii. There is also a forecast that the Ministry, in partnership with FAPESP and the Internet Steering Committee in Brazil, will create eight centers for applied research in artificial intelligence. There is also the IA² MCTI program, which aims to promote research and development projects focused on artificial intelligence solutions.

All in all, analyzing these documents tells us that i) the Brazilian government understands cybersecurity exclusively as a matter of protecting critical infrastructure; ii) the strategic arrangement they lay out concentrates responsibilities with the Institutional Security Office (GSI) and the Ministry of Defense; and iii) with the exception of the Strategy of Artificial Intelligence, a detailed document with recommendations already being put into practice, the trio of strategies mentioned in this section revolves around rhetorical provisions with no clear implementation plan.

Institutional meanders

The Brazilian government's dismissiveness of cyber threats not directly linked to critical infrastructure is not new. Diniz et al. (2014) had already shed light onto this disposition when most of the documents mentioned in the previous section had not been written yet. The authors argue that, although organized crime is one of the biggest threats to Brazilian cyberspace, resources are directed towards military solutions, more suited to extremely exceptional cases of armed conflict.

According to the authors, there was not much emphasis on police capabilities, as those of the Federal Police, to identify cyber crimes in general and respond to them. Little is discussed about the actors responsible for cyber threats, modus operandi and motivations. Brazil doesn't distinguish between different types of cyber threats. The absence, continue Diniz et al. (2014), of a unified government position on the matter – the article, let it be noted, is from 2014 and, therefore, before the National Cybersecurity Strategy was launched – and of reliable data on cyber crimes made the Brazilian approach on the issue unbalanced. This has not significantly changed since 2014.

In spite of these murky points, the authors believe that the Brazilian government has built a relatively dense cybersecurity and defense infrastructure. It focuses only on a few points of cyber threats, in particular those arising from foreign actors. This is why the authors attribute to the Army's

Cyber Defense Command (CDCiber) centrality in the country's stance on the matter. There is a mismatch between the evolution of threats and the Brazilian cybersecurity apparatus, aimed at responding to cyber wars and combating terrorism.

Thus, they say, it is possible to conclude that the Brazilian government has adopted a securitized approach to cyber threats, to the detriment of challenges that directly affect citizens, such as crimes committed in digital environments, for instance. "This not only has consequences for public policy and spending; the oversized military response also risks compromising citizens' fundamental rights owing to, among other things, pervasive surveillance and censorship", (Diniz, Muggah and Glenny, 2014, p. 4).

This securitized approach would go hand in hand with an effort to redefine the role of the Brazilian armed forces – a subject that will be dealt with in a later subsection. On the one hand, say the authors, the armed forces have strengthened border control and the fight against drug trafficking; on the other, they have expanded their reach and influence over the cyber domain.

Multiple public agencies are involved in managing cybersecurity in Brazil. As it turns out, it is a hierarchical scheme. The Institutional Security Office (GSI) takes precedence over most of the civilian agencies presented. The Information Security Department (DSIC) is subordinated to the GSI, responsible for ensuring the availability, integrity, confidentiality and authenticity of communications and information from the federal public administration in coordination with the Ministry of Civil Affairs. The Secretariat for Strategic Affairs (SAE) and the Chamber of Foreign Affairs and National Defense of the Council of Government (Creden) are also subordinated to the GSI. For the authors, DSIC, SAE and Creden are important to the country's debates on cybersecurity.

Also noteworthy are the Federal Police Department (DPF), which, under the supervision of the Ministry of Justice (MJ), has units dedicated to cybersecurity; the Brazilian Intelligence Agency (Abin), which is responsible for protecting public institutions, an activity carried out through the Research and Development Center for the Security of Communications (Cepesc); and the Ministry of Defense (MD), which oversees the armed forces and, of particular interest to the topic, the Joint Chiefs of Staff of the Armed Forces (EMCFA).

For the authors, the scheme demonstrates that the Brazilian government has been preparing the armed forces to lead the protection of Brazil in the cyber field, though the use of this space is mostly civilian. This is not a neutral choice, because as they point out, in Latin America – which, it should be remembered, has seen different authoritarian regimes throughout the 20th century – only Colombia has encouraged similar levels of involvement of the armed forces in the cyber issue.

The reason, they continue, has multiple layers. Mainly, according to the authors, the armed forces are making a bid to expand their protagonism in Brazilian affairs. When they wrote their

article, their evaluation was that this growing influence in civilian issues had yet to be subjected to much domestic scrutiny. The situation has somewhat changed since the election of Brazil's current president, Jair Bolsonaro, who has populated the government with active duty military officers (Lis, 2020; Marchesini, 2021).

Diniz et al.'s argument on the secrecy of the armed forces' activities in cyberspace still holds. As the authors put it, "there is no public record of information detailing when the army first started developing its operational capacities in cyberspace", (Diniz, Muggah and Glenny, 2014, p. 24). For the authors, it is problematic that the armed forces have been given control of the apparatus with supervisory prerogatives also over civilian affairs - the Cyber Defense Command (CDCiber), which coordinates with the Ministry of Defense and which, in turn, follows GSI guidelines' in this domain. It should be noted that CDCiber has a cyber war simulator and a malicious code analysis laboratory at its disposal.

This approach entails four main risks, according to Diniz et al.. First, Brazilian cyber architecture delegates clear competences to its main actors in a domain that is diffuse. Here, the authors refer specifically to the still difficult issue of attribution, which could lead the Army, for example, to become involved in situations in which it would not have clear legal and operational attributions. This point would also explain the importance of cooperation between the government agencies involved in Brazilian architecture.

Second, the aforementioned agencies' discourse is biased, say Diniz et al.. "Many military actors refer to 'ungoverned spaces' and the 'Wild West' when describing cyberspace. These terms are typically accompanied by assertions of the need to conquer and control this space", (Diniz, Muggah and Glenny, 2014, p. 26). This is problematic due to the misrepresentation of cyber incidents' real character, as well as their possible effects. For the authors, given the country's recent history of authoritarianism, this discourse is disturbing precisely because of the real chance that military personnel will soon have access to private civilian data. This calls into question issues of privacy and democratic control of the armed forces.

Thirdly, for the authors, these Brazilian initiatives have been implemented before the clear and unified design of a strategy – I recall the date on which the text was published. And fourth and last, scarce resources are diverted from priorities and spent inappropriately, as, they say, "although the primary threats to Brazil's cyberspace are arguably related to economic crime and should result in corresponding increases in resources allocated to police entities, the armed forces are receiving the bulk of support", (Diniz, Muggah and Glenny, 2014, p. 26).

And the diplomatic dimension in this scenario? For the trio of authors, Brazilian moves have been promising. They cite the holding of the NetMundial conference in São Paulo, in 2014, in

partnership with Germany and the Internet Corporation for Assigned Names and Numbers (ICANN), as well as the Brazilian proposal at the event to create a global Civil Framework for the internet, whose multi stakeholder governance should be deepened. Emphasis is also given to the country's regional performance through the Organization of American States (OAS), in particular the efforts to coordinate the fight against cybercrime and the adoption by Brazil of the OAS' guidelines contained in the Comprehensive Inter-American Strategy to Combat Threats to Cyber-Security, a document adopted by the organization's General Assembly in 2004. Within the scope of the Union of South American Nations (Unasur), Brazil fostered coordination efforts between the ministers of Defense, Justice and the Interior. It is still unclear whether this verve will be maintained in the Forum for Progress and Development in South America (Prosul).

It is necessary to update the information brought by Diniz et al. on the Brazilian diplomatic role in cyber. Indeed, even though Brazil has had a period of relevant diplomatic activity in the wake of the 2013 revelations about espionage undertaken by the National Security Agency (NSA) of the United States - some of these activities, by the way, in partnership with Germany - it doesn't seem that this momentum has been maintained over time. Yes, it is true that the topic raised at the time was privacy in digital media. But after 2014, there were few initiatives with themes related to this issue (Brazil, 2015, 2017a), so the actions of 2013 and 2014 (Brazil, 2013a, 2013b, 2014b), including those mentioned by the authors, were reactions to the revelations about the NSA's methods, and not necessarily the first steps of a coherent foreign policy strategy on an issue of growing relevance. Statements from multilateral meetings, such as 2019's Osaka Declaration from G20 Leaders (Brazil, 2019a), for example, or 2017's Xiamen Declaration (Brazil, 2017b), do mention building digital societies, but cybersecurity is not considered in these documents.

In terms of binding legal instruments, there are not many examples of agreements or memoranda that deal with security or even cyber cooperation. Of the 11,935 acts signed by Brazil since 1822 (Brazil, 2021a), around 13 are related to the topic, most incidentally in the context of mutual legal assistance - on cyber crimes, then - or cooperation in telecommunications, science and digital economy. The only instrument that specifically deals with cybersecurity was signed with Suriname in November 2020, and aims at establishing guidelines for the execution of a project to create a cyber incident response center in that country.

In consultations with the Institutional Security Office (GSI), the Ministry of Justice and Public Security, the Ministry of Foreign Affairs, the Ministry of Defense, the Army High Command and the Navy High Command, based on law number 12.527 (Brazil, 2011), the Freedom of Information Act (LAI, in Portuguese), I asked if there were inter-ministerial working groups, or equivalent groups, on cybersecurity or cyber defense in which each agency was involved. If they did exist, I also asked

what was the frequency of meetings, the hierarchical level of the participants and the scope of the group's work.

The GSI, for instance, only participates in the Information Security Management Committee, established on December 26, 2018. The Committee meets on an ordinary basis every six months, and may be called at any time by the coordinator, the GSI itself. The scope of the work is to advise the GSI on activities related to information security. In addition to the GSI, the Federal Comptroller General (CGU), the General Secretariat of the Presidency of the Republic, the Government Secretariat of the Presidency of the Republic, the Federal Attorney General (AGU) and the Central Bank (Bacen), the Ministries of the Civil House; of Justice and Public Security; of Defense; of Foreign Affairs; of the Economy; of Infrastructure; of Agriculture, Livestock and Supply; of Education; of Citizenship; of Health; of Mines and Energy; of Science, Technology, Innovations and Communications; of the Environment; of Tourism; of Regional Development; and of Women, Family and Human Rights are also involved. According to the answers provided by the Freedom of Information Act consultation, they are represented in this Committee not by career public servants, but by hired ministerial employees, who can be fired at their supervisor's accord.

There are no inter-ministerial groups on cyber defense. In addition to the Information Security Management Committee, the Ministry of Defense also participates in the Internet Management Committee in Brazil (CGI.br). There is, however, an Interforce Working Group (GTI) for the cyber sector, whose meetings take place at the Cyber Defense Command (ComDCiber). The list of participants is not disclosed for security reasons, so the hierarchical level of the participants is not known. According to the Navy's High Command, officers from different ranks participate. No civilians are allowed in this group.

It can only be concluded, then, that the most organized cybersecurity structures are military ones. Civilian coordination instruments are lax, having a narrow subject scope and an uncertain work agenda. As far as interaction with society goes, this occurs only on a sporadic basis and is not a permanent fixture of Brazilian cybersecurity endeavors. Even if discourse in the country's strategies makes a possible nod to an ample coalition of cybersecurity actors, this does not translate into practice. There is, therefore, a significant bridge between what official documents say and what actually happens within governmental structures.

What about militarization?

The truth is that the participation of the armed forces in Brazilian political life precedes the very foundation of the country as an independent political entity, say Mathias and Guzzi (2010), in reference to the confrontation between D. Pedro I and commander Jorge de Avilez's troops on the

deposition of the Count of Arcos and the appointment of judge Álvares Diniz to the position of Minister of the Kingdom. The construction of the national state, they argue, took place in parallel with the rise of military autonomy, and "to date, the government has not fully decided on the complete subordination of the military apparatus to civilians, which mitigates democracy in the country", (Mathias and Guzzi, 2010, p. 41).

Complementary Law Number 69, published on July 30, 1991, partially solved the definition of the armed forces' role in the new democratic Brazil, they argue. It established that the use of armed forces for actions to defend the homeland, constitutional powers, the law and of the order, is under the authority of the President of the Republic. But, in light of the example of re-established democracies, Mathias and Guzzi continue, removing the armed forces from public security actions is essential to ensure their subordination to civilian authorities. This is not what the Brazilian government has been doing – see the spike in Law and Order Guarantee Operations (GLO) (Cláudio Silveira, 2014). The result is the trivialization of the use of the armed forces in the country, employed as guarantors of internal security.

Such trivialization does not necessarily mean an increased risk of an overt coup d'état. It could be argued that contemporary militaries in Latin America have self-imposed limits and revised calculations about the risks and benefits of authoritarianism, concluding that the professional and political costs of reintervention are higher than in the past and political and economic forces in favor of democratic sustenance are much more solid than before (Pion-Berlin, 2001). In Brazil, given how recent redemocratization is, there are still stages of maturation to be gone through both in the stability of political institutions and in civil-military relations before cooperation, productivity and co-responsibility become second nature (Migon, 2013). According to the author, part of State and civil society structures are still influenced by last century's ideological shadows. For some in the armed forces, for instance, military intervention in politics is still seen as legitimate; therefore, the central question is how civilians and military perceive each other.

Still, not only in public security are the armed forces called to action by civilian leaders, but also in politics. For Diamint (2015), the armed forces have become a tool for neutralizing opposition to public policies. As an example of this type of instrumentalization of military contingents, the author mentions Bolivia, Ecuador and Nicaragua. The endgame for the armed forces has been the possibility to secure their corporate interests and to reap material benefits. In the end, it is about subjective civilian control, whereby a specific group of civilians equips the armed forces to achieve their own objectives. The ideal model, says the author, would be objective civilian control, which would only be possible in countries where military contingents systematically and principally abstained from involvement in political affairs.

Granted, fusionism, or the idea that the line between the military and the political has become so blurred that the distinction has lost its meaning, is an old debate in civil-military relations (Feaver, 1999). Interestingly, Burk (2002) hints at this stance by laying out his skepticism of a divide between the civilian political sphere and the military one. He argues such distinction between means of war, policy decisions by political elites and operational decisions by military elites is not clear in the weapons of mass destruction era, as those spheres are interpenetrating.

Even if Burk raises important points on the "pro-civilian political oversight" skewness of the literature on this topic, Feaver's argument that monitoring mechanisms enhance civilian control by bringing military conduct to the attention of responsible civilians is compelling. Yes, Burk has a point when arguing that studies focused on liberal or civic republican models of democracy are of limited usefulness because they assume that the problems of civil-military relations are exclusive to the sovereign state. But, in the Brazilian case, wouldn't the greater willingness of civilian leaders to punish non compliant behavior render monitoring mechanisms more effective in securing civilian tutelage, so to speak? Could that affect military effectiveness (Nielsen, 2005)?

That is a possibility, according to Bruneau and Matei (2008). Increased democratic control may improve effectiveness in the military, they argue. The reasoning is straightforward: civilians controlling the army makes it easier for the armed forces to maintain its focus. Naturally, too much oversight might hamper the army's activities. In general, though, top-level direction and general oversight guidance leads to improved effectiveness.

Perhaps thinking about the issue through a rational choice understanding (Hunter, 2001) is useful for analyzing motivations and drawbacks. How is reason employed to satisfy the Brazilian armed forces' and politician's interests? How does it explain the military's influence? Can we understand the pragmatic adaptation they made to the new order? Does it account for variations in armed forces influence in different issues? How does it explain different strategies presidents and legislators take toward the military?

This is why Enloe's (2007) reflections are so important. She states that to become militarized is to adopt militaristic values and priorities, to see military solutions as particularly effective, to see the world as a dangerous place best approached with militaristic attitudes. It is a way of understanding and interpreting one's political and social context. Interestingly, most militarized people are civilians, the author informs. Militarization can look less like conventional aggressiveness and more like deferential passivity. The general argument is that the effect of some government decisions is not only to militarize one country's national security, but also to militarize global politics.

The more militarized the understanding of what national security is, the more likely it will be that the conversation about national security and international security will be a masculinized

affair, because the area is seen as one in which only "rational" people can be taken seriously, which in turn has made a certain kind of masculinity the passport into national security discussions. This argument is somewhat related to what Gilbert (2012) stresses on claiming climate change as a military issue or Passos and Acácio (2021) comment on using the armed forces as crisis managers for health crises, such as the COVID-19 pandemic. This is a useful framework to think about the Brazilian case, especially considering the expansion of citizenship rights through the militarization of social interactions between the government and marginalized populations (Fleury, 2012).

Militarization is changing in the digital age, and this is important for International Relations (Jackson et al., 2020). In this sense, militarism is a disposition toward and social purpose to use military force. Militarization, on the other hand, is an embedded sociological process underpinned by communication; it prepares for, normalizes and legitimizes war.

The authors say that studying militarization in the digital era - or, better yet, Militarization 2.0 - means moving beyond the military itself and focusing on what the authors call war's insidious presence in civilian institutions. Thinking about how the ubiquity of technology encourages uses of violence and fosters the assembly of virtual communities which contribute to the creation of political spaces out of the state's reach leads to the conclusion that ICTs drive and highlight the changes security, militarization and war are currently undergoing.

It is reasonable to assume, then, that the identification of the mechanisms through which social media and crowdfunding assist transformations in the way violence is organized and facilitated is important. Militarizing processes have always had a direct link to civilians' daily, mundane lives. Thus, war-waging was normalized to people far away from battlefields. Imagination is important in fueling an insinuating militarizing process. Therefore, understanding the appeal of militarization begs the analysis of more than just strategic actors and doctrines. A growing cast of militarizers strive to convince legislators and regular civilians that the world is dangerous, which works as a justification for militarization.

Which brings us back to Brazil. Understanding civil-military relations in the country through the "Military Party" lenses proposed by Mathias and Penido (2021) seems productive. In this way, since their professionalization after the Second World War, the armed forces can be conceptualized as an organization similar to political parties because it organizes and shapes demands brought forth by their constituents, military officers, and envisions gaining political clout to bring these demands into fruition. The Military Party is a privileged organization, though, because it is not subject to the rules imposed onto civilian political parties; has a committed cohort of supporters made of the most disciplined public employees in the country; and possesses its own organized financing mechanisms.

This perspective helps understand the directions given in E-ciber, then, particularly the prominence given to the GSI and the Ministry of Defense. If the Military Party has the ultimate goal of consolidating power in all three government branches, controlling their own press, business and international affairs ecosystem is a logical step. As Mathias and Penido argue, it is concerning, then, if the military way - based on obedience and hierarchy, not on dialogue and common understanding - permeates life in general, because it threatens the maintenance of a healthy, plural democratic regime.

It should be stressed that the military is a necessary organization, and vital one. Enlarging their role beyond constitutional provisions (Brazil, 1988), though, is imprudent in a democracy. The armed forces' training is particularly suited for armed conflict situations, and this specific set of skills does not necessarily translate into the managerial verve necessary to rule government institutions. Furthermore, as I hinted at this work's introduction, the cyber issue is not primarily a military one. Even if one considers the importance of military technology innovation in this context, a vital issue with manifold ramifications, the principal use of cyberspace is civilian, not to mention that cyber technology innovation is brought forth mainly by them. It is counterproductive, then, to imagine cybersecurity strategies can be successfully implemented if they are singularly a military responsibility. This is a common issue to be dealt with by the government and society as a whole.

Looking to the future

Taking the government as a unit of analysis, it is common and understandable that different ministries and departments take responsibility for some aspect of national cybersecurity. Absent a coherent strategy, it becomes difficult to establish cohesive actions. The challenge is to improve coordination among governmental actors, through the creation of a comprehensive work group – even if this is subdivided into thematic axes – or through the improvement of interdepartmental processes without creating new government agencies. Of utmost importance is the constancy of coordination, which must be continuous. Sparse encounters are not enough to reach an optimal level of interaction. Agility is fundamental, as it is a neuralgic attribute of the cyber issue. There is some precedent, even though the scale is different from what is proposed here. Just remember the cases of cooperation during major events, such as the 2014 FIFA World Cup and the 2016 Olympic Games, not to mention the recent example of Operation Southern Border - Ágata 21, which brought together the 5th Army Division and federal and state security agencies.

In the international arena, "the emphasis must be on relationships with all the relevant actors within specific systems (in particular, but not limited to the field of 'internet governance')", (Klimburg and NATO Cooperative Cyber Defence Centre of Excellence, 2012, p. 31). This requires

the government to choose a focal point, which may not be part of the government structure. This actor must have the freedom to be flexible enough to engage with stakeholders around the world. Foreign policy responses to the ambiguity of relationships in cyberspace must also be developed. It is not possible to do without the massive and focused involvement of the Ministry of Foreign Affairs in the matter. It does not seem efficient, moreover, to delegate its functions to other government bodies – as E-ciber suggests that it be done for the GSI, which would have a mere auxiliary in the Ministry of Foreign Affairs. Brazilian diplomacy must be intimately involved in all the themes and developments of the cyber issue. Naturally, the way in which this happens is linked to the instructions that the Ministry of Foreign Affairs itself receives from the Presidency of the Republic regarding Foreign Policy guidelines. It is necessary, however, to create awareness of the fundamental role that diplomacy plays in this domain.

At the national level, building relationships between government, security service providers and technology-critical infrastructure companies is important. The whole of nation, or whole of society, approach encourages a variety of non-state actors – private businesses, think tanks and civil society – to cooperate with the government on cybersecurity issues. Even though there are variations in the style of cooperation to be adopted, some level of interaction should be encouraged. At the moment, there are no initiatives in this direction. Despite the incompleteness of the diagnosis of cyber threats that is currently faced, E-ciber advocates the importance of involving society as a whole, which was recognized by the interviewed authorities, in fact. It is foolhardy to neglect this point. Brazil has public servants of undeniable competence; they alone, however, cannot handle the cyber issue. Nor does the Brazilian government have the technical capacity to keep abreast of constant technological innovations and implement them, when necessary. The expertise and input of the private sector are fundamental.

In the end, there needs to be a broad understanding in society as a whole about what cyberspace is and what the nature of cybersecurity threats is to avoid failure. Klimburg and NATO (2012, p. 141) mention six problems to be avoided: leaving a public policy vacuum with a clear strategic vision; allow the sharing of information within government in particular, and with stakeholders in general to be cluttered; writing obsolete legislation that does not respond to the challenges posed by cyberspace; strengthen cooperation between government agencies and between government and society; communicate inefficiently; tolerate cyber illiteracy of public agents, decision makers, members of the judiciary, politicians in general, academia, private initiative and civil society; neglect the international dimension. It is necessary to implement public policies aimed at increasing digital literacy in Brazilian civil society. Coordination with the academy is also absolutely necessary. Here, it is worth mentioning Elisabeth Braw's considerations.

On deterrence by denial, Braw (2021), echoing Wigell (2019), considers that civil society has a crucial role in defending against present and future gray zone aggressions precisely because this type of action is directed to civil society. "When trying to improve defense and deterrence while leaving society out, governments practically guarantee they will be overstretched while leaving civil society (…) passive observers of their own fate" (Braw, 2021, p. 4). That is, even if the government wanted to become ubiquitous in terms of deterrence in the cyber field, the costs would be too high – and the effort inefficient. However, if the purpose of defense is also to discourage hostile actions, the whole of government approach signals to potential adversaries that an essential part of society will not be involved in these efforts and is considered a liability by its own government. It's almost an invitation to attack. It should be clarified that, by society, Braw means not only citizens, but also private initiative.

The author suggests, for citizen engagement, awareness campaigns, societal stress testing exercises, resilience training courses, and the conscription of high school graduates to serve in all government sectors involved in crisis management. For the involvement of private businesses, Braw's main suggestions are briefings between government and industry leaders, engagement of the artistic class in the production of cultural content - series, films, etc - that address the theme, joint exercises between the armed forces and the private sector on gray zone aggressions and courses on national security.

Conclusions

Brazil has strategies and laws that address the cyber issue, but it does not have mechanisms for implementing the strategic guidelines it already has, such as inter-ministerial working groups on cyber security and defense. The only instance is the Information Security Management Committee, whose meetings do not happen periodically. With regards to Brazilian diplomacy, there are instruments that approach the subject tangentially, especially in the context of mutual legal assistance.

Recognition of the need for involvement of other sectors of society, even if it exists, does not translate into concrete actions. This is the largest weakness in the Brazilian system, as it leads to cybersecurity actions being largely a military issue. I have argued in this work that this is an imprudent approach, especially considering Brazil's political instability history.

The concentration of attributions in the GSI and in the Ministry of Defense is reckless, as the militarization of cyber threat management is very much a reality in this scenario. Furthermore, the government's diagnosis of the cyber issue is partial and, let us insist, does not recognize hybrid threats or gray zone aggressions, only protecting information and critical infrastructure. The country

is vulnerable. Finally, it must be said that the Brazilian government should change not necessarily its organizational structure, but the way it handles the issue.

The expectation when this research project began was that the Brazilian strategy would be completely inefficient, which is not the case. It's incomplete, yes; it doesn't have solid implementation mechanisms, either. But there is encouraging awareness of the importance of the issue. This is positive. If we count on the activism that the Brazilian government has shown on artificial intelligence, the scenario is not bleak, but it inspires care. As it stands, the degree of militarization already underway in Brazilian cybersecurity has yet to be an object of ample debate by Brazilian society, given how impactful this arrangement may be for matters of privacy, in particular, and human rights, in general.

Predicting diagnoses and solutions on the pages on which this work was written is relatively simple compared to the herculean task that must be undertaken for Brazil to adapt to the challenges that are already present. Indeed, changing processes and methods of formulating public policies, even if in a sectoral and delimited way, as well as including segments of society that normally do not have an active role in government activities in any thematic field, would be, in an absolutely shallow comparison, as move an ocean liner "by hand only". Much more so when the ocean liner is a country with extensive territory, huge population and a public machine of pharaonic proportions.

This field of studies is booming and still needs a lot of research. There was no ambition here to fill gaps, but it is hoped that future readers will recognize the need to study cybersecurity and cyber defense. Researchers have barely covered the surface of the cyber "ocean" and its consequences in various fields of human life. There is still a lot of work to be done. If there is a more exciting study prospect, this author has yet to hear of it.

References

Bioni, B. R. (2021) Proteção de dados pessoais: A função e os limites do consentimento. 3rd edn. Editora Forense.

Bradshaw, S., Bailey, H. and Howard, P. N. (2021) Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Working Paper. Oxford: University of Oxford, p. 26.

Braw, E. (2021) The Defender's Dilemma: Defining, Identifying, and Deterring Gray-Zone Aggression. Washington, D.C: American Enterprise Institute, p. 11.

Brazil (1988) Constituição da República Federativa do Brasil. 1st edn. Brasília: Senado Federal, Coordenação de Edições Técnicas. Available at:

https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf (Accessed: 19 August 2021).

Brazil (2011) Lei no 12.527: Lei de Acesso à Informação. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (Accessed: 23 August 2021).

Brazil (2013a) O Direito à Privacidade na Era Digital, Ministério das Relações Exteriores. Available at: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/o-direito-a-priv acidade-na-era-digital (Accessed: 28 August 2021).

Brazil (2013b) ONU aprova resolução sobre o Direito à Privacidade na Era Digital, Ministério das Relações Exteriores. Available at: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/resolucao-sobre -o-direito-a-privacidade-na-era-digital (Accessed: 28 August 2021).

Brazil (2014) CPI da Espionagem: Relatório final. Brasília: Congresso Nacional, p. 301. Available at: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco.

Brazil (2014a) Lei no 12.965. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Accessed: 23 August 2021).

Brazil (2014b) Relatório da Alta Comissária para Direitos Humanos da ONU sobre 'O Direito à Privacidade na Era Digital', Ministério das Relações Exteriores. Available at: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/relatorio-da-alta -comissaria-para-direitos-humanos-da-onu-sobre-o-direito-a-privacidade-na-era-digital (Accessed: 28 August 2021).

Brazil (2015) Criação da Relatoria Especial sobre 'O Direito à Privacidade na Era Digital', Ministério das Relações Exteriores. Available at: http://antigo.itamaraty.gov.br/pt-BR/notas-a-imprensa/8460-criacao-da-relatoria-especial-sobr e-o-direito-a-privacidade-na-era-digital (Accessed: 28 August 2021).

Brazil (2017a) Direito à privacidade na Era Digital, Ministério das Relações Exteriores. Available at: http://antigo.itamaraty.gov.br/pt-BR/notas-a-imprensa/15971-direito-a-privacidade-na-era-digi tal (Accessed: 28 August 2021).

Brazil (2017b) IX Cúpula do BRICS: Declaração de Xiamen, Ministério das Relações Exteriores. Available at: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/nona-cupula-do -brics-declaracao-de-xiamen-xiamen-china-4-de-setembro-de-2017 (Accessed: 28 August 2021).

Brazil (2019a) Declaração de Osaka dos Líderes do G20, Ministério das Relações Exteriores. Available at: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/declaraca o-de-osaka-dos-lideres-do-g20 (Accessed: 28 August 2021).

Brazil (2019b) Decreto no 10.046. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm (Accessed: 23 August 2021).

Brazil (2019c) Lei no 13.853. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 (Accessed: 23 August 2021).

Brazil (2020a) Decreto no 10.332. Available at: https://www.in.gov.br/en/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358 (Accessed: 23 August 2021).

Brazil (2020b) Estratégia Nacional de Segurança Cibernética. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm (Accessed: 19 August 2021).

Brazil (2020c) Livro Branco da Defesa Nacional. Brasília: Ministério da Defesa, p. 98. Available at: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf (Accessed: 20 August 2021).

Brazil (2020d) Política Nacional de Defesa e Estratégia Nacional de Defesa. Brasília: Congresso Nacional, p. 41. Available at: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf (Accessed: 18 August 2021).

Brazil (2021a) Acervo de atos internacionais do Brasil, Ministério das Relações Exteriores. Available at: https://concordia.itamaraty.gov.br/ (Accessed: 28 August 2021).

Brazil (2021b) Estratégia Brasileira de Inteligência Artificial (EBIA). Brasília: Ministério da Ciência, Tecnologia e Inovações, p. 52. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf (Accessed: 23 August 2021).

Bressan, S. and Sulg, M.-L. (2020) 'Welcome to the grey zone: Future war and peace', New Perspectives, 28(3), pp. 379–397. doi: 10/gjsgzn.

Bruneau, T. C. and Matei, F. C. (CRIS) (2008) 'Towards a New Conceptualization of Democratization and Civil-Military Relations', Democratization, 15(5), pp. 909–929. doi: 10/fc727s.

Burk, J. (2002) 'Theories of Democratic Civil-Military Relations', Armed Forces & Society, 29(1), pp. 7–29. doi: 10/c6q3xt.

Cláudio Silveira (2014) 'A garantia da lei e da ordem como justificativa de intervenção militar na sociedade'. Available at: http://www.ihu.unisinos.br/entrevistas/535301-a-garantia-da-lei-e-da-ordem-como-justificativa-de-intervencao-militar-na-sociedade-entrevista-especial-com-claudio-silveira- (Accessed: 28 August 2021).

Coutinho, I. C. (2018) 'Articulação entre política externa e política de defesa do Brasil: obstáculos e avanços', Revista de Discentes de Ciência Política da UFSCAR, 6(3), pp. 192–213.

Diamint, R. (2015) 'A New Militarism in Latin America', Journal of Democracy, 26(4), pp. 155–168. doi: 10/gmkhx9.

Diniz, G., Muggah, R. and Glenny, M. (2014) Deconstructing cyber security in Brazil: threats and responses. Strategic Paper 11. Rio de Janeiro: Igarapé Institute, p. 35. Available at: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (Accessed: 18 August 2021).

Eck, K. and Hatz, S. (2020) 'State surveillance and the COVID-19 crisis', Journal of Human Rights, 19(5), pp. 603–612. doi: 10/gjfm6z.

Enloe, C. H. (2007) Globalization and militarism: feminists make the link. Lanham: Rowman & Littlefield (Globalization).

Feaver, P. D. (1999) 'CIVIL-MILITARY RELATIONS', Annual Review of Political Science, 2(1), pp. 211–241. doi: 10/bj8fz7.

Fleury, S. (2012) 'Militarização do social como estratégia de integração: o caso da UPP do Santa Marta', Sociologias, 14(30), pp. 194–222.

Gilbert, E. (2012) 'The Militarization of Climate Change', ACME: An International E-Journal for Critical Geographies, 11(1), pp. 1–14.

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', International Studies Quarterly, 53(4), pp. 1155–1175. doi: 10/cwhqrz.

Hanson, F. et al. (2019) Hacking democracies: Cataloguing cyber-enabled attacks on elections. Policy Brief 16/2019. Canberra: Australian Strategic Policy Institute, p. 36.

Hunter, W. (2001) 'Reason, Culture, or Structure? Assessing Civil-Military Dynamics in Brazil', in Pion-Berlin, D. (ed.) Civil-military relations in Latin America: new analytical perspectives. Chapel Hill, NC: University of North Carolina Press.

Jackson, S. T. et al. (2020) 'Forum: Militarization 2.0: Introduction', International Studies Review, pp. 1–26. doi: 10/gkspnz.

Klimburg, A. and NATO Cooperative Cyber Defence Centre of Excellence (2012) National cyber security framework manual. Talinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence. Available at: http://ccdcoe.org/369.html (Accessed: 24 August 2021).

Lamer, W. (2017) 'From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe', Global Campus Human Rights Journal, 1(2), pp. 393–413. doi: https://doi.org/20.500.11825/422.

Lis, L. (2020) 'Governo Bolsonaro mais que dobra número de militares em cargos civis, aponta TCU', G1, 17 July. Available at: https://g1.globo.com/politica/noticia/2020/07/17/governo-bolsonaro-tem-6157-militares-em-cargos-civis-diz-tcu.ghtml (Accessed: 28 August 2021).

Lopez, D. (2017) 'Securitisation and its impact on human rights in Latin America', Global Campus Human Rights Journal, 1(2), pp. 463–477. doi: https://doi.org/20.500.11825/417.

Marchesini, L. (2021) 'Em 70 órgãos, militares ocupam 18,3% dos 14,6 mil cargos comissionados no governo Bolsonaro', Metrópoles, 1 August. Available at: https://www.metropoles.com/brasil/em-70-orgaos-militares-ocupam-183-dos-146-mil-cargos-comissionados-no-governo-bolsonaro (Accessed: 28 August 2021).

Mathias, S. K. and Guzzi, A. C. (2010) 'Autonomia na lei: as forças armadas nas constituições nacionais', Revista Brasileira de Ciências Sociais, 25(73). doi: 10/cdmfh8.

Mathias, S. K. and Penido, A. (2021) 'O projeto de poder do Partido Militar e os riscos da "militarização da vida": Entrevista especial com Ana Penido e Suzeley Kalil'. Available at: http://www.ihu.unisinos.br/611312-o-projeto-de-poder-do-partido-militar-e-os-riscos-da-militarizacao-da-vida-entrevista-especial-com-ana-penido-e-suzeley-kalil (Accessed: 26 August 2021).

Mendes, L. S. (2008) Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. Masters. Universidade de Brasília. Available at: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf (Accessed: 18 August 2021).

Mendes, L. S. and Fonseca, G. C. S. da (2020) 'Proteção de dados para além do consentimento: tendências contemporâneas de materialização', REI - Revista Estudos Institucionais, 6(2), pp. 507–533. doi: 10/gmhrj9.

Migon, E. X. F. G. (2013) 'Segurança, defesa e as relações civis-militares: (re)leituras em apoio à construção de uma nova agenda brasileira', Revista de Ciência Militares, 1(1), pp. 101–122.

Nielsen, S. C. (2005) 'Civil-Military Relations Theory and Military Effectiveness', Public Administration and Management, 10(2), pp. 61–84.

Nuñez-Mietz, F. G. (2019) 'Resisting human rights through securitization: Russia and Hungary against LGBT rights', Journal of Human Rights, 18(5), pp. 543–563. doi: 10/gmhrzr.

Office of the United Nations High Commissioner for Human Rights (2008) Human Rights, Terrorism and Counter-terrorism. Fact Sheet 32. Geneva: United Nations, p. 76. Available at: https://ohchr.org/Documents/Publications/Factsheet32EN.pdf (Accessed: 18 August 2021).

Passos, A. M. and Acácio, I. (2021) 'The militarization of responses to COVID-19 in Democratic Latin America', Revista de Administração Pública, 55(1), pp. 261–272. doi: 10/gktf9g.

Pauwels, E. (2019) The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI. New York: United Nations University Centre for Policy Research, p. 83.

Pion-Berlin, D. (2001) 'Introduction', in Pion-Berlin, D. (ed.) Civil-military relations in Latin America: new analytical perspectives. Chapel Hill, NC: University of North Carolina Press.

Rid, T. (2012) 'Cyber War Will Not Take Place', Journal of Strategic Studies, 35(1), pp. 5–32. doi: 10/b4fkhh.

Strachan, H. (2014) 'Strategy in the Twenty-First Century', in Strachan, H. and Scheipers, S. (eds) The changing character of war. Repr. Oxford: Oxford University Press, pp. 503–523.

Valeriano, B. and Maness, R. C. (2014) 'The dynamics of cyber conflict between rival antagonists, 2001–11', Journal of Peace Research, 51(3), pp. 347–360. doi: 10/gkzbkh.

Valeriano, B. and Maness, R. C. (2016) 'The Impact of Cyber Conflict on International Interactions', Armed Forces & Society, 42(2), pp. 301–323. doi: 10/f8ctf4.

Valeriano, B. and Maness, R. C. (2018) 'How We Stopped Worrying about Cyber Doom and Started Collecting Data', Politics and Governance, 6(2), pp. 49–60. doi: 10/gf6j96.

Wigell, M. (2019) 'Democratic Deterrence: How to Dissuade Hybrid Interference', The Washington Quarterly, 44(1), pp. 49–67. doi: 10/gmdgqv.