



Revista Brasileira de Política Internacional

ISSN: 0034-7329

ISSN: 1983-3121

Centro de Estudos Globais da Universidade de Brasília

Devanny, Joe; Goldoni, Luiz Rogério Franco; Medeiros, Breno Pauli
The rise of cyber power in Brazil

Revista Brasileira de Política Internacional, vol. 65, no. 1, e013, 2022
Centro de Estudos Globais da Universidade de Brasília

DOI: <https://doi.org/10.1590/0034-7329202200113>

Available in: <https://www.redalyc.org/articulo.oa?id=35870295010>

- ▶ [How to cite](#)
- ▶ [Complete issue](#)
- ▶ [More information about this article](#)
- ▶ [Journal's webpage in redalyc.org](#)




Scientific Information System Redalyc

Network of Scientific Journals from Latin America and the Caribbean, Spain and Portugal

Project academic non-profit, developed under the open access initiative


Joe Devanny¹

¹King's College London - War Studies
London, United Kingdom
(joseph.devanny@kcl.ac.uk).

 ORCID ID:
orcid.org/0000-0001-6031-2397


Luiz Rogério Franco Goldoni²

²Escola de Comando e Estado-Maior do
Exército - Instituto Meira Mattos, Rio de
Janeiro, Brazil
(luizrfgoldoni@gmail.com).

 ORCID ID:
orcid.org/0000-0001-5257-9470

Breno Pauli Medeiros³

³Escola de Comando e Estado-Maior do
Exército - Instituto Meira Mattos, Rio de
Janeiro, Brazil
(breno.pauli@gmail.com).

 ORCID ID:
orcid.org/0000-0002-9839-5252

Copyright:

• This is an open-access article distributed under the terms of a Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided that the original author and source are credited.

• Este é um artigo publicado em acesso aberto e distribuído sob os termos da Licença de Atribuição Creative Commons, que permite uso irrestrito, distribuição e reprodução em qualquer meio, desde que o autor e a fonte originais sejam creditados.



The rise of cyber power in Brazil

DOI: <http://dx.doi.org/10.1590/0034-7329202200113>

Rev. Bras. Polít. Int., 65(1): e013, 2022

Abstract

The advent of cyber power in inter-state competition is frequently addressed in academic literature skewed towards global powers, commonly overlooking regional powers. The article addresses this gap by investigating how cyber power is conceived and implemented by Brazilian Governmental actors. It draws on the analysis of primary data concerning Brazil's policy documentation and institutional framework. The article begins with a broader view of cyber power and investigates its relationship with cyber defense and security, illuminating the current Brazilian understanding of cyber power as an operational tool within the military sphere.

Keywords: Cyber Power; Cyber Strategy; Cyber Defense; Cyber Security; Brazil.

Received: February 07, 2022

Accepted: July 01, 2022

Introduction

Brazil is the leading economic and military power in South America, a region characterized in the academic literature as “a unipolar zone of peace without major aggressive rivalries between Brazil and the secondary powers” (Flemes and Wehner 2012). For over 20 years, Brazil has enjoyed a relatively benign geopolitical position, amplified by a diplomatic strategy that emphasized Brazil's role as a cooperative member of the international system. The advent of cyber power – “the available human and material resources within a strategic environment that can be utilized to generate effects in and through cyberspace” (Bebber 2017, 427) – creates both opportunities and challenges for Brazil's ambitions of rising in international prominence.

Brazil's relatively benign position in traditional geopolitical relations is challenged by the operationalization of cyberspace, which subverts tradition perception of borders, territory, and sovereignty (Medeiros and Goldoni 2020). Edward Snowden's (2013) revelations highlighted the national security value of

improved communications and data security (Harris 2015) as well as Brazil's cyber vulnerabilities (Greenwald and MacAskill 2013; Medeiros et al. 2020). The number of reported cyber incidents in Brazil has increased sharply since 2010, earning it the unwanted description as an "epicenter of a global cybercrime wave" (Muggah and Thompson 2015). It was estimated that, in 2018, there were 70 million victims of cybercrime, producing economic losses of US\$20bn (BNAmericas 2019), rendering Brazil the country second-worst affected by cybercrime (BNAmericas 2020). More recently, the country's infrastructure has also been targeted with cyber-attacks. In December 2021, several systems of the health ministry were taken down, among them the Conecte-SUS app that provides Brazilians with vaccination certificates ("Brazil health ministry website hit by hackers, vaccination data targeted." 2021).

Brazilian diplomacy aims to create a constructive national role within and beyond South America. Brazil's international position was increasingly active and prominent under the presidencies of Luiz Inácio Lula da Silva and Dilma Rousseff. Brazilian foreign policy up to and including this period can be summarized as a "traditional preference for non-confrontational politics, non-coercive strategies, and ideational resources of leadership – such as consensus building and persuasion" (Rezende et al. 2018, 385). This strategic narrative was relatively consistent until the Jair Bolsonaro presidency. Bolsonaro's approximation to the Trump administration (Samuels 2019) marked a break with the strategy that had largely benefited Brazil economically from rising Chinese demand (Fausto and Fausto 2014; Stuenkel 2020).

Despite this recent fluctuation in Brazil's foreign policy, the country has historically pursued an assiduously broad diplomacy, cultivating an international role as a constructive and cooperative partner to a wide range of states. Even so, Brazil is arguably yet to demonstrate willingness to address the "graduation dilemma" (Harig and Kenkel 2017; Milani, Pinheiro and Lima 2017), embracing the responsibilities and costs of distributional and multilateral leadership implicit in the "cooperative hegemony" of regional leadership (Flemes and Wehner 2012).

Focusing on Brazil's cyber power, this article draws from academic literature on cyber strategy in which regions such as South America have been under-represented, and which is skewed towards consideration of the United States and its most prominent cyber adversaries (Devanny and Stevens 2021). The extant literature often ignores emerging countries where digital technologies play a large role, such as Brazil.

The article aims to fill this gap in the literature by addressing the following research question: How is cyber power conceived and implemented by Brazilian governmental actors? This question implies the integration of cyber power with existing interpretations of Brazil's regional and global roles, requiring an appraisal of Brazil's defense strategy and geopolitical role conceptions, as well as the shortcomings of Brazil's national security apparatus (Burgess 2013; Lima, Silva and Rudzit 2021). Such a strategic appraisal requires structured consideration of the decisions facing Brazil in developing its cyber power domestically and through foreign partnerships. Any analysis of the strategic utility of cyber capabilities should be holistic, reflective, and careful not to exaggerate benefits or inflate costs. It should also recognize that the variety of models for developing cyber

power emerged from distinct national contexts: what was considered desirable (and feasible) for the U.S., for example, would not necessarily satisfy Brazilian requirements.

This reflective use of the concept of “cyber power” illuminates interdependencies between cyber policies and broader national strategy. Besides critically engaging with the literature on cyber power as it applies to Brazilian defense and security strategy, the article also supports its arguments using primary data. The article adopts a qualitative approach both in methodology and in its subject. Firstly, it establishes a systematic analysis of policy documents to highlight the role of cyber power in the Brazilian institutional framework. This analysis is then compared with available information regarding budgetary planning and expenditure to assess Brazil’s strategic perceptions and priorities regarding military cyber capabilities. Both the institutional framework and budgetary analysis are contextualized by guided interviews with two top Brazilian Army officers involved in national cyber defense: Colonel Edson Ribeiro dos Santos Junior and Colonel João Marinonio Enke Carneiro. Both served as Senior Governance Advisors to General Guido Amin Naves, the Commander of the Brazilian Cyber Defense (ComDCiber) between 2018 and 2021. Col. Edson served from 2018 to 2020, before his retirement; as did Col. Carneiro, from 2020 to 2021. Alongside only two other high-ranking officials, Col. Edson and Col. Carneiro are representative of a small cohort of Army officers with direct access to the highest levels of Brazilian cyber defense.¹ As such, they are well positioned to comment on the military’s role in conceiving and implementing cyber power alongside other governmental actors. Guided interviews were chosen as a methodological approach because they offer a thematic framework that enables in-depth appraisal of the issues, but still allow for the spontaneity and flexibility of the interviewee (Patton 2002). This flexibility is necessary due to the inevitable sensibilities involved in discussing classified aspects of Brazilian defense strategy. This approach has recognized limits – for example, the value of further interviews to illuminate the consequential roles of other institutional stakeholders, such as the Institutional Security Office (*Gabinete de Segurança Institucional da Presidência da República*, or GSI).

Structurally, the article begins with a brief overview of cyber power’s theoretical roots and how it is defined in Brazilian defense and security policies. Then it draws from the policy and defense documental analysis to narrow down the role of cyber power within Brazil’s institutional framework. The article then shifts focus to analyze Brazil’s military budgetary expenditure and measures as indicators of strategic cyber-power prioritization. It concludes by appraising Brazil’s relational cyber power and its balance of cyber defense, cyber security, and offensive cyber capabilities. It advocates for a series of reforms and initiatives to improve the coherence, coordination and impact of Brazil’s cyber strategy.

¹ Col. Edson was also Gen. Guido Amin’s assistant until July 2020, when he went into the military reserve after more than 30 years of military service. He gave the interview as a retired officer. Before becoming Gen. Amin’s Senior Governance Advisor, Col. Carneiro was a professor of cyber defense at the Inter-American Defense College and cyber defense consultant of the Inter-American Defense Board from 2018-2020. Interviews were conducted in Portuguese in October 2020.

The Rise of Cyber Power

Relational power and threat perception have long been important concepts in international relations theory, particularly emphasized by realists and neorealists. States can choose to either balance against or bandwagon with states they perceive to be threats. A threatened state's assessment of its own relational power and the availability of allies shape its strategic choices (Walt, 1987). A central assumption of neorealism is that "the scope and ambition of a state's foreign policy is driven first and foremost by its relative power capabilities" (Rose 1998, 146). Accordingly, a perceived threat shapes a state's capability development and resource allocation. In this dynamic, technological innovation can enable a state to devise new ways to achieve its strategic objectives (Morgenthau 2003). The rise of the concept of 'cyber power' is an example of this effect, as states and non-state actors increasingly compete to acquire, use and signal cyber capabilities to pursue national strategic objectives. There is a rapidly-increasing effort to define and measure relational cyber power. It is a function of broad international dimensions (the impact of global norms and a state's foreign partnerships) and domestic factors, including governmental, military, economic and socio-cultural considerations. So conceived, cyber power is consistent with Brooks's (2007, 229) reflection that: "the sources of military power are likely to be far more diverse, and embedded in broader social, institutional, and international forces, than conventional analyses of military capabilities often suggest." Its cultivation and exploitation require a "comprehensive" approach that some have argued is easier for authoritarian governments than liberal democracies to embrace (Inkster 2017).

The ubiquitous use of digital and telecommunications technology has elevated cyber power as a new instrument in inter-state (and other forms of) competition and conflict (Arquilla 2021). Inter-state competition is exacerbated by the perceived ability of cyber power to reduce traditional gaps in relational power (Nye 2010). Like other instruments of national power, cyber power should not be conceived in isolation, but as part of a wider toolkit: it is one amongst several means to achieve objectives, both in times of war and peace, and with effects that are not solely confined to cyberspace (Nye 2011; Jervis 2016). The operational modalities of cyber power, particularly in the potential strategic consequences of misperceiving, for example, digital espionage as an offensive cyber operation, amplify the already significant impact of ambiguity and uncertainty in inter-state relations (Jervis 2016; Jervis 2017; Devanny, Goldoni and Medeiros 2020; Devanny, Martin and Stevens 2021). Hence, its strategic purpose can be summarized as "the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment" (Sheldon 2011, 95).

Particularly over the last decade, international relations theory has been increasingly applied to the context of inter-state (and non-state actor) cyber competition and conflict, characterized by persistent engagement in campaigns and the pursuit of advantage below the threshold of war (Fischerkeller and Harknett 2017) – i.e., in the "gray zone" (Raine 2019). Cyber power has

been seen by some theorists as a potent tool in contemporary inter-state competition, in which: “the nonviolent methods of unpeace can be more potent sources of national power and influence than the overt violence of the Clausewitzian war” (Kello 2017, 18). This article does not engage directly with the parallel debate about the merits of conceptualizing offensive cyber operations as ‘cyber warfare’, or the viability of deterrence in cyberspace. Preferring the strategic campaign framework adopted by Harknett and Smeets (2020) and emphasizing, in the Clausewitzian sense consistently applied by Gray (2013), the need to integrate the analysis of cyber capabilities alongside other instruments of national power, which selectively employ instruments including the (threat of) use of force to achieve a politically mandated objective (Rid 2012; Stone 2013). It is also worthwhile to remember Jervis’s admonition against cyber exceptionalism: “cyber is an instrument that, like many others, can be used to support national policies, including ones of deterrence and, more broadly, coercion” (Jervis 2016, 66).

Notwithstanding the scholarly debate about the precise meaning and utility of the concept of ‘cyber warfare’, the evidence suggests an increasingly widespread use of cyber operations as an alternative or complement to military operations in other domains. This is, for example, clear from the Trump administration’s reported choice of limited cyber operations as a more proportionate and controlled response to Iranian operations, including the shooting of a US unmanned aerial vehicle (Barnes 2019; Wagtendonk, 2019). Similarly, Russia has long used cyber operations as part of its efforts to preserve and enhance its influence over neighboring states (Connell and Vogler 2017; Greenberg 2019; Devanny, Goldoni and Medeiros 2020).

Considering its operational flexibility and perceived calibration to reduce escalation risks, cyber is widely seen by influential policy-oriented commentators as “a formidable instrument of national power” (Willet 2019, 85), a striking example of “hybrid” threats exacerbated by globalization and the ubiquity of digital technologies (Hoffman 2018, 38). Cyber is, therefore, a new instrument that should be incorporated in the rank-ordering of relational power between states, whether those states are great powers or primarily actors in a regional security complex (Buzan and Wæver 2003; Nye 2011; Lobato and Kenkel 2015).

In contrast to the aforementioned states, there is no evidence that Brazil has used offensive cyber capabilities. Rather, the country focuses on the development of cyber defensive capabilities. Notwithstanding this posture, cyber power is defined in documents relating to national defense as the “[a]bility to use Cyberspace to create advantages and influence events in this and other operational domains and instruments of power” (Ministério da Defesa do Brasil 2015, 211), which could be interpreted as a more offensively-permissive posture regarding cyberspace operations.

The Brazilian definition of cyber power is present in the 2014 cyber defense doctrine (Ministério da Defesa do Brasil, 2014) and the Glossary for the Armed Forces (Ministério da Defesa do Brasil, 2015). More recent and higher-ranking strategic documents, the National Information-Security Policy (Brasil 2018), and its glossary (published in 2019, updated in 2021), refrain from defining cyber power as well as other terms relating to cyber security and defense, such as: “cyber source” and “cyber protection”. Despite having similar definitions for cyber

security, the National Information Security Glossary takes a more neutral, holistic approach to cyber defense than the Glossary for the Armed Forces, which overtly specifies cyber defense as including offensive, defensive and exploratory actions in cyberspace, in accordance with the Armed Forces' interpretation of cyber power.

The difference in focus between Brazilian documents regarding cybersecurity and cyber defense calls into question the extent to which these two lines of national activity – ideally complementary components of an integrated national strategy – are conceived and executed coherently at the executive level. Despite its similarity in significations, the fact that “cyber power” appears only in the Armed Forces glossary and Cyber Defense Doctrine might suggest a narrower, operational-specific conception of Brazil's cyber power, rather than the more expansive conceptions advocated in the academic cyber-power literature (Nye 2011; Sheldon 2011; Bebber 2017). The following section focuses on the evolving institutional and policy framework in Brazil, and how it encompasses cyber power.

Cyber institutional and policy framework in Brazil

Mirroring the experience of many other states, cyber has been an increasingly salient feature of Brazilian defense and security debates since the mid-2000s (Oliveira 2009; Ramos and Goldoni 2016; Ramos and Matos 2019). At a conceptual level, Brazilian strategy recognizes cyber as a cross-cutting national security theme, relevant across different elements of national power – military, political, economic, and scientific/technological (Franko 2014). The challenge of national cyber strategy is to apply this conceptual understanding in practice through institutions, operational and policy frameworks.

Institutionally, the official documentation of Brazil's strategic conception of cyberspace has evolved since the first iterations of the National Defense Policy (PND) and National Defense Strategy (END), respectively in 2005 and 2008. The END established cyber as a strategic sector – alongside nuclear and space – for which the Army has the lead responsibility. Subsequent iterations of the PND and END were followed by an exploratory cyber defense green book (2010) and a doctrine (2014).

These documents laid the groundwork for Brazilian cyber defense structures: the Center for Cyber Defense (CDCiber - 2012); the National College for Cyber Defense (ENaDCiber), created in 2015 to develop the military cyber workforce; and a joint-service Cyber Defense Command (ComDCiber - 2016), responsible for strategic cyber defense, with CDCiber as its operational arm. This strategic institutionalization of military cyber power includes CDCiber's role establishing the joint cyber defense detachment (JCDD), which provides national cyber warfare capabilities – conducted at a tactical level by the joint detachment of cyber warfare (JDCW).

Comparatively, implementation of the Brazilian cyber defense apparatus mirrors that of its allies, despite discrepancies related to budget and force disposition. The establishment

of ComDCiber as a joint-service arrangement of cyber warfare responsibilities resembles the approach of U.S. Cyber Command – comprising personnel solely from Armed Forces and civilian defense establishment – rather than the broader integration pursued by the U.K. National Cyber Force, which incorporates in one organization not only armed service and defense civilian offensive cyber personnel, but also intelligence officers from beyond the defense establishment (Devanny *et al.* 2021). In contrast, cyber defense of British military networks is more siloed than in Brazil, overseen by service-specific agencies and network-incident treatment centers (CTIRs) (Silva 2019).

The 2018 PNSI (Brasil 2018) announced further reforms of the institutional framework for Brazilian cyber security and defense, bringing it closer to the British model. It established Information Security as a systemic area, encompassing cybersecurity, cyber defense, physical security, and the protection of organizational data. Under the umbrella of Information Security, the 2018 policy promotes the GSI as the lead on cyber security, and effective executor of the Information-Security Policy plans, with the Defense Ministry (MD) – specifically the Army (EB) – responsible for cyber defense. The PNSI states that the MD must support GSI in activities related to cybersecurity, developing guidelines, devices and procedures that act on systems related to national cyber defense.

This is representative of a shift in the institutional framework that elevates cyber security as a priority attributing cyber defense a secondary role – arguably due to the current perception of cybercrime as Brazil's main cyber threat. This new governance structure is a contentious point according to Col. Edson:

the main threat to Brazil is structural and organizational. We have a structure and organization, but what we have we must evolve in terms of legislation, organization, and internal governance. In military terms, we have a structure built, but in terms of everything that goes beyond Defense, it must be built.

A major issue of near-term development is the extent to which defense and GSI lines of effort evolve separately or through coordinated leadership, recognizing the complementarity between cybersecurity and cyber defense.

The PNSI also establishes a National Information-Security Strategy (ENSI) to be developed in five modules: cyber security; cyber defense; security of critical infrastructures; security of confidential information; and protection against data leakage. Currently, only the first module has been published. The national cyber security strategy (E-Ciber – 2020) reiterates PNSI's institutional attributions, restating GSI's cybersecurity leadership and reserving cyber defense to the MD.

The E-Ciber (Gabinete de Segurança Institucional, 2020) balances an overview of the cybersecurity environment with some actionable steps to improve Brazil's cybersecurity. It highlights cyber threats – including from non-state actors – to the Brazilian economy and

critical infrastructure. The prominent strategic threat of cybercrime is reflected in E-Ciber's three objectives: enhanced prosperity and safety of the digital economy; greater resilience against cyber threats; and improved engagement in cyber diplomacy (Gabinete de Segurança Institucional 2020). The strategy proposes more centralized and powerful cyber governance systems; greater government protection of critical infrastructure; improved collaboration with domestic and international partners; and the longer-term development of social maturity and a legal framework for cybersecurity issues. It is, of course, one thing to propose these developments – reactively, amid a cybercrime wave – and another to deliver improved national cybersecurity.

This cybersecurity strategy has been criticized as overly-fragmented, poorly-coordinated and undermined by differing degrees of “cyber maturity” between public- and private-sector actors (Hurel 2020). Furthermore, it refrains from acknowledging Brazil's pioneering developments in internet banking (Longaray et al. 2021), electronic election systems (Saldanha and Silva 2020), and Brazil's leading global role in advocating against cyber espionage (Maurer and Morgus 2014).

As mentioned earlier, neither PNSI nor E-Ciber explicitly define cyber power. Given the organizational shift promoted by the PNSI, the lack of emphasis on integrated national cyber power is perhaps attributable to the lead role of GSI – rather than MD – in matters concerning cyber strategy. The current institutional and policy framework therefore highlights the extent to which Brazil's conception of cyber power is shaped within the context of the national defense establishment, specifically within the Armed Forces. Cyber power is not used as a higher-level, integrating national strategic concept to unify Brazil's separate institutional efforts to promote cybersecurity, resilience and cyber defense.

Notwithstanding this apparent institutional tension in contemporary Brazilian cyber strategy, to achieve optimal coordination and synergy between cybersecurity and cyber defense, force structure analysis should proceed within a wider review of national cyber power, including MD, GSI and other institutional actors. Persistent, effective executive leadership is indispensable for successful development of cyber power (Bebber 2017). This is needed to transcend administrative and institutional divisions between defense and security, federal and state responsibilities. Improved leadership could establish clear lines of responsibility and provide Brazil with the ‘champions for change’ that have been identified as integral to the process of building military cyber maturity (Blessing and Austin 2022, 5). There is therefore an imperative both for senior cyber advisory roles in the presidency, and for more effective legislative oversight and civil-society engagement in cyber strategy.

Given the narrow, militarized conception of cyber power stemming from the siloed prioritization of cybersecurity and doctrinal views that constrain cyber power to the operational level, Brazilian cyber power has been framed within the cyber defense sphere. Hence, the next section offers a focused analysis concerning the Army's (as Brazil's lead cyber service) expenditure, actions, and challenges concerning the development of national cyber power.

Military efforts towards the development of cyber power

As Dagnino (2010) notes, the relevance of a public policy can be seen in its budget. The Plan for Articulation and Equipment (PAED) is END's budgetary counterpart. For the 2012-2031 period, PAED - Table 1 - estimated a budget of almost US\$ 72b (an average of US\$ 3.6b p.a.) for military projects and programs. Cyber defense is listed among other strategic programs, such as Guarani (armored vehicles), Sisfron (border monitoring), and Astros 2020 (missiles and rocket systems). The PAED budget is considered excessively optimistic – based on stable GDP growth of 4.5-5% per year during its time frame, which would make the Brazilian GDP the fifth or fourth biggest in the world in 2030 (Giesteira, Matos, Ferreira 2021). Nonetheless, its planning and execution appear – from analysis of the Multiannual Plan (PPA) – to demonstrate the relative importance of cyber defense within the wider defense budget.

Table 1. EB Programs and Projects X Forecast Budget in PAED X PPA Budget Execution (2012-2019)

EB Programs	PAED Period	Overall value estimated by PAED (US\$) (a)	% of PAED for the EB projects	PAED budget average per year	PPA Executed Value (2012-2019)	PPA Average Executed Value per year (2012-2019)	PAED execution rate (%)
Cyber Defense	2010-2023	162.504.537	1,48	13.542.045 (b)	16.264.075	2.033.009	10,01
Guarani	2011-2034	3.786.878.402	34,54	189.343.920 (c)	87.464.253	10.933.032	2,31
Sisfron	2011-2023	2.176.406.533	19,85	181.367.211 (b)	42.047.197	5.255.900	1,93
Astros 2020	2011-2023	207.985.481	1,90	17.332.123 (b)	33.432.112	4.179.014	16,07

(a) The conversion rate was calculated at US\$1 = R\$ 5,51 according to the market on October 18th 2021; (b) 2012-2023; (c) 2012-2031. Source: author's own elaboration based on (Giesteira, Matos and Ferreira 2021, 21-22).

Although designated as a strategic sector, according to the END, the percentage allocated by PAED for cyber defense (1.48%), as compared with allocations for other Army programs could signify relatively low importance for cyber in the Army. Alternatively, it might demonstrate the lower cost of cyber capabilities, as compared with platform (e.g. armored vehicle) procurement. This is reiterated by the literature concerning cyber power that characterizes it as a strategic domain with lower entry-costs as compared with other military capabilities (Nye 2010, 2011; Sheldon 2011). PAED's total executed value and executed rate percentage for 2012-2019 highlight this difference between non-cyber and cyber costs. An analysis of the PPA (2016-2019)'s National Defense Program helps to clarify the difference in expenditure between strategic programs. As table 2 shows, cyber defense's goals (albeit modest) were totally accomplished during the period.

Table 2. Evolution of National Defense Program goals during the 2016-2019 PPA

Goals	2016	2017	2018	2019
Implement 5.6% of the Cyber Defense Program in national defense	1%	2%	3%	5.6%
Obtain 300 vehicles from the New Armored Wheels Family	35	96	137	197
Conclude the implementation of Sisfron in Mato Grosso do Sul	0.45%	0.5%	0.56%	0.61%
Implement 9% of Sisfron in Acre, Mato Grosso, Rondônia, Paraná and Santa Catarina	0.3%	1.16%	2.04%	2.8%
Implement 85% of the Astros 2020 Multiple Rocket Launcher System	40%	44%	49%	52%

Source: PPA 2016-2019, In: (Giesteira, Matos and Ferreira 2021, 46-47).

In 2019, cyber defense received US\$3.988m, almost double the average across the 2012-2018 period. In September of the same year, during debates around the Cyber Defense Program in the Senate Commission for Foreign Affairs and Defense, cyber defense was projected to receive additional funding in the 2020-23 planning period: US\$10.860m in 2020 and US\$21.753m p.a. from 2021, a total of US\$76.119m (Comissão de Relações Exteriores e de Defesa Nacional 2019), almost five times more than the 2012-2019 period.

There has, however, been a tendency for the actual budget to fall short of senate-appropriated figures. Skepticism remains about whether the projected increase will take full effect (Comissão de Relações Exteriores e de Defesa Nacional 2019). For example, the economic impact of the coronavirus pandemic may undermine commitments to increasing cyber-defense funding, unless a strategic decision is made by the executive to protect the cyber budget (Collucci 2020; Mari 2020; Medeiros et al. 2020).

Budgets, force size and force structure are potentially useful indicators of comparative military cyber power. Given the institutional similarities within the military sphere, a brief comparison with the U.S. is pertinent for contextualizing Brazilian cyber defense expenditure in relation to the leading cyber power. The US's annual cyber defense budget for 2020 was much larger than Brazil's: circa US\$9.6bn, with a similar request (US\$9.8bn) for 2021. The US figures comprise: US\$3.8bn (offensive and defensive operations); US\$5.4bn (cyber security); and US\$556m (cyber-related science and technology investment) (Pomerleau 2020a). Operational investment is manifest in the US Cyber Command's cyber mission force (CMF), comprising 133 teams (6200 personnel) (Cyberspace Solarium Commission 2020). The total relevant force size is, however, twice that of the CMF, including network-management and cyber-security personnel (Pomerleau 2020b).

The vast gap between Brazilian and U.S. military cyber capabilities is not unique. All its allies maintain more modest cyber capabilities than the U.S. For example, the U.K.'s offensive cyber force is an integrated partnership between its signals-intelligence agency, Government Communications Headquarters (GCHQ); the Ministry of Defence (MOD), including the Defence Science and

Technology Laboratory (DSTL); and the human-intelligence agency, the Secret Intelligence Service (SIS). The U.K. launched this national cyber force in 2020 (delayed from 2019), comprising 500 personnel with a US\$343m budget², aiming to grow to 3000 personnel by 2030 (Kerbaj 2019; Sabbagh 2020; Devanny et al. 2021).

The contrast between U.S. and U.K. offensive cyber budgets provokes two further reflections on Brazil's strategic requirement for specific cyber capabilities and force structure. It is unclear, first, to what extent U.S. and U.K. force structures are determined solely by assessed need – especially due to the prominence of cyber defense, as well as cyber security threats – or are compromises between desired force structure and finite resources. In Brazil, the strategic priority of cybersecurity over cyber defense implies competing budgetary expenditures relating to cybersecurity, institutionally associated with GSI. However, given the focus of this article on the narrower, militarized conception of Brazilian cyber power, non-military budgetary analyses are out-of-scope, albeit consequential for any future, holistic account of Brazil's cyber strategy.

Second, beneath force size and budget are deeper questions about expertise, skills-balance and financial resources. As Rebecca Slayton notes: “Without skilled hackers to continually develop new surprises, cyber weapons are readily made obsolete” (Slayton 2016). This is emphasized by both Col. Edson and Col. Carneiro. For the latter: “HR [Human Resources] is the core of the system. You can't get anything done without HR. But the challenges that come with it. Mainly to recruit, train and retain this workforce.” Another key question is the wage differences between the military and the private sector. As Col. Carneiro said: “How do you keep [in the force] a young lieutenant when a private company offers him a salary three times bigger than that of a General?” These challenges are not, however, exclusive to Brazil, but a constant presence in countries developing cyber capabilities, including the U.S. (Ware 2017).

Expertise within a military cyber workforce determines the range of missions – tactical, theater-level and strategic – as well as the need to prioritize between missions, allocating finite resources to developmental, support and operational activities. Brazil must decide what size and balance is needed in its military cyber workforce, including how many top developers of high-quality cyber capabilities are needed (and can be afforded), and the requisite number of less qualified operators. Using that number as a starting point, it should plan to recruit, retain, and train this workforce: what proportion of the target can realistically be met by recruitment into the Armed Forces, as compared with training existing personnel to the required level or incentivizing qualified candidates to join a cyber reserve? Workforce strategy should determine whether it is necessary for uniformed personnel to conduct all defensive and offensive cyber operations: what activities could be performed by civilians, including contractors?³

² The conversion rate was calculated at US\$1 = £ 0,73 according to the market on October 18th 2021.

³ It should be noted that the prestigious Brazilian Army and Air Force engineering institutes both offer computer science courses to civilians and military personnel.

The development of Brazil's defense-industrial base (BDIB) has been a long-term strategic priority (END 2008). The creation of a cyber defense industrial base should now be considered a similar priority, avoiding possible pitfalls, pointed out by Dagnino (2010) when analyzing the BDIB's development, i.e., risks related to inefficiencies and lack of economic and technological competitiveness provided by excessive subsidies and domestic protectionism. Defense strategy should consider how the government can actively manage the growth and international competitiveness of Brazil's private-sector cyber defense and cybersecurity industry. Several policy instruments are available, including incentives for leading multinational companies to increase their Brazilian presence, and designating cyber education as a national priority to accelerate the generation of a talent pipeline of Brazilian students in Brazilian and overseas higher education institutions. Embraer's recent investment in two Brazilian cybersecurity companies is an example of integrating cyber into mainstream defense industry operations (Reim 2020).

National capabilities are important, but alliances and partnerships should also contribute to cyber strategy – as has arguably been underlined by the cyber aspects of the current conflict in Ukraine (Devanny 2022). As stated by the policy documents and interviews, international cooperation is a main pillar in the development of cyber capabilities. Brazil's cyber power benefits from cooperative exercises with its historical allies and partners, including further development of its NATO partnership. In 2019, Brazil took part in a NATO exercise as a team integrated into the Spanish Army, but further participation in 2020 was prevented by the coronavirus pandemic. This raises the question of how neighboring states would respond to Brazil's development of military cyber capabilities. Brazil is well-situated to exercise leadership, bilaterally through horizontal cooperation and memoranda of understanding, and multilaterally through the South American Defense Council or other, ad hoc arrangements. Regional cooperation could include: integrating cyber threat intelligence, assessment and data sharing; developing joint cyber defense capabilities; and coordinating cybercrime strategies.

For the two colonels interviewed, regional alliances are essential for Brazilian cyber defense, and Brazil is perceived as a regional leader. According to Col. Carneiro: "There are many wealthier countries that talk a lot about cooperation, but the caveats are so big that it ends up being superficial." Enhancing trust is essential: "Without cooperation, you make very little progress". Regional cyber cooperation is evident in forums such as the Organization of American States, the Inter-American Defense Board, and in specific activities such as Brazil's support for the cyber security of the 2019 Pan-American Games hosted by Peru.

Besides its regional reach, Brazil is active in multilateral forums, including internet governance diplomacy. A Brazilian diplomat chaired the 2019-21 UN Group of Government Experts (UNGGE) proceedings on "Advancing responsible State behavior in cyberspace in the context of international security." Additionally, Brazil has been described as a leading "swing state" in multilateral negotiations about future global internet governance (Maurer and Morgus 2014).

Applying the defense acquisition trilemma - i.e., balancing national priorities in light of the globalization of technology and production, economic sustainability, and security autonomy - Brazil

must ensure balance between its competing priorities of autonomy, affordability, and technical sophistication in the development of cyber capabilities (Franko 2014). Developing defensive and offensive cyber capabilities and a thriving cyber defense industrial base are clear priorities. This is reiterated by E-Ciber's emphasis on the development of partnership between academia, the public and private sector; and the expansion of Brazil's international cooperation as strategic actions to be taken. The fastest route to the best capabilities is likely to be partnerships with allies and multinational companies, with careful management to ensure that these partnerships contribute directly to rapid and sustainable development of Brazilian cyber capabilities. Even though it comes with its own set of issues – especially in the international arena – the collaborative approach is valid for improving national cyber power, countering cybercrime, defending critical infrastructure against cyber operations, and developing the offensive cyber capabilities needed to credibly threaten a symmetrical response.

Conclusion

Continuation of Brazil's relatively benign geostrategic position and prominent cooperative role within a context of broader auspicious conjuncture (Flemes and Wehner 2012) cannot be taken for granted. The advent of cyber power multiplies security and defense threats and complexifies inter-state (and non-state) competition. National strategy should recognize the potential impact of politico-security trends, domestically and in neighboring states, as well as transnational security threats, and the modulation of relations with external powers such as China and the U.S. Each of these levels of analysis – domestic, regional, and international – should shape development of Brazilian strategy, including the role of cyber power in achieving national objectives. Decisions about cyber capability development, force structure and workforce planning will determine the future effectiveness of Brazil's military cyber power, whether it is aimed at war fighting, coercion, or deception (Lindsay and Gartzke 2020).

These are not solely technocratic or military decisions. Effective use of cyber power requires political decision-makers with sufficient understanding of cyber strategy. As Jervis (2016) noted, politicians' comprehension and risk appetite are important factors in state practices that will shape the understandings of the cyber escalation ladder. This is a dynamic field: reported cyber operations and responses between the US and Iran (Nakashima 2019) – and between Iran and Israel (Baram, Lim 2020) – will be likely to further shape theoretical speculation about how cyber operations are (and should be) conducted (Jervis 2016). Brazil is yet to face a severe disruptive or destructive cyber operation emerging from competition or contestation with another state. It should nonetheless learn from the experiences of other, less fortunate states.

Of the four approaches to reducing cyber risk highlighted by Nye (2016) – deterrence by punishment, denial, entanglement, and normative taboo – Brazil has been visibly active in three: improving cyber defense and broader national cybersecurity; pursuing an internationalist foreign

policy; and playing an active role in international diplomatic negotiations about internet governance and norms. Less visible, but no less important, is its development of offensive cyber capabilities. The assumption that cyber favors offense over defense has been contested (Slayton 2016), but the utility of offensive capabilities as part of a wider strategy of “persistent engagement” has been argued influentially, particularly by Harknett, Fischerkeller and Goldman. Harknett observes that:

the condition of constant contact, and the shifting nature of terrain combine to produce a distinct dynamic: offense persistence – a strategic environment characterized by actors with continuous willingness and capacity to produce security challenges (Harknett 2017, 198).

The persistent nature of threat activity should broaden and deepen the understanding of the contribution of military cyber capabilities to Brazil’s national strategy. They offer more than the current, narrow conception in policy documents as a supportive tool for traditional military operations. The forthcoming module of the National Information Security Strategy, dedicated to cyber defense, will be read closely to determine whether such a shift is emerging.

Not every cyber operation requires a response in cyberspace, but symmetrical responses are an emerging feature of contemporary, inter-state cyber competition. Sovereign offensive cyber capabilities afford states the potential to respond in cyberspace, potentially reducing escalation risk whilst “signaling displeasure” (Valeriano, Jensen and Maness 2018, 43). Not all capabilities are equal, however – as Nye (2010, 9) argues: “relative reduction of power differentials is not the same as equalization”. A mature offensive cyber capability requires years of development and investment, integrating a range of national assets, including the intelligence collection and analysis necessary to understand not only the targeted networks, but also the likely impact of a given operation on the adversary, including assessment of the political consequences and potential for escalation.

Effective cyber power requires more than investment in the military-technical expertise and infrastructure to develop and conduct discrete cyber operations. It includes the development and integration of supporting and enabling structures, encompassing national intelligence capabilities, and the strategic understanding to exploit the technical effects of a cyber operation to achieve specific political objectives (Smeets 2018, 395). Viewed holistically, national efforts to improve relational cyber power might necessitate reforms in cognate areas, such as training and deployment of intelligence analysts in civilian and military agencies (Devanny et al. 2018). National strategy is neither conceived nor implemented in a vacuum. It should include reflection on the implications of strategic developments in other states, e.g. the U.S. turns towards “persistent engagement,” the feedback loops this has created, and how Brazilian cyber strategy should respond (Healey 2019).

For decades, Brazil has not faced a significant state-actor threat to its homeland. There is, to date, no indication that Brazil’s neighbors have developed offensive cyber capabilities sufficient to pose a significant threat, nor indeed that any state in the region possesses the intent to use

such capability were it to exist, or to foster instrumental relationships with cyber-capable allies or proxies (Maurer 2018). However, the affordances of cyber power reduce the historical geostrategic advantage of Brazil's location. Put simply, given the modalities of cyber threats attendant on geopolitical competition, can Brazil afford not to prepare for "persistent engagement" when other states are increasingly active in the cyber domain?

The strategic dimensions of cyber power require an integrated approach to developing capabilities, doctrine, and processes. This approach should recognize imprecise causal relationships and interdependence between political decisions and the fluctuating level and complexity of cyber threats. It should also acknowledge that successful cyber strategy requires more than conventional, bureaucratic approaches. As Hoffman (2018, 42) has observed: "The capacity to generate and execute effective strategies across governmental lines, including private sector and international organizational contributions, is especially salient in complex contingencies." The logic is not "one size fits all": no state should develop offensive cyber capabilities without considering the strategic context in which these capabilities might assist decision-makers in the pursuit of national objectives (Devanny et al. 2021; Blessing and Austin 2022).

This is a cyber manifestation of Gray's (2016, 42) broader proposition that: "Defense planning is the practice of military strategy in grand strategy, and is conducted in a thoroughly political process". Effective reflection on the strategic interplay of military-technical and political factors requires a forum for communication and mutual comprehension between technical and politico-strategic cohorts within national security systems, something that cannot be assumed to occur without facilitation, particularly not in Brazil's current national strategic apparatus (Adamsky 2017; Lima, Silva and Rudzit 2021). The more active and assertive Brazil's international role becomes, the more imperative it will be to reflect on these interdependencies between national strategy and the development of Brazil's cyber power.

Acknowledgements

The article is part of the effort of the Science, Technology and Innovation in Defense: Cybernetics and National Defense research project, approved by the public notice 27/2018, and the Program to Support Teaching and Scientific and Technological Research in National Defense - PRO-DEFESA.

References

- Adamsky, D. "The israeli odyssey toward its national cyber security strategy." *The Washington Quarterly* 40, no. 2 (2017): 113-127.
doi: <https://doi.org/10.1080/0163660X.2017.1328928>

- Arquilla, J. *Bitskrieg: the new challenge of cyberwarfare*. Cambridge: Polity, 2021.
- Baram, G., and K. Lim. "Israel and Iran just showed us the future of cyberwar with their unusual attacks." *Foreign Policy*, June 5, 2020. <https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/>
- Barnes, J. "U.S. cyberattack hurt iran's ability to target oil tankers, officials say." *Nytimes.com*, August 28, 2019. <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>
- Bebber, R. J. "Cyber power and cyber effectiveness: an analytic framework." *Comparative Strategy* 36, no. 5 (2017): 426-436. doi: <https://doi.org/10.1080/01495933.2017.1379833>
- Blessing, J., and G. Austin. *Assessing military cyber maturity: strategy, institutions and capability*. London: International Institute of Strategic Studies, 2022.
- BNAmericas. "Brazil Watch: cable costs, cyber losses." *BNAmericas*, September 7, 2019. <https://www.bnamericas.com/en/news/brazil-watch-cable-costs-cyber-losses>
- BNAmericas. "Why is Brazil so vulnerable to cyber attacks?" *BNAmericas*, January 6, 2020. <https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks>
- Brasil. "Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a política nacional de segurança da informação, dispõe sobre a governança da segurança da informação, e altera o decreto Nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso ix, da lei Nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional." *Diário Oficial da União*, December 27, 2018.
- "Brazil health ministry website hit by hackers, vaccination data targeted." *Reuters*, December 10, 2021. <https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/>
- Brooks, R. A. "Conclusion." In *Creating military power: the sources of military effectiveness*, edited by R. A. Brooks and E. A. Stanley, 228-237. Stanford: Stanford University, 2007.
- Burges, S. "Mistaking Brazil for a middle power." *Journal of Iberian and Latin American Research* 19, no. 2 (2013): 286-302. doi: <https://doi.org/10.1080/13260219.2013.853358>
- Buzan, B. and O. Wæver. *Regions and powers: the structure of international security*. Cambridge Studies in International Relations. Cambridge: Cambridge University, 2003.
- Collucci, C. "Criminosos aproveitam pandemia de Covid-19 para aplicar golpes virtuais." *Folha de S. Paulo*, June 4, 2020. <https://www1.folha.uol.com.br/cotidiano/2020/06/criminosos-aproveitam-pandemia-de-covid-19-para-aplicar-golpes-virtuais.shtml>
- Comissão de Relações Exteriores e de Defesa Nacional. *Relatório de avaliação de política pública: a política nacional sobre defesa cibernética*. Brasília: Senado Federal, 2019. <https://www25.senado.leg.br/web/atividade/materias/-/materia/136367>
- Connell, M., and S. Vogler. *Russia's approach to cyber warfare*. Arlington: Center for Naval Analyses, 2017. <https://apps.dtic.mil/sti/pdfs/AD1032208.pdf>

- Cyber Solarium Commission. *cyber solarium commission report*. Washington, 2020.
<https://www.solarium.gov/home>
- Dagnino, R. *A indústria de defesa no governo Lula*. São Paulo: Expressão Popular, 2010.
- Devanny, J. “Cyber attacks are part of Russia-Ukraine conflict but the west can’t rely on them to stop Putin.” *iNews*, February 25, 2022. <https://inews.co.uk/opinion/cyber-attacks-russia-ukraine-war-rest-cant-rely-stop-putin-1481763>
- Devanny, J., A. Dwyer, A. Ertan and T. Stevens. *The national cyber force that britain needs?* London: The Policy Institute at King’s College, 2021. <https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf>
- Devanny, J., and T. Stevens. “What will britain’s new cyber force actually do?” *War on the Rocks*, May 26, 2021. <https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do/>
- Devanny, J., C. Martin and T. Stevens. “On the strategic consequences of digital espionage.” *Journal of Cyber Policy* 6, no.3 (2021): 429-450.
 doi: <https://doi.org/10.1080/23738871.2021.2000628>
- Devanny, J., L. R. F. Goldoni, and B. P. Medeiros. “The 2019 venezuelan blackout and the consequences of cyber uncertainty.” *Revista Brasileira de Estudos de Defesa* 7, no 2 (2020): 37-57.
- Devanny, J., R. Dover, M. S. Goodman and D. Omand. “Why the British Government must invest in the next generation of intelligence analysts.” *The RUSI Journal* 163, no. 6 (2018): 78-89. doi: <https://doi.org/10.1080/03071847.2018.1562027>
- Fausto, B., and S. Fausto. *A concise history of Brazil*. 2nd ed. Cambridge: Cambridge University, 2014.
- Fischerkeller, M. P., and R. J. Harknett. “Deterrence is not a credible strategy for cyberspace.” *Orbis* 61, no. 3 (2017): 381-393. <https://doi.org/10.1016/j.orbis.2017.05.003>
- Flemes, D., and L. Wehner. *Drivers of strategic contestation in south America*. Hamburg: GIGA German Institute of Global and Area Studies, 2012.
- Franko, P. “The defense acquisition trilemma: the case of Brazil.” *Strategic Forum*, no. 284, (2014): 1-16.
- Gabinete de Segurança Institucional – GSI. “Decreto no 10.222, de 5 de fevereiro de 2020. Aprova a estratégia nacional de segurança cibernética.” *Diário Oficial da União*, February 6, 2020.
- Gabinete de Segurança Institucional – GSI. *Glossário de segurança da informação*. Brasília, 2021. <https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370>
- Giesteira, L. F., P. O. Matos, and T. B. Ferreira. *TD 2672 - a defesa nacional e os programas estratégicos de defesa no PPA 2016 – 2019*. Brasília: Instituto de Pesquisa de Econômico Avançada, 2021. https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=38429

- Gray, C. S. *Making strategic sense of cyber power: why the sky is not falling*. Carlisle: US Army War College, 2013,
- Gray, C. S. *Strategy and defence planning: meeting the challenge of uncertainty*. Oxford: Oxford University, 2016.
- Greenberg, A. *Sandworm: a new era of cyberwar and the hunt for the kremlin's most dangerous hackers*. New York: Knopf Doubleday, 2019.
- Greenwald, G. and E. MacAskill. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*, 2013. <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>
- Harig, C., and K. M. Kenkel. "Are rising powers consistent or ambiguous foreign policy actors? Brazil, humanitarian intervention and the 'graduation dilemma'." *International Affairs* 93, no. 3 (2017): 625-641. doi: <https://doi.org/10.1093/ia/iix051>
- Harknett, R. J., and J. S. Nye Jr. "Is deterrence possible in cyberspace?" *International Security* 42, no. 2 (2017): 196-199. doi: https://doi.org/10.1162/ISEC_c_00290
- Harknett, R. J., and M. Smeets. "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies* (2020), doi: <https://doi.org/10.1080/01402390.2020.1732354>
- Harris, S. *@ war: the rise of cyber warfare*. London: Headline, 2015.
- Healey, J. "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): 1-15. doi: <https://doi.org/10.1093/cybsec/tyz008>
- Hoffman, F. G. "Examining complex forms of conflict: gray zone and hybrid challenges." *Prism* 7, no. 4 (2018): 30-47.
- Hurel, L. *Brazil's first national cybersecurity strategy: an analysis of its past, present and future*. Atlanta: Internet Governance Project, 2020. <https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/>
- Inkster, N. "Measuring military cyber power." *Survival* 59, no. 4 (2017): 27-34. doi: <https://doi.org/10.1080/00396338.2017.1349770>
- Jervis, R. "Some thoughts on deterrence in the cyber era." *Journal of Information Warfare* 15, no. 2 (2016): 66-73.
- Jervis, R. *Perception and misperception in international politics: new edition*. Princeton: Princeton University, 2017.
- Kello, L. *The virtual weapon and international order*. Yale: Yale University, 2019.
- Kerbaj, R. "Female spy to net terrorists as head of 'cyber-SAS'." *The Sunday Times*, September 8, 2019. <https://www.thetimes.co.uk/article/female-spy-to-net-terrorists-as-head-of-cyber-sas-jdxv7bv2m>
- Lima, R. C., P. F. Silva, and G. Rudzit. "No power vacuum: national security neglect and the defence sector in Brazil." *Defence Studies* 21, no. 1 (2021): 84-106, doi: <https://doi.org/10.1080/14702436.2020.1848425>

- Lindsay, J. R., and E. Gartzke. "Politics by many other means: the comparative strategic advantages of operational domains." *Journal of Strategic Studies* (2020): 1-34. doi: <https://doi.org/10.1080/01402390.2020.1768372>
- Lobato, L. C., and K. M. Kenkel. "Discourses of cyberspace securitization in Brazil and in the United States." *Revista Brasileira de Política Internacional* 58, no. 2 (2015): 23-43. doi: <https://doi.org/10.1590/0034-7329201500202>
- Mari, A. "Brazilian army gets hacked." *ZDNet*, November 13, 2015. <https://www.zdnet.com/article/brazilian-army-gets-hacked/>
- Mari, A. "Coronavirus-related cyberattacks surge in Brazil." *ZDNet*, April 6, 2020.
- Maurer, T. *Cyber mercenaries: the state, hackers, and power*. Cambridge: Cambridge University, 2018.
- Maurer, T., and R. Morgus. "Tipping the scale: an analysis of swing states in the internet governance debate." Global Commission on Internet Governance Paper Series no. 2, Centre for International Governance Innovation, Waterloo, Canada, 2014.
- Medeiros, B. P., and L. R. F. Goldoni. "The fundamental conceptual trinity of cyberspace." *Contexto Internacional* 42, no. 1 (2020): 31-54. doi: <https://doi.org/10.1590/S0102-8529.2019420100002>
- Medeiros, B. P., L. R. F. Goldoni, E. S. Batista Junior, and H. R. Rocha. "The use of cyberspace by the public administration in the Covid-19 pandemic: diagnosis and vulnerabilities." *Revista de Administração Pública* 54, no. 4 (2020): 650-662.
- Milani, C. R. S., L. Pinheiro, and M. R. S. Lima. "Brazil's foreign policy and the 'graduation dilemma'." *International Affairs* 93, no. 3 (2017): 585-605. doi: <https://doi.org/10.1093/ia/iix078>
- Ministério da Defesa do Brasil. *Doutrina militar de defesa cibernética – MD31-M-07*. Brasília, 2014. https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf
- Ministério da Defesa do Brasil. *Glossário das forças armadas - MD35-G-01*. Brasília, 2015. https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf
- Morgenthau, H. J. *A política entre nações*. Brasília: Universidade de Brasília, 2003.
- Muggah, R., and N. Thompson. "Brazil's cyber crime problem." *Foreign Affairs*, September 17, 2015. <https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem>
- Nakashima, E. "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers." *Washington Post*, June 22, 2019. https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html
- Nye Jr., J. S. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3 (2016): 44-71.
- Nye Jr., J. S. *Cyber power*. Cambridge: Harvard University, 2010.

- Nye Jr., J. S. *The Future of power*. Public Affairs, 2011.
- Oliveira, E. R. “A estratégia nacional de defesa e a reorganização e transformação das Forças Armadas.” *Interesse Nacional*, April-June, 2009, 71–83.
- Patton, M. Q. *Qualitative research and evaluation methods*. Thousand Oaks: Sage Publications, 2002.
- Pomerleau, M. “Pentagon cyber budget is flat in new request”. *Fifth Domain*, February 10, 2020a. <https://www.fifthdomain.com/dod/2020/02/10/pentagon-cyber-budget-is-flat-in-new-request/>
- Pomerleau, M. “House members worry if the cyber force is the right size”. *Fifth Domain*, March 5, 2020b. <https://www.fifthdomain.com/dod/cybercom/2020/03/05/house-members-worry-if-the-cyber-force-is-the-right-size/>
- Raine, J. “War or Peace? Understanding the grey zone.” *International Institute of Strategic Studies*, April 3, 2019.
- Ramos, A. F., and P. O. Matos. “Changes in the profile of war and reflections on the preparation and use of Brazilian AirPower.” *Journal of the Americas* 1, (2019): 127-139.
- Ramos, W. M., and L. R. F. Goldoni. “Os projetos do exército brasileiro e o alinhamento com as diretrizes da Estratégia Nacional de Defesa.” *Revista Política Hoje* 25, no. 1 (2016): 153-175.
- Reim, G. “Why Embraer defense is investing in two cybersecurity companies.” *Flight Global*, July 23, 2020. <https://www.flightglobal.com/farnborough-2020/why-embraer-defense-is-investing-in-two-cybersecurity-companies/139460.article>
- Rezende, L. B., et al. “Brazilian national defence policy: foreign policy, national security, economic growth, and technological innovation.” *Defense & Security Analysis* 34, no. 4 (2018): 385-409. doi: <https://doi.org/10.1080/14751798.2018.1529084>
- Rid, T. “Cyber war will not take place.” *Journal of Strategic Studies* 35, no 1 (2012): 5–32. doi: <https://doi.org/10.1080/01402390.2011.608939>
- Rose, G. “Neoclassical realism and theories of foreign policy.” *World politics* 51, no. 1 (1998): 144-172. doi: <https://doi.org/10.1017/S0043887100007814>
- Sabbagh, D. “UK to launch specialist cyber force able to target terror groups.” *The Guardian*, February 27, 2020. <https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups>
- Saldanha, D. M. F., and M. B. Silva. “Transparency and accountability of government algorithms: the case of the Brazilian electronic voting system.” *Cadernos EBAPE.BR* 18, no spe (2020): 697-712. doi: <https://doi.org/10.1590/1679-395120190023x>
- Samuels, B. “Trump officially designates Brazil a non-NATO ally”. *The Hill*, July 31, 2019. <https://thehill.com/homenews/administration/455642-trump-officially-designates-brazil-non-nato-ally>
- Sheldon, J. B. “Deciphering cyberpower: strategic purpose in peace and war.” *Strategic Studies Quarterly* 5, no 2 (2011): 95–112.

- Silva, M. G. *Cyber security: a case study of Brazil*. MSc Diss, National Defense University, 2019.
- Slayton, R. “What is the cyber offense-defense balance? Conceptions, causes, and assessment.” *International Security* 41, no. 3 (2016): 72-109.
doi: https://doi.org/10.1162/ISEC_a_00267
- Smeets, M. “Integrating offensive cyber capabilities: meaning, dilemmas, and assessment.” *Defence Studies* 18, no. 4 (2018): 395-410.
doi: <https://doi.org/10.1080/14702436.2018.1508349>
- Stone, J. “Cyber war will take place!” *Journal of Strategic Studies* 36, no 1 (2013): 101-198.
doi: <https://doi.org/10.1080/01402390.2012.730485>
- Stuenkel, O. “China’s diplomats are going on the offensive in Brazil.” *Foreign Policy*, May 15, 2020. <https://foreignpolicy.com/2020/05/15/chinas-diplomats-are-going-on-the-offensive-in-brazil/>
- Valeriano, B., B. M. Jensen, and R. C. Maness. *Cyber strategy: the evolving character of power and coercion*. Oxford: Oxford University, 2018.
- Wagtendonk, A. “Trump called off a military strike against Iran: the US targeted its computer systems instead.” *Vox*, June 23, 2019. <https://www.vox.com/2019/6/23/18714327/iran-us-donald-trump-cyberattack-drone-strike>.
- Walt, S. M. *The origins of alliances*. Ithaca: Cornell University Press, 1987.
- Ware, T. “Feds, DoD need substantial investment to keep skilled cyber talent, says survey.” *Fifth Domain*, May 9, 2017. <https://www.fifthdomain.com/home/2017/05/09/feds-dod-need-substantial-investment-to-keep-skilled-cyber-talent-says-survey/>.
- Willett, M. “Assessing cyber power.” *Survival* 61, no 1 (2019): 85-90.
doi: <https://doi.org/10.1080/00396338.2019.1569895>