

DISINFORMATION IN INTERNATIONAL RELATIONS: EXAMINING THE VULNERABILITIES OF BRAZIL

Leandro Loureiro Costa¹

Introduction

The expansion of Information and Communication Technologies (ICT) in the early 21st century has substantially increased the importance of the internet in individuals' lives. Although, there is no consensual concept for ICTs, definitions are generally proposed to represent all devices, applications, network components, data, systems, and infrastructures involved in modern computing. Thus, the internet, mobile phones, computer programs, social networks, wireless networks, and other services that enable data access, storage, transmission, and processing are considered types of ICTs.

The evolution of systems and tools surrounding this type of technology, along with the increase in connectivity between societies, has also brought new threats. As a result, issues such as information security, cybercrime, cybersecurity, and cyber defense have entered the agendas of various states, particularly Great Powers.

Brazil, at least through normative documents, has emphasized the importance of this issue. The editions of the National Defense Policy have consistently highlighted that the cyber sector is strategic for the country, stressing the need to enhance information and communication technologies, not only within the Armed Forces but also across all state structures. Moreover, through the National Cybersecurity Strategy (E-Ciber 2020), Brazil acknowledges that the intensification of developments in the field of information and communication technology has led to increased use of cyberspace for various activities, including the provision of public services. Furthermore, the expansion of ICTs has enabled an exponential growth in social interactions within the cyber dimension.

In the context of major powers, with the annexation of Crimea by

¹ Federal University of Rio de Janeiro, Rio de Janeiro, Brazil. E-mail: leandroloureirocosta@gmail.com. ORCID: <https://orcid.org/0000-0003-3787-9015>.

Russia and the support for separatist organizations in eastern Ukraine by Moscow, United States authorities have noted the expansion of Kremlin-sponsored disinformation campaigns against Washington and its allies. This advancement occurs through state media outlets, such as Russia Today and Sputnik, but also through increased presence on social networks with hired trolls and the creation of new information emitters (Bunce and Hozíć 2016, 440).

In 2017, reports from U.S. intelligence agencies suggested the possibility that the Russian government had financed the creation and dissemination of disinformation during the U.S. presidential elections, aiming to undermine the campaign of the Democratic Party candidate, Hillary Clinton. Following this event, the European Union (EU) and the North Atlantic Treaty Organization (NATO) sponsored the establishment of the Hybrid Threats Centre of Excellence in Helsinki, designed to investigate potential disinformation threats directed at Europe (Lanoszka 2019). Conversely, in the same year, Russia also raised concerns about the possibility of disinformation campaigns originating from Europe, particularly from the United States, accusing Washington of sponsoring destabilization efforts in various regions of the world, including Ukraine in 2014 during the Euromaidan protests.

States are increasingly improving their capabilities for widespread propaganda and disinformation to alter how people think and act. Furthermore, international actors are also investing in mechanisms of protection to combat this type of threat, such as banning of portals from Russian state media by EU member countries and Canada or the Golden Shield Project of China which blocks content from various sites that are considered threats to security such as the Voice of America (Nichols and Corrêa 2023).

Hence, there is a justification for qualitatively and quantitatively investing in research on the impacts of this new situation in Brazil. The objective of this investigation is to identify vulnerabilities of Brazil relating to the impacts of disinformation operations promoted by state or non-state actors. The development of new insights about the State's weakness regarding disinformation campaigns also contributes to analyzing the technological development of the country in a national security context, especially in the ICT area. In these terms, the cyber sector must be perceived as an indispensable part of national strategy.

Within the realm of information security, the revelations of Edward Snowden in 2013 about the espionage program conducted by the National Security Agency exposed that Brazilian authorities, including President Dilma Rousseff, had their phones tapped by the U.S. agency. In addition, according to BNAméricas (2020), Brazil is the second country most affected

by cybercrime, totaling 70 million victims and 80 billion dollars in financial losses.

More research is also needed to investigate the potentialities and vulnerabilities of Brazil in an international competition context, where various attributes of the ICT domain can impact the distribution of material capabilities among states. Henceforth, technologies such as the Internet of Things, artificial intelligence, 5G, virtual/augmented reality and big data acquire strategic value. All of this, coupled with the increasing need for microprocessors and other types of hardware, requires Brazil, a state proposing itself as a power, to develop its industries in line with these new technologies to compete with main international system actors and ensure its own security.

Methodology

This investigation addresses the concept of disinformation applying it to the field of International Relations (IR). So, the relation of this term as part of a subversion strategy is detailed. To achieve this, the literature on this terminology is reviewed to position it within the dynamics of competition existing in the international system. Thus, the analysis of Lanoszka (2019) about the effectiveness of disinformation operations in altering a state's policy is discussed.

In the case of Brazil, three hypotheses constructed by Lanoszka (2019) concerning the ineffectiveness of disinformation campaigns in producing changes in target states according to interests of the perpetrator are tested: H1) international anarchy generates uncertainties about any information transmitted by adversaries, so rival governments will always expect the worst actions from enemies and will build means of protection against them; H2) citizens that generally trust more in their past experiences, hold preconceptions about foreign political elites and are more likely to adopt ideological perspectives when thinking about the international dimension than state elites, a factor that increases the difficulty of influence from external actors; H3) the state can employ countermeasures even in a scenario of political polarization; it is not incapable of taking actions to reduce the impacts of disinformation campaigns and may even develop a counter-disinformation campaign to minimize the damage from the adversary's operation.

By testing these hypotheses, it is possible to map Brazil's perceptions of risks and defense policies about information security and cybersecurity. This facilitates an examination of potential threats to the information domain,

the formulation of new hypotheses for testing in other investigations and the creation of contributions for future theorizations around the theme of subversion.

The adopted methodology by this investigation aspires to provide a concrete understanding of current context, exploring Brazil's main vulnerabilities to disinformation campaigns. This analysis focuses on contributing to the planning of civilian and military institutions to minimize potential occurrences and ensure a competitive advantage for the state in events related to the instrumentalization of information for political destabilization.

The concept of cyberspace

It is important to highlight that, according to Kramer et al. (2009), there are over 28 definitions of cyberspace, indicating a lack of conceptual consensus. However, in a project led by Professor Nazli Choucri (2015), involving several institutions and titled "Explorations in Cyber International Relations," cyberspace is understood as encompassing: (1) physical structures and telecommunication devices that enable the connection of technological and communication networks; (2) computer systems; (3) networks connecting computer systems; (4) networks of networks linking computer systems; (5) user access nodes and intermediate routing nodes; and (6) constituent data.

Cyberspace is a strategic domain, yet it is also a social one. According to Brazil's Military Doctrine on Cyber Defense (2023), cyberspace is perceived as a virtual dimension formed by computational devices connected to networks, where digital information is transmitted, processed, and stored. Furthermore, cyberspace is classified as an area of action for cyber defense, conceptualized as a set of practices conducted within the framework of a national strategic-level plan aimed at "protecting information assets of national defense interest, acquiring data for intelligence knowledge production, and seeking superiority over the opponent's information systems." The 2020 National Defense White Paper, on the other hand, considers cyberspace as a multifaceted threat scenario, encompassing both state and non-state actors, which can jeopardize the integrity of critical infrastructures essential to systems associated with national security.

Daniel Ventre (2013) characterizes cyberspace as both a strategic and social domain. The author divides cyberspace into three layers. The first is the hardware layer, which comprises the physical devices that support the second layer, the virtual layer, encompassing programs, applications, and information (software). This second layer, in turn, is used and manipulated

by the cognitive layer of users, referred to as “peopleware.” Ventre’s approach reinforces the concept that cyberspace is shaped by user experiences. The existence of the peopleware layer socializes cyberspace, framing it not merely from an electronic and/or mechanical perspective. The way peopleware engages with cyberspace transforms it into a space of social interactions and, consequently, a space of power.

This new operational dimension is substantially exploited on social media, where mass sharing of personal information by users increases risks to national security. Another aspect is that flexibility of privacy enables content customization based on user profiles, defined through data collection of individual behavior during platform access, or even when not in use. This selection is carried out by algorithms based on data collection, allowing dissemination of narratives tailored to the user. Thus, there is an intensification of potential to affect the cognitive field due to easing of sharing, speed of spreading and reaching (Stassun and Assmann 2012; Nichols and Corrêa 2023).

Information and disinformation in IR

The evolution of data analysis technologies, artificial intelligence and machine learning has revolutionized both the ability to economically and politically influence other actors and decision-making related to security. It has also enabled using information as a form of coercion and manipulation on a large scale and increased speed of communication. The significance of this process can be observed in the 2017 United States National Strategy, which includes a chapter on ‘information statecraft,’ highlighting potential risks from Russia and China on this topic (Rosenbach and Mansted 2019).

States have engaged in a “zero-sum race” for data extraction and operationalization. This technological sector tends to have monopolistic companies due to a virtuous cycle: the more data obtained, the more applications developed by these corporations are improved, the increase of profits improve skills to extract and instrumentalize larger amounts of data. This accumulation of data becomes a relevant tool for employing disinformation through the use of algorithms for content targeting.

Disinformation is a type of information designed to deceive. Disinformation campaigns are understood as the systematic effort of an actor to influence the political process by using disinformation to deceive an audience (Fallis 2011; Lanoszka 2019). Disinformation is a component of deception operations that seek to manipulate beliefs to gain advantages and

produce a coercive relationship. Rid (2020) indicates that in the mid-2010s, disinformation operations were altered to a new format in face of technological innovations and internet culture. In this new era, disinformation activities are faster, do not require operational qualification and can be conducted remotely and in a decentralized manner.

A complicating factor is the political use of the term “disinformation.” By pointing out another actor of conducting disinformation campaigns, the accuser seeks to undermine trust in the information released by the accused target, legitimize censorship and sanctions, and strengthen their own credibility. The mutual accusations between the United States and Russia exemplify the use of the term “disinformation” as a tool to influence public opinion. For instance, during the conflicts in Ukraine, the White House accused Moscow of spreading disinformation to justify its military actions, including claims of genocide in the Donbass region or the potential existence of Ukrainian biological weapons laboratories. The United States also accused the Kremlin of sponsoring narratives against vaccines produced by U.S. companies during the Covid-19 pandemic. Conversely, Russia has accused the United States of employing disinformation to destabilize governments not aligned with the West and to incite internal protests in Russia.

Regarding theoretical perspectives, the topic of disinformation is understudied in International Relations (IR). The structural realism approach prioritizes the status of the distribution of material capabilities in the international system and there is no consensus on dealing with intelligence/counterintelligence as a material capability. Lanoszka (2019, 5) suggests that a hypothesis supporting the understanding of intelligence as a component of material capabilities is the comprehension of intelligence as a tool capable of empowering one state in relation to another. In that case, international disinformation campaigns can be considered within the logic of structural realism by interpreting them as an instrument which undermines the material capabilities of the target or weakens the political process of the aimed society.

Although not directly addressing disinformation, classical realists considered the role of information translated by cultural factors which have the ability to influence how states seek to increase their power. Morgenthau highlights ‘cultural imperialism’ as the most effective cultural instrument of power, seeking to control individuals’ minds with the aim of altering power relations between nations. Carr, in turn, refers to power over opinion as being conditioned by status, interests, and economic and military superiority, which facilitate the imposition of ideas on others. Similarly, Aron identifies the “idea” as one of the three objectives pursued by states, alongside power and glory (Suppo 2011, 49).

Lanoszka (2019, p. 5) argues that rationalist theories are the most effective for analyzing the effects of disinformation, as they assume that information holds significant relevance in international relations. Rathbun (2007) notes that rationalists align with structural realists in recognizing that anarchy generates uncertainty regarding the intentions of other actors, though this uncertainty can be managed. Glasser (1994) asserts that states can acquire information about the intentions of other states, allowing them to classify these states as either status quo defenders or revisionist actors, as well as distinguishing between offensive and defensive characteristics.

According to Lanoszka (2019, p. 6), there is no reason to indicate that international anarchy has less force in the relationship between the actors who practice disinformation and those players targeted by these campaigns. On the contrary, disinformation erodes trust and norms, with adversaries being the primary targets of this type of operation. This context is more similar to the international anarchic system than a system where anarchy is constrained (Lanoszka 2019, 6).

Indeed, international anarchy seems to dictate the dynamics in the process of disinformation as the major operations of this kind occurred during times when the anarchical international system was explicitly materialized, e.g. campaigns against Japan in the 1920s propagated by Moscow and the CIA operations against East Germany. However, it is crucial to note that direct antagonism is not a necessary condition for the use of disinformation campaigns. It must also be considered that the actor conducting such operations aims to alter the behavior of its target, either to shift the balance of power in its favor, maintain it, or destabilize the target internally.

The existence of international anarchy does not establish a causal relationship in the construction of “barriers” or “filters” that would enable a state to block all information from other actors. In a conflictual international system, states will strive to seek new areas of influence while also maintaining existing ones. Encountering resistance does not prevent states from instrumentalizing information or achieving some degree of success through its use.

Although uncertainty is considered a central element in realist theory, it is mistaken to assume that distrust invalidates any form of communication signals from external actors or that such signals would always be met with skepticism. Another important point, countering the argument that uncertainty renders information campaigns unfeasible, is that states possess internal characteristics that may facilitate the penetration of these signals.

In summary, the field of International Relations theory still lacks robust explanations regarding disinformation campaigns or the use of information

for political purposes. Reflecting this gap, there is a need to develop analyses capable of constructing theoretical models that address this issue within the complex interactions among actors in the international system.

Subversion and IR

In searching for theorization in International Relations (IR), the perspective on subversion as the reversal of structural power and as a strategic instrument stands out (Maschmeyer 2022; Maschmeyer 2023; Krieg 2023). Actors who hold structural power have the capacity to create interaction structures and shape these frameworks to ensure advantages. Subversion seeks to exploit the structure of the targets to convert advantages into disadvantages for those holding structural power. Vulnerabilities in the structure rules and practices, as well as the agents interacting within and through them, are also explored by subversion. Moreover, subversion operations may also aim to affect shared constitutive identity understandings.

Two crucial factors determine the effects that subversion activities can cause: the structural position of the target entity and the depth of subversion. Regarding the first factor, it is necessary to consider that subversive power cannot change structural positions but can exploit them according to its interests. Consequently, an assessment of possible targets is required for the success of operations through efforts to influence public opinion by disseminating disinformation in the media. Second, the depth of subversion depends mainly on the perpetrator's capacity. When attempting to subvert an adversary, it is necessary to identify vulnerabilities and develop best ways to exploit them. Reversing structural power requires some familiarity with structure's type of structure one strives to attack; thus, states with structures and levels of structural power similar to targets have fewer barriers than those lacking these conditions (Maschmeyer 2022, 88).

Conversely, Krieg (2023) conceives subversion as a strategic tool. He differs from Maschmeyer (2022, 2021) by seeking to relate subversion and war based on Clausewitz's traditional approach. Krieg points out that the characterization of subversion as an instrument of power orchestrated by information networks in coordination without the presence of conventional military operations seems incompatible with traditional definitions of war. Subversion seeks to change the behavior of opponents blurring boundaries between war and peace - even without using coercive means. Additionally, it also exploits socio-psychological, physical and infrastructural vulnerabilities in the target's informational environment to alter socio-political consensus.

Thus, the strategic functionality lies in directing individual and mass awareness and causing regime change in more extreme cases.

For Krieg (2023, 73), narratives are decisive in subversion since they construct realities, manufacture identities for individuals in a community, and are like plots that benefit themselves from “our socio-psychological weaknesses to create “truth” as a socially constructed phenomenon.” This strategic use of narratives in a subversion context is classified as ‘weaponized narratives’ which look to change communication levels between rulers and the ruled and shift communication patterns among various actors coexisting in the decision-making process, such as the press, academia, civil society, and politicians. To be considered subversive, a weaponized narrative must be capable of generating mobilization, fabricating a high level of social orchestration through various networks, and galvanizing violent activism to compel reactions from political leaders.

Mobilization is made of the chaos of the informational ecosystem with intentionally or unintentionally disseminated false information. The consequence is that it becomes nearly impossible to filter information for political decision-making. Moreover, the political incapacity for effective decision-making relatively diminishes trust and legitimacy in government bodies and polarizes public discourse. For this reason, to question government’s incapacities in addressing public concerns can particularly provoke political violence through insurgencies.

On the vulnerability of states to the impacts derived from disinformation activities, Lanoszka (2019) argues that these actions lack effectiveness since they should refute three hypotheses to be successful: H1) international anarchy generates uncertainties about any information transmitted by adversaries; therefore, rival governments will always expect the worst actions from enemies and will build means of protection against them; H2) citizens generally trust more in their previous experiences, hold prejudices about foreign political elites and would be more likely to adopt ideological perspectives when thinking about the international dimension than state elites, a factor that increases the difficulty of influence coming from external actors; H3) states can employ countermeasures even in a scenario of political polarization; it is not incapable of taking actions to reduce the impact of disinformation campaigns and may even develop a counter-disinformation action to minimize the damage from the adversary’s operation .

First hypothesis

The first factor diminishing the effectiveness of disinformation campaigns is that international anarchy generates uncertainties about information from adversaries. Therefore, communication signals emitted by external actors will always be seen ambiguously since there is no certainty about the nature of threats and what can be done to counter them. For a disinformation campaign to succeed in influencing society and destabilizing the political process, it must be considered that individuals would accept any type of external information. To test this first hypothesis in the Brazilian case, it is necessary to understand how the country generally receives and interprets information transmitted by external actors and to analyze the penetration level of foreign media in the Brazilian press environment.

Although not restricted to the internet, main coordinated disinformation efforts in recent years have been carried out in the virtual environment especially through social networks (Rid, 2020). Lanoszka agrees with this trend underlining Russia's increased activities on the internet and the case of Cambridge Analytica capturing data from Facebook for use in the campaigns of U.S. presidential election 2016. In the first decades of the 21st century, there has been a pivotal growth in the number of users on social networks, texting apps and video streaming platforms in Brazil. These services are provided by a few corporations that monopolize this sector. For instance, Instagram and Facebook, the largest social networks in terms of users in Brazil, belong to the same business group: Meta Inc. Furthermore, WhatsApp, the most widely used texting app by Brazilians with a significant advantage over competitors, also belongs to the same conglomerate as Instagram and Facebook.

Google, Android, Gmail, and Chrome respectively are the most used search engine, mobile operating system, email server, and browser in Brazil. All of them belong to the Alphabet Inc., conglomerate known for holding the largest amount of individual data worldwide controlling over 90% of the Brazilian search engine market. YouTube, the largest streaming platform globally and the most used in Brazil, is also owned by Alphabet.

This concentration of Brazilian internet in basically two U.S. companies reveals uncertainty, not only about the security of citizens' information due to these companies' possession of sensitive data, but also about the selection of content accessed by users which are defined by algorithms controlled by very few actors. For example, the algorithm of Instagram and Facebook selects certain types of posts to appear in the primary section (feed) of these social networks and tends to highlight controversial themes that generate a certain type of engagement. This kind of process is accompanied by the possibility of disseminating information with a particular bias through a herd behavior.

This suggests that the lower the diversity of corporations providing services in the social media or data storage sector, the greater the possibility of channels for disseminating disinformation. Further, the absence of active national companies in this area also amplifies the scenario of uncertainty.

Particularly, even before the start of the war with Ukraine (2022), the most used social network by Russian citizens was VK, a private national company. The conflict with Kiev and the worsening of relations between Moscow and the West led to the banning of Facebook in the country. In the search engine market, Google lost to Yandex, and in the texting apps market Telegram also surpassed WhatsApp as the most popular messenger. Something similar also occurs in China; WeChat, Weibo, and Baidu, Chinese companies, surpass all their foreign competitors.

High corporate concentration in the ICT sector and the dominance of foreign companies combined with the weak performance of national industry and lack of political interest in developing this area of economy, leads to the conclusion that the first hypothesis/obstacle is refuted in the Brazilian case. The total control of user data by these companies and the oligopoly of content selection algorithms enable an informational penetration field by potential adversaries; furthermore, it allows the use of sensitive user data, which could pose risks to national security. Thus, the manufacturing of identity and meaning in a community becomes feasible thanks to the management capacity of these corporations over what reaches the user of their services (Krieg 2023). This scenario also reflects the role of the subversive actor, as defined by Maschmeyer (2022), in exploiting the target structure to convert existing advantages in Brazil's informational ecosystem (structural power) into disadvantages.

The construction of a secure information environment and the attainment of strategic advantages also involve the analysis of economic areas related to the technological sector and to the debate on national security. Consequently, the quantity of resources and economic growth can be positive for military power and the lack of them can produce vulnerabilities to state security (Knorr 1977). One of its considerations that most impacts this research certainly relates to the importance of technological innovation in military-economic potential. If expansion of production is more structured in technological development, translated into higher worker productivity, than in simple economic growth it will have greater benefits concerning military potential because economic activities that involve high technology have more synergies with the military industry (Knorr 1973).

To increase the economic-military potential of a state, it becomes essential to make public investments in Research and Development. This can

be evidenced by observing the share of global spending in the area which is substantially concentrated in the most industrially developed countries, with an emphasis on Research and Development in the military sector. In these terms, a state needs to associate national security with development of its high-technology sectors related to the cyber/informational nexus striving to increase industrial productivity and enhance its defense against cyber attacks, building an environment of synergy between the development of economic strategic sectors and means of deterrence against this type of influence. The absence of national companies in this sector demonstrates that Brazil is far from achieving the security-economy nexus, at least in terms of the information and communication area.

Second hypothesis

The hypothesis that citizens trust more in their past experiences, harboring preconceptions about foreign political elites and, for this reason, would be more skeptical about being influenced by foreign actors, is also contested in the case of Brazil. On this hypothesis, the relationship between state and society generally affects how the government conducts its foreign policy. Information access and processing vary between these two entities. For instance, executive members involved in foreign policy decision-making process possess privileged information due to state political-military institutions controlled by these agents. These leaders may make wrong decisions in information processing, relative power calculations, identification of alternatives to address problems, and assessment of consequences of a particular action (Lanoszka 2019).

Nevertheless, society does not have access to this kind of information like decision-makers. Regarding views on foreign policy conduct, citizens usually rely more on their experiences, which is uncommon for those involved in the foreign policy decision-making process. Additionally, citizens would be more inclined to adopt ideological perspectives when thinking about the international dimension than state elites.

In Lanoszka's (2019) view, disinformation campaigns intend to create diligence among executive members involved in foreign policy and the general public, impacting the target's alignment in the international system according to the interests of the state undertaking the operation. For disinformation operations to be effective the capacity of individuals influencing state policies must be considered.

Some contradictions arise when applying this hypothesis in

Brazil and can be explained from a sociological standpoint. Souza (2020) highlights historical-structural elements that train the Brazilian middle class in reproducing an anti-corruption discourse, which in practice ended up overflowing its meaning. This historical-structural process is expressed in the ontological difference between human beings, the foundation of political and social life. It translates into the idea that there is an irrefutable solution to the social and political life of the world, and this answer becomes treated as solid and impossible to contest. For this, a solution must be accepted as universally valid scientific knowledge, defining what is true and what is not.² Those who control these definitions of knowledge validity also tend to decide what is fair and unfair and can justify any form of social and political domination.

In the public context, the competition for success of scientific messages occurs through accessing investment in resources and powerful personal relationships, based on the symbolic dimension of ideas and their effectiveness in social life. Modern Nation-State emerges in the scientific context and in the struggling for legitimacy that is translated through identity presuppositions such as the idea of the “chosen people” and “chosen nation,” as is in the USA, which has resources to strengthen these discourses. In states like Brazil, where a colonized elite has had and continues to have its wealth built through intermediation work and exploitation of those they command, national identity does not assume the “chosen nation” sense but rather that of the “underdog”. The Brazilian identity is the negative image of American identity: while Americans are perceived as better, Brazilians perceive themselves as the worst and the most corrupt.

The colonized Brazilian elite reflects this identity creating its own science from practice and transforms existing knowledge according to the interests of large companies and governments, indicating which knowledge will be hegemonic. In this process of adaptation, the Brazilian elite is deeply influenced by the American elite, in a relational dynamic aimed at the expansion of U.S. capital. Consequently, the “inferiority complex” opens individuals’ cognition to external influence. This trend highlights the instrumentalization of the elite itself by foreign actors.

Penido and Stédile (2020, 44) also stress attempts to colonize Southern strategic thinking carried out through the structuring of cooperation, training, and education actions involving US armed forces and those of other Latin American countries. Among the proposals are the budgetary

² Souza (2020) argues that a significant portion of the idea of scientific knowledge as absolute truth arises from the Enlightenment historical perception of knowledge production detached from any sector or political view. This framework stems from the view of continuity between religion and science, prevalent in the Western context.

limits for the defense industry that are incompatible with local development needs, the transformation of Latin American armed forces into police forces, especially with the growth of military actions against organized crime, and the maintenance of physical US military bases in the region. Meanwhile, internally, Washington does not follow these measures propagated to the rest. States with little investment capacity continue to bet on misguided strategies that accentuate their status of strategic dependence. The aspects of subordination and dependence of elites enable the spread of disinformation movements to be supported by institutions in the state apparatus, without the morphology of a new political class or a new social movement.

Concerning individual predispositions, it is important to mention that narratives exploit social and psychological weaknesses in society (Krieg 2023, 73). These are metaheuristic shortcuts that create meaning and divide the world into good/bad and legitimate/illegitimate. For the formation of these weaponized narratives, pre-existing political polarization, schisms in social fabric and other tension potentials are considered. For these reasons, in addition to the fact that the information and communication sector has a significant external influence, internal fractures in Brazil are a major vulnerability signal for disinformation campaigns.

Third hypothesis

The third hypothesis constructed by Lanoszka (2019) suggests that states can employ countermeasures to minimize the consequences of disinformation operations. The State is not an inert object without the ability to make decisions to reduce the force of disinformation operations. Additionally, the state can counterattack using the same *modus operandi*.

The implementation of these countermeasures involves decision-making processes in the political arena. Lanoszka mentions that the requirement for a rapid response capability to debunk disinformation is crucial for minimizing consequences. However, in the current digital revolution, as Rid (2020) asserts, the spread of disinformation made an extremely complex task the perpetrator identification. Moreover, countermeasures commonly used, such as fact-checking websites or the punishment of internal actors that disseminate disinformation, usually focus on the mitigation of damage caused to the target. Due to the rapid spread facilitated by internet technologies, damage control cannot keep up with the dynamism of disinformation operations.

Regarding the institutional dimension and considering the interactions

between information security and the cyber sector in Brazil, the strategic conception of cyberspace began to take shape with the National Defense Policy (2005) and the National Defense Strategy (2008). The latter positions cybernetics as a strategic domain controlled by the Exército Brasileiro (Brazilian Army). In the following years, other interactions between the documents became concrete, such as the exploratory elaboration of a cyber defense green book in 2010 and a doctrine in 2014.

These documents are the foundation for building Brazil's cyber defense structures, such as the Cyber Defense Center (CDCiber) in 2012, The National School of Cyber Defense (ENaDCiber) created in 2015, and the establishment of the joint service involving The Cyber Defense Command, established in 2016, responsible for strategic cyber defense, with CDCiber performing operational functions. The strategic institutionalization of military power permeated CDCiber in establishing The Joint Cyber Defense Detachment, whose goal is to provide capabilities for cyber warfare conducted at the tactical level by The Joint Cyber Warfare Detachment.

In 2018, The National Information Security Policy (PNSI) was instituted, bringing reforms to the state structure for cybersecurity and cyber defense. The new model defines Information Security as a systemic area covering cybersecurity, cyber defense, physical security and data protection. PNSI designates The Institutional Security Cabinet (GSI) as the cybersecurity administrator and executor of information security policy planning alongside The Ministry of Defense (MD).³ The document stipulates that MD must support GSI in activities related to cybersecurity. Additionally, it must build guidelines and procedures that can be used in systems connected to cyber defense. According to Devanny et al. (2022, 7), this change in the institutional model increases the priority level of cybersecurity, relegating a secondary role to cyber defense.

PNSI also creates The National Information Security Strategy (ENSI), outlining its development in five modules: cybersecurity, cyber defense, critical infrastructure security, confidential information security and protection against data leakage. The development of these modules is still ongoing, and currently, only the cybersecurity module has been published through E-Ciber (The National Cybersecurity Strategy). E-Ciber reinforces that cybersecurity is under GSI's command and cyber defense is under MD's command.

The E-Ciber outlines a series of strategic objectives for Brazil in the field of cybersecurity. The first is to make the country more prosperous and trustworthy in the digital environment. The second is to enhance the country's

³ Primarily the Brazilian Army (EB), which is responsible for cyber defense.

resilience to cyber threats. Lastly, the third objective is to strengthen Brazil's role in the field of cybersecurity on an international level.

Despite the establishment of these institutional frameworks, Devanny et al. (2022, 9) emphasize that there is a kind of conceptual confusion, with the absence of a clear definition for cyber power, coupled with institutional tension mainly due to the organizational shift towards cybersecurity promoted by PNSI. Thus, cyber power is not used as a concept for national strategic integration to unify efforts that exist separately to enable cybersecurity and cyber defense. Despite these distortions, it is important to note that, at least in these publications, Brazil prioritizes the development of defensive and offensive cyber capabilities along with the construction of a cyber defense industrial base. E-Ciber points out the need to foster partnerships between academia and the public and private sectors, as well as the necessity of international cooperation for strategic purposes.

Another mechanism constructed by Brazil to ensure the state's information security is Decree No. 11,856, of December 26, 2023, establishing The National Cybersecurity Policy (PNCiber) and The National Cybersecurity Committee. It defines the principles, objectives, and instruments of The National Cybersecurity Policy and addresses the competence and composition of The National Telecommunications Committee.

The objectives of PNCiber include promoting the development of nationally-oriented products, services, and technologies for cybersecurity; ensuring the confidentiality, authenticity, and availability of solutions and data used in the processing, storage, and electronic/digital transmission of information; promoting responsible behavior for children, adolescents, and the elderly in cyberspace; contributing to combating cybercrime and other malicious actions; promoting the use of cybersecurity protection measures and risk management for the prevention, mitigation, and neutralization of vulnerabilities and cyber attacks; enhancing the resilience of public and private entities to cyber attacks; promoting cybersecurity training in society; contributing to scientific research, technological development, and innovation related to cybersecurity; encouraging coordination and the exchange of cybersecurity information between federal entities, the three branches, the private sector, and society; creating regulatory, supervisory, and control devices to enhance national cybersecurity and developing strategies for cybersecurity cooperation (Brazil 2023).

Regarding the Armed Forces and their relationship with cyber power, Devanny et al. (2022) highlight which, despite being designated as a strategic sector in The National Defense Strategy, the percentage allocated to the area in the budget of the Equipment and Defense Articulation Plan is only 1.48%

compared to other Army programs. It is important to note that the entry cost for technologies associated with cyber power is relatively lower compared to other military capabilities, nevertheless, in 2019, the budget for cyber defense almost doubled on average compared to the period between 2012 and 2018.

On the subject of social media, there is a growing debate on platform regulation, especially following the vandalism of the headquarters of The Three Branches on January 8, 2023, as many of those responsible were mobilized through these websites. A crucial example is the resumption of discussions about the bill 2630/2020, known as the Fake News Bill, to control the spread of misinformation on these platforms. Discussions about regulation are still in their early stages and face significant opposition, both from corporations like Meta and Google and from far-right groups, some of which are known for proliferating misinformation on social media. Despite this, in a survey published by Atlas Intel in April 2023, 78% of Brazilians support the need for legislation that establishes well-defined rules for the operation of social media in the country (Atlas Intel, 2023).

In the juridical arena, Brazil has implemented some countermeasures and prevention activities regarding combating misinformation. As mentioned, the Brazilian electoral process has been dealing with the spread of misinformation since the popularization of social media, reaching its peak in the 2018 and 2022 presidential elections. Since 2019, The Superior Electoral Court (TSE) has adopted measures to combat disinformation focused on campaigns that intend to legitimize Electoral Justice. For the 2022 elections, the Permanent Program to Combat Disinformation was created through Ordinance No. 510, of August 4, 2021 (TSE 2021), and various measures were taken against fake news and profiles that spread this type of content, as well as punishments against social media that kept this information online. These measures brought a series of criticisms regarding the reduction of freedom of expression rights, mainly from multinational corporations operating in the country.

As regards to the analysis of the third hypothesis, it can be affirmed that Brazil has adopted some institutional countermeasures against disinformation campaigns. This does not mean that the country has a completely secure environment regarding this problem. There are still various criticisms that can be made, especially about the lag in the national intelligence system. Nonetheless, it is evident that this hypothesis is the one most corroborated in the Brazilian case. Certainly, the country is not static in the fight against disinformation and has put into practice a series of combat and prevention actions.

Conclusion

This research was conducted to analyze the effectiveness of disinformation campaigns in Brazil and to discuss the policies developed by this state to mitigate the impacts of such activities. Thus, it was necessary to identify Brazil's vulnerabilities regarding the possibility of being a target of disinformation operations promoted by states or non-state actors. To achieve this, the hypotheses/obstacles constructed by Lanoszka (2019) in an article published in the *European Journal of International Security*, titled 'Disinformation in International Politics,' were utilized. In his analysis, the author attempts to corroborate the argument that disinformation campaigns are not effective, because of the existence of various limits to their success. In contrast, Lanoszka's hypotheses (2019) support the assumption of ineffectiveness if applied only to major powers or states with a relatively established ICT sector. They seek to spend efforts in cybersecurity, through the development of this pivotal area for national strategy.

In this research, it was found that the first two hypotheses of Lanoszka failed in the Brazilian case, but the third was partially corroborated. In the first, the high concentration in the ICT sector by foreign companies along with the incipient presence of national industry and the lack of political interest in this area of the economy, indicates that Brazil is vulnerable to disinformation campaigns. As shown by data on the ICT sector, Brazil still has much smaller numbers in terms of encouraging national development in this area compared to other developing states, such as India. The lack of state control over these companies' algorithms and the collection of sensitive user data by corporations also emphasizes risks to national security. Most internet services are provided by U.S. big tech companies: Meta, Alphabet, and Microsoft.

The second hypothesis is also refuted, on account of Brazilian society having internal predispositions that increase the likelihood of the success of disinformation operations, such as political polarization and external cultural influence. Polarization is translated not only through highly contested elections but also by the growth of a moral condemnation discourse among groups, especially from the idea of the existence of moral representatives against a corrupt ensemble that becomes responsible for all social evils. This external cultural influence manifests in the colonial experience that hinders the development of autonomous national thinking and dictates perceptions like innate corruption in Brazilian society and Western primacy.

In conclusion, through testing the third hypothesis, it can be stated that Brazil partially complies with the requirements proposed in this obstacle

by Lanoszka. There are several mechanisms that provide countermeasures by the country's authorities regarding information security and cybersecurity, such as PNSI and PNCiber. Preventive measures also emerge within the scope of the Superior Electoral Court to try to preserve the course of elections. There is also a considerable increase in public awareness of the need for the regulation of social networks regarding the proliferation of disinformation, which could provide more countermeasure alternatives.

Further studies are needed to investigate the effectiveness of this type of disinformation instrumentalization, as well as investigations that analyze the impact of subversion in a strategic perspective. It becomes essential to conceive the differences between states regarding defense capabilities in relation to the problem, as much of the literature on the subject restricts itself to major powers and ignores the operational space of emerging states where digital technology plays a crucial role.

References

- Atlas Intel. 2023. Pesquisa sobre o impacto das redes sociais no bem-estar e segurança dos brasileiros. <https://cdn.atlasintel.org/95c2051e-cfcf-480d-b69b-d91c413bbd97.pdf>.
- Barnett, M. e R. Duvall. 2005. "Power in international politics". International Organization, v. 58, n. 1, 39-75.
- Brasil. 26 dez. 2023. Presidência da República. Casa Civil. Decreto nº 11.856. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,que%20lhe%20confere%20o%20art.
- Bunce, V. e A. Hozic. 2016. "Diffusion-proofing and the Russian invasion of Ukraine", *Demokratizatsiya*, vol. 24, n. 4.
- Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge: MIT Press.
- Claverie, B. e F. Du Cluzel. 2022. *Cognitive warfare: the advent of the concept of cognitics in the field of warfare*. NATO Collaboration Support Office.
- Fallis, D. 2016. "What is disinformation?". *Library Trends*, v. 64, n. 3.
- Knorr, K. 1973. *Power and Wealth*. New Jersey: Princeton University Press.
- Knorr, K. 1977. "Economic Interdependence and National Security". Em *Economic Issues and National Security*. Kansas: Allen Press.

- Krebs, R. e P. Jackson. 2007. "Twisting tongues and twisting arms: the power of political rhetoric". *European Journal of International Relations*, v. 13, n. 1.
- Krieg, A. 2023. *Subversion: the strategic weaponization of narratives*. Washington, DC: Georgetown University Press.
- Lanoszka, A. 2019. "Disinformation in international politics". *European Journal of International Security*, v. 4, n. 2, 227-248.
- Maschmeyer, L. 2021. "The subversive trilemma: why cyber operations fall short of expectations". *International Security*, v. 46, n. 2, 51-90.
- Maschmeyer, L. 2022. "A new and better quiet option? Strategies of subversion and cyber conflict". *Journal of Strategic Studies*.
- Maschmeyer, L. 2023. "Subversion, cyber operations, and reverse structural power in world politics". *European Journal of International Relations*, v. 29, n. 1, 79-103.
- Ministério da Defesa [Brasil]. 2023. *Doutrina Militar de Defesa Cibernética – MD 31-Mo7*. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31Mo7DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf>,
- . 2020. *Defense White Paper*. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivreimportugues2020.pdf.
- Nichols, G. C. Leal e C.R. Corrêa. 2023. "A Guerra Cognitiva nas Redes Sociais e suas Implicações para a Segurança dos Estados". *Revista da Escola Superior de Guerra*, v. 38, n. 82, 101-121.
- Penido, A e M. E. Stédile. 2021. *Ninguém regula a América: guerras híbridas e intervenções estadunidenses na América Latina*. São Paulo: Expressão Popular/Fundação Rosa Luxemburgo.
- Rid, T. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
- Rosenbach, E. e K. Mansted. 2019. "The Geopolitics of Information". The Belfer Center for Science and International Affairs.
- Souza, J. 2020. *A guerra contra o Brasil: como os EUA se uniram a uma organização criminosa para destruir o sonho brasileiro*. Rio de Janeiro: Estação Brasil.
- Stassun, C. e S. Assmann. 2012. "Hipermobilidade estética e dispositivos de controle de circulação: o desejo de ser notado encontrado na internet". *Revista FAMECOS*, Porto Alegre, v. 19, n. 2, 153-168. <https://doi.org/10.15408/famecos.v19n2p153-168>.

org/10.5007/1984-8951.2012VI3n102p153.

Strange, S. 1998. *States and Markets*. London: Bloomsbury Academic.

Suppo, H. R. 2011. “A importância do chamado soft power no paradigma realista clássico”. *Mural Internacional*, v. 2, n. 2, 47–50.

TSE. 2021. Secretaria de Gestão de Informação e do Conhecimento. Portaria nº 510. Brasília. <https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-510-de-04-de-agosto-de-2021>.

Ventre, Daniel (ed). 2013. *Cyber Conflict: Competing National Perspectives*. Hoboken: John Wiley & Sons.

ABSTRACT

Some of the foremost concerns regarding information security in International Relations revolve around the repercussions of misinformation on the internal political process, with the aim of undermining adversary states. Certain studies have indicated the inefficacy of such endeavors in yielding substantial results in modifying the behavior of the targets. Given this assumption, this research endeavored to assess, in the context of Brazil, three hypotheses questioning the efficacy of this type of instrument. The conclusion is that the country finds itself in a state of strategic vulnerability but has undertaken institutional efforts to counteract the potential ramifications of a disinformation campaign.

KEYWORDS

Disinformation, Subversion, Information Security, Brazil

Received on January 21, 2024

Accepted on January 30, 2025