Contexto Internacional
vol. 42(1) Jan/Apr 2020
http://dx.doi.org/10.1590/S0102-8529.2019420100002

The Fundamental Conceptual Trinity of Cyberspace

Breno Pauli Medeiros*
Luiz Rogério Franco Goldoni**

Abstract: This article is based on the premise that the increasing human interaction in cyberspace elevates it to the level of a strategic domain and, as such, raises theoretical and practical challenges for International Relations. It is founded on an epistemological reflection on the fundamental assumptions of the paradigms that permeate International Relations. The main objective is to conceptualise cyberspace as the strategic domain in the 21st century, as well as to develop an analytical framework that will both provide evidence and investigate the resilience of the foundations of current International Relations, these being specifically, the following precepts: i) sovereignty based on territoriality, ii) state monopoly of power, and iii) accountability between international actors. With this in mind, the approach refers to defence documentation and scientific sources in order to reach a definition that will characterise cyberspace, considering its technical, scientific and strategic aspects. At the same time, the bibliographic work underpins the development of the analytical tool known as the Fundamental Conceptual Trinity of Cyberspace, based on the characteristics of the cyberspace domain: i) deterritoriality, ii) multiplicity of actors, and iii) uncertainty.

Keywords: cyberspace; cybernetics; territory; accountability; International Relations.

Introduction

This research is about the inherent aspects of cyberspace: deterritoriality, multiplicity of actors and uncertainty. These characteristics elicit reflection about the basic elements relative to the state: territory, concentration of power and accountability. The analytical tool "Fundamental Conceptual Trinity of Cyberspace[1]" (FCT) was developed with the aim of improving the understanding of those aspects and how they may affect the theoretical bases of International Relations (IR) and Political Science. It relates to an analytical-reflexive effort that is limited both by the complexity of the theme and by the spatial limitations of this publication. The work aims to contribute to the recent, albeit already broad

* Brazillian Army Command and General Staff College (ECEME), Rio de Janeiro-RJ, Brazil; breno.pauli@gmail.com. ORCID iD 0000-0002-9839-5252.

** Brazillian Army Command and General Staff College (ECEME), Rio de Janeiro-RJ, Brazil; luizrfgoldoni@gmail.com. ORCID iD 0000-0001-5257-9470.

literature that addresses the theoretical and practical interfaces between cyberspace and international relations, as illustrated in the works of Reardon and Choucri (2012), Kremer and Müller (2013), Cavelty (2015) and Kello (2017), among others.

In his studies, Thomas S. Kuhn notes that the evolution of science is defined by paradigms that were established to solve specific problems. Social and technological development raises continuous challenges for the existing paradigms, reaching a point where science in its *status quo* can no longer explain certain social and technological transformations, requiring the development of new scientific paradigms (Kuhn 2018). Although Kuhn's reasoning is applied to natural science, it prompts reflections on social sciences and works as a starting point for dealing with the theoretical uneasiness addressed in this work.

Cyberspace emerges as an interactive domain capable of challenging the *status quo* of IR theory due to its peculiarities, which escape the traditional logic of the state. In this respect, this article considers Kuhn's views as it relates to the fundamental precepts of IR in the context of increasing interaction between society and cyberspace.

Human activity disassociates itself from a physical space to the extent in which society advances into the technical-scientific-informational environment (Santos 2009). Although the virtualisation of day-to-day activities is neither complete nor definitive, it is strong enough to permeate relationships of power between people, states, businesses and various other actors.

The interaction between society and the cyber domain engenders social change, posing practical challenges to international relations, starting where cyberspace becomes a distinct domain compared to the traditional land, air and sea domains.[2] While the latter domains are governed by a territorial concept due to the materiality of land borders and conceptions of air and sea space, cyberspace is characterised by its partial immateriality, expressed by the interconnectivity of information networks.

Among the elements affected by the peculiarities of the cyber domain are the fundamental territory precepts, the state as the exclusive and legitimate holder of power,[3] and accountability. These stand out because they are more regularly observed in the relations between states in the 20th century. Therefore, they are the ones more relevant to this work.

The prominence of the 'cyber' theme alluded to in defence documentation, political speeches, and the media in general, supports the belief that society is gradually becoming more dependent on this domain. Thus, analogous to other spaces, it is considered strategic in nature, according to the interpretation that different countries give to cyberspace (The Federal Government of Germany 2016; Ministry of Defence [Brazil] 2016; The White House 2017; The State Council Information Office [China] 2019).

As far as understanding international relations is concerned, the ubiquity of human relations in cyberspace gives rise to social developments that can be interpreted as anomalies.[4] In order to highlight its unusual nature, it is necessary to analyse some of the peculiarities inherent in cyberspace.

The work begins with a brief conceptualisation of cyberspace through a bibliographical review that elicits an analysis of the contents of scientific articles and defence documentation. The documents were selected according to two principles: firstly, the state's lev-

el of influence, one that illustrates a broad – although comparable – strategic perception of cyberspace from different global (USA and China) or regional (Brazil and Germany) actors; and secondly, a more practical principle, namely that several other players in the cyber domain do not make public comparable documentation regarding their strategic views towards cyberspace, for example, Israel, Russia and North Korea.

According to Krippendorff (2004), this approach enables theoretical-epistemological sequencing of the analysed content. Thus, the development of the concept of cyberspace through the bibliography reviewed expresses both the scientific definition of the cyber domain and the strategic value that certain states place on it.

After conceptualising cyberspace, this study analyses how its peculiarities challenge the fundamental precepts of IR. Lastly, the work proposes the development of the 'Fundamental Conceptual Trinity of Cyberspace' (FCT), an analytical tool which prioritises three conceptual premises inherent in the cyberspace domain: i) deterritoriality; ii) multiplicity of actors; and iii) uncertainty.

Defining cyberspace

In view of the indiscriminate use of expressions derived from the cyber domain, it is important to clarify the term 'cyberspace' itself. 'Cyberspace' and 'cyber domain' will be treated here as synonyms. The prefix 'cyber' followed by nouns such as 'war,' 'terrorism,' or 'space' induces in the reader's imagination the transposition of concepts represented by those nouns to a virtual arena. While this practice simplifies and transmits the message to the receiver, albeit crudely, it is analytically reductionist, as it does not consider conceptual aspects inherent in the cyber domain. Therefore, it is important to conceptualise cyberspace as a social interaction domain.

To this end, this work uses definitions of cyberspace found in the armed forces manuals, official defence documentation and scientific publications. The different interpretations of cyberspace constitute a spectrum that goes from more technical definitions on the electromagnetic field, where the flow of information and the interconnectivity of cyberspace are developed (Cohen 2007; Rattray 2009), to more theoretical definitions that consider the interposition of physical and technical layers working in synergy to allow cyberspace to function (Libicki 2009; Ventre 2013). It includes interpretations that consider cyberspace a new domain for power relations (Kuehl 2009; Sheldon 2011).

The technical end of the spectrum of cyberspace definitions is prominent in the defence documentation of different countries, and when examined, they illustrate these countries' interest in cyberspace. The analysis of the interpretations provided by defence agencies and institutions from different countries is significant due to its recognition of cyberspace as the fifth strategic domain. According to Lobato and Kenkel (2015), the recurring presence and the perspective given to cyberspace in defence documentation legitimises it as a new arena for human interaction and particularly for war. These documents also consider deterritoriality in the nature of cyberspace and as a driver of new threats, albeit not necessarily state threats.

In its Military Cyber Defence Doctrine (2014: 18), Brazil views cyberspace as a 'virtual space, consisting of computational devices connected to networks or not, where digital information travels, is processed and/or stored'. The breadth of the definition contained in that document fulfils its doctrinal role, but it does not address the inherent nor the resulting nature of cyberspace, such as its ability to cross borders or its status as a new strategic domain.

The 2016 National Defence White Paper[5] (LBDN in the original), in turn, recognises that cyberspace enables the advent of state and non-state threats. Cyberspace is considered a strategic domain due to the possible damage to critical infrastructure that a cyberattack can cause. According to the document, 'a cyber threat has become a concern because it endangers the integrity of sensitive infrastructures that are essential to the operation and control of various systems and agencies directly related to national security' (Ministry of Defence [Brazil] 2016: 57).

In its turn, Germany's *White Paper 2016: On German Security Policy and the Future of the Bundeswehr* (The Federal Government of Germany 2016) considers cyberspace as a realm for new, though not necessarily state, threats, such as terrorism, cybercriminals, fraudulent use of identity, industrial espionage and damage to infrastructure. The document also provides a brief definition of cyberspace: 'Cyber space is the virtual space of all IT systems linked and linkable at data level on a global scale' (The Federal Government of Germany 2016: 36). This definition previously appeared in the 2011 'Cyber Security Strategy for Germany' (Federal Ministry of the Interior [Germany] 2011: 14), which addresses cyberspace in the following way:

> The basis for cyberspace is the internet as a universal and publicly accessible connection and transport network, which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.

On the other hand, the Dictionary of Military and Associated Terms (DOD), of the Office of the Chairman of the Joint Chiefs of Staff (2019: 56), defines cyberspace as: 'A global domain within the information environment, consisting of an interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.'

The view adopted by the National Security Strategy of the United States of America (The White House 2017) takes the technical conception established by the DOD's dictionary further, by treating cyberspace as one of the domains for ensuring the stability and security of the American people, and by defending the infrastructure and critical institutions for the country's operation from cyberattacks. The document also recognises the deterritoriality and the multiplicity of actors in cyberspace, making it clear that many actors can rival US capabilities through the use of cyberspace and without necessarily crossing the borders of the country.

The document recognises cyberspace as a tool for projecting power and influence, and as a key element in modern warfare. In this sense, cyberspace is treated as a means of preserving peace by renewing capabilities together with the defence industrial base, and the military, nuclear, space and intelligence areas.

The recently published Chinese Defence White Paper, in turn, does not provide a clear definition of cyberspace. Nonetheless, it places cyberspace as a vital strategic domain for Chinese security:

> Cyberspace is a key area for national security, economic growth and social development. Cyber security remains a global challenge and poses a severe threat to China. China's armed forces accelerate the building of their cyberspace capabilities, develop cyber security and defence means, and build cyber defence capabilities consistent with China's international standing and its status as a major cyber country. They reinforce national cyber border defence, and promptly detect and counter network intrusions. They safeguard information and cyber security, and resolutely maintain national cyber sovereignty, information security and social stability (The State Council Information Office [China] 2019: 14).

Generally speaking, the defence documentation of different countries views cyberspace as an existing space dependent on the interconnectivity of physical elements, which allows the creation of a global information network. As society becomes dependent on this new domain, defence documentation characterises it as strategic and essential for security and defence. The documentation also recognises the deterritoriality and multiplicity of actors in cyberspace.

The definitions and interpretations presented in this work do not contemplate the more theoretical approaches found on the academic side of the definition spectrum of cyberspace. In this conceptual myriad, there is room for a more general understanding of cyberspace, such as that arising from the interconnectivity of interlinked devices, a view that is presented in the defence documentation. Rattray's (2009: 254) approach works as a bridge between the technical and theoretical sides, taking into account that he views cyberspace as a physical and artificial domain: 'However, cyberspace is actually a physical environment; it is created by the connection of physical systems and networks, managed by rules set in software and communications protocols.'

Cohen (2007: 255) considers that cyberspace is best understood 'as connected to and subsumed within an emerging, networked space that is inhabited by real, embodied users and that is apprehended through experience'. His approach is noteworthy for presenting an understanding of cyberspace based on the experiences of the users. Given this perspective, the use that multiple actors make of its peculiarities transforms cyberspace. The ability of various actors to transform and exploit cyberspace – which is the operational domain where critical infrastructure, public networks and weapons systems are embed-

ded – contributes to the destabilisation of the state's assumption of itself as the sole holder of power, as will be demonstrated later.

Other authors treat cyberspace as a domain created by physical and electronic layers. These approaches encompass the technical and theoretical aspects of cyberspace. Daniel Ventre (2013) views cyberspace as a domain that cuts across the traditional natural domains. Ventre organises cyberspace starting from the hardware layer, a set of physical devices capable of supporting the virtual layer of programmes, applications, and information (software), which in turn are used and manipulated by the cognitive layer of users, called 'peopleware.' Ventre's approach supports the concept that cyberspace is shaped by the users' experience. The existence of the peopleware layer socialises cyberspace by not considering it solely from an electronic and/or mechanical point of view. The use peopleware makes of cyberspace is what transforms it into a social relations space and, therefore, a space of power.

Libicki (2009) also adopts the view that cyberspace is the result of the interaction between different layers. According to Libicki, a physical layer (hardware) represents the basis of cyberspace, consisting of boxes and wires. In other words, the physical electronic components represented in all types of smart and interconnected devices. The second layer is syntactic, consisting of the instructions and commands given to the devices by the developers to comply with their programming and to communicate with each other. Lastly, comes the semantic layer, which represents the information contained in the machines. Libicki's approach also recognises the cyber domain as a less tangible medium compared to land, air and sea, since it is configured by immaterial elements in the form of binary data, which constitutes the syntactic and semantic layers.

When dealing with the strategic aspect, given the permeability of cyberspace relative to traditional domains, Sheldon's (2011: 96) interpretation is noteworthy:

> It is worth noting the difference between the terms cyberspace and cyber power. Cyberspace is the domain in which cyber operations take place; cyber power is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can be cognitively effective with individual human beings.

After studying the different interpretations of cyberspace, Kuehl (2009: 28) views it as an artificial and unique domain, whose main differentiating factor is that it was originally developed by the human use of computer networks. In this respect, Kuehl proposes his definition:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

The different conceptions presented above represent a range of interpretations appropriate to the scope of the cyber domain. However, in order to establish a starting point for the FCT, it is necessary to define cyberspace so that it takes the elements set out in the previous definitions into account and, at the same time, can work as a benchmark for its use in this article.

Thus, cyberspace can be understood as a unique domain of artificial human interaction, disassociated in part from physical elements, which permeates the traditional domains. It exists through the connection of different layers: technological, technical and personal. It has unique peculiarities, made possible by its partial immateriality and expansive interconnectivity. Cyberspace is constantly evolving as technology advances, and is constantly changing as different actors use it, shaping it to meet the most diverse needs.

The proposed cyberspace concept is in line with previous definitions. It is considered a unique domain because, in contrast to the natural domains, it was created by human beings. It is partially disassociated from physical space because, although it exists in the electromagnetic spectrum, cyberspace is anchored by electronic equipment that works as nodes in an expansive network made up of such devices and connected by a flow of binary data being sent from one device to another. As new equipment, technologies and actors are being connected through cyberspace, new meanings are attributed to the network, which, in turn, is transformed concomitantly into a strategic tool for weapons systems, a space for demonstrations through social networks, and a commercial environment for banking systems, companies, customers and so on.

As a domain shaped by user experience and technological advances, cyberspace is constantly changing. Therefore, the proposed definition is not definitive and needs regular updating, as the use of a growing number of actors shape and transform cyberspace.

Peculiarities of cyberspace

At this stage, the three pillars that form the FCT – deterritoriality, multiplicity of actors and uncertainty – will be introduced. Each of the intrinsic characteristics of cyberspace can at times independently challenge specific territory concepts and pretexts, the state as the sole holder of power, and accountability. However, theoretical and practical challenges occur mainly when these peculiarities work in synergy and various actors use them to pursue their own agendas.

The deterritoriality of cyberspace

Unlike traditional domains, actions in cyberspace are not constrained by territorial boundaries or border controls. The immateriality of cyberspace is demonstrable in the flow network of the electromagnetic spectrum. However, it is anchored by mobile devices operated in traditional domains. Thus, cyberspace simultaneously permeates and encompasses other domains.

The paradoxical character of the territorialising and deterritorialising elements of cyberspace is notorious. On the one hand, material layer devices are inserted in different territories and are therefore subject to all traditional territorial precepts. However, once the virtual layer is triggered and becomes indistinguishable binary data transmitted at instantaneous speeds by the electromagnetic spectrum – immaterial in nature – territorial precepts based on physical elements do not hold. This results in an alternative, partially immaterial space, without borders, airspace and/or national waters (Hildebrandt 2013).

The partial immateriality of cyberspace enables the transposition of physical boundaries by different informational flows of the electromagnetic spectrum, as highlighted by the defence documentation presented earlier. Thus, the most obvious peculiarity of cyberspace is its break with the traditional concepts of territory as physical space bounded by borders.[6] The virtual flows of cyberspace that ignore physical territorial boundaries drain the zonal concept of territory.

The concept of territory, according to Haesbaert (2004: 95-96), 'unfolds along a continuum that goes from the more "concrete" and "functional" political-economic domination to the more subjective and/or "cultural-symbolic" appropriation' of an area, or zone, demarcated by border limits, deeply associated with the exercise of power, by virtue of its boundary limitations. It is up to the borders to delimit the territory as a zone of power, recognised and legitimised in the form of the national state. Thus, the national territory is the (physical) space in which the state acts, guaranteeing its legitimacy and power over its resources, population, wealth and other material aspects, serving as the geographical basis of the sovereignty of a state (Coelho Neto 2013).

The conception of national territory is expanded with the concept of territorialisation, as different groups demonstrate power in a precise area, delimiting it and having the limits recognised by others (Raffestin 1993). From territoriality, other actors, not necessarily states, construct and deconstruct territories, appropriating the physical space in different times and modes. Souza (1995: 81) remarks on the multiple scales and different temporalities that the territory can assume, due to the territoriality processes:

> Territories exist and are constructed (and deconstructed) on the most diverse scales, from the narrowest (e.g., a street) to the international (e.g., the area formed by all the territories of the member countries of the United Nations North Atlantic Treaty Organisation – NATO); territories are constructed (and deconstructed) within the most different time scales: centuries, decades, years, months or days; Territories may have a permanent character, but they may also have a periodic, cyclical existence.

The process of territorialisation corresponds to the 'attempt by an individual or group to reach, influence or control people, phenomena and relationships, by delimiting and asserting control over a geographical area' (Haesbaert 2002: 119). The instrument for delimiting and controlling access to a geographical area is the border, which allows some to enter and excludes others. In this sense, the territory assumes the character of a zone. That

is, the delimitation of boundaries by the process of territorialisation gives rise to a certain zone in which power is exercised, transforming it into a territory.

According to Ayres Pinto, Freitas and Pagliari (2018), the zonal nature of the territory becomes the fundamental foundation of the sovereignty of the modern state. However, given the current scenario of globalisation, the zonal conception of the territory faces the phenomenon of global networks. Commercial, criminal, and financial networks, among others, penetrate and interconnect different territories. In the globalised world, 'the network is conceived as a technical matrix, referring to the existence of a dense, complex and interconnected system of technical infrastructures that enable the new possibilities of territorial organisation of societies and presents itself as a locomotive of social transformation' (Coelho Neto 2013: 22).

By transferring Coelho Neto's understanding of networks to the cyber domain, the network as a matrix of dense and interconnected technical infrastructures can have its nodes represented by the different expressions of the physical layer in cyberspace, such as interconnected cables, satellites and devices. The flows that make up the networks are represented by infoways, that is, 'the means by which digitalised information circulates' (Ferreira Neto 2017: 7). Thus, the cyber domain becomes an interconnected network that encompasses traditional domains.

When connecting the different nodes of the network (physical devices), the flows of the infoways (virtual layer) take on a reticular logic.[7] These flows, when sent from one device to another, are disassociated from physical space because they consist of information transmitted by the electromagnetic spectrum. Thus, while physical devices are within territories, the flows that interconnect these devices cross the boundaries of different territorial zones.

This development in the human relationship with space transforms territories, as Haesbaert (2007: 30) remarks:

> Thus, within the territorial diversity of our time, we must first take into account this growing distinction between a zonal territorial logic and a reticular territorial logic. They interpenetrate and intermingle in such a way that the effective hegemony of the state-zone territories that marked the great political patchwork, allegedly uniterritorial (in the sense of only admitting the State form of political-territorial control) of the modern world, today realises it is forced to live with new circuits of power that design complex territorialities, usually in the form of network territories, such as the territorialities of drug trafficking and globalised terrorism.

Because of the interrelationship of reticular and zonal logic, cyberspace becomes a space of power, whereas infoways represent the social expression of different actors in a space anchored by physical devices – but expressing themselves virtually in the electromagnetic spectrum.

Compared to a space of power in today's social relations, and because of its immaterial nature, cyberspace poses practical and theoretical challenges to the concept of territory as a power zone, while the concept of zone territory is understood because the access to physical space across borders can be controlled. The immateriality (even partial, considering that it depends on physical elements to work) of cyberspace guarantees free circulation in the globalised world, the crossing borders of freely and the penetrating of territories without major problems.[8]

Territory is no longer understood as a delimited physical space, but as the 'locus in which the inherent power in a relationship is constantly exercised and confronted' (Ferreira Neto 2014: 8). It can be observed in cyberspace while flows and infoways represent the means for social relations.

While the concept of territoriality has been traditionally based on physical space, as society integrates the cyberspace network, the flows of the cyber domain can be understood as the territoriality of different actors expressed by an artificial and partially immaterial domain. The territorialising effect of flows in the globalised world by more able actors is acknowledged by Milton Santos (2002: 239) when arguing that networks and territories undergo corresponding transformation, 'above all in the interest of the hegemonic actors in economy, culture and politics, and are fully incorporated in the new world trends. The technical-scientific-informational environment is the geographical expression of globalisation.'

In the globalised world marked by the integration of networks, advances in telecommunications can be demonstrated, among other things, by the flows of social relations in the cyber domain. This flow legitimises the cyber domain as a space of power in the 21st century, and challenges territorial concepts based on material zonal logics. The flow of information and data that make up the reticular logic of infoways, being partially disassociated from material space, does not obey the same zonal logic of territories. Therefore, it cannot be contained by a physical boundary that limits the traditional reticular logic for systems of transport, trade, and weapons, among others.

As explained above, border flow control, together with its delimitation, are the main defining elements of the territorialisation process (Haesbaert 2007). However, if the immaterial flow of cyberspace infoways is capable of overcoming the control of border flows, it becomes endowed with a deterritorialising character, as far as physical territorial logic is concerned.

Because it is a space of power without physical delimitations (when seen in its virtual layer), which does not obey the basic assumptions of territory, the reticular logic of cyberspace results in draining, even if partially, of the zonal logic of the territory. This draining, in turn, is a demonstration of the deterritorialising aspect of cyber space.

The disassociation of physical space provided by the internet and cyberspace[9] enables the circulation of flows regardless of origin, destination or content. The interconnected infoways in cyberspace represent the scope and the instantaneous temporality of the current globalisation process.

The operationalisation of the cyberspace virtual layer undermines the physical limitations of traditional domains and poses significant challenges for different areas of international relations, security and defence. The practical challenges present themselves when the effects of the operationalisation of the electromagnetic spectrum appear in the physical layer of cyberspace, which is inserted in other territories, resulting in different reactions and having repercussions in other domains. Thus, acts performed on devices physically located in a given territory may have effects or consequences on others, under the sovereignty of different states, but connected to the same network.

Cyberspace has a deterritorialising nature because of its partial immateriality, unlike traditional concepts of territory, where access can be controlled and the zonal logic is physically limited. Nevertheless, at the same time and paradoxically, because it is the object and means of relationships of power, when able actors use the peculiarities inherent in cyberspace to pursue their different interests, cyberspace is territorialising.

The territorialising and deterritorialising paradox of cyberspace not only highlights a range of practical challenges for international relations and globalised society in general, but also demonstrates the complexity of the theme, reverberating the theoretical challenges to paradigmatic concepts that underlie the current understanding of international relationships. In this sense, the paradox of the concept of territory in the cyber domain generates challenges to the zonal logic of the territory as a geographical outline in which the state dominates by controlling border flows.

The multiplicity of actors

In its conception, cyberspace is considered a military tool, evolving from ARPANET to the worldwide computer network that, in its ubiquity, typifies today's society (Castells 2003). As cyberspace becomes the stage for power relations through the performance of able individuals, the number of actors able to access and interact with this new power domain grows exponentially, increasing the number of users by around 1.125% in the world, between 2000 and 2019 (Internet World Stats 2019).

Today, more than half of the world's population uses the internet and enters cyberspace more broadly. The low costs to access and operate it is what differentiates the cyber and space domains. Although similar to cyberspace in deterritoriality and strategic value,[10] space can only be accessed and/or operated by a select group of entities with sufficient technical and financial means (Choucri 2012).

As elements of civil and military infrastructure fall into the cyber domain, and the number of actors in the domain grows, states are no longer the only ones able to exploit it. The increasing number of users, together with the insertion of critical infrastructure in the cyber domain, generates a proliferation of vulnerabilities and threats due to the increasing dependence of different sectors of today's society on cyberspace.

As society's dependence on cyberspace increases, individuals or groups with expertise and interconnected devices are able to exploit it according to their agendas. According to Sheldon (2011: 98): 'Rather, the character of cyberspace is such that the number of actors

able to operate in the domain and potentially generate strategic effect is exponential when compared to the land, sea, air, and space domains.'

Due to its ubiquity and low costs of usage, cyberspace enables the gap of capability between different actors to narrow down. Nye Jr. (2012: 173) refers to this phenomenon as 'diffusion of power,' 'represented by the large number of actors involved and the relative reduction of power differentials between them.' That is, new actors have the ability to exert power in the cyber domain[11] through actions aimed at harming infrastructure, people and/or institutions. Despite the fact that the state is the sole legal holder of power, the diffusion of power allows it to be exercised by any individual or group with connected devices that could exploit the growing worldwide dependence on cyberspace.

Adding to the diffusion of power, the ease in developing and distributing cyber weapons, that is, computer code with the aim of exploiting vulnerabilities and/or causing some direct or indirect damage, contributes to the pursuit of increasingly aggressive cyber capabilities by different actors, effectively undermining the highly interconnected global security system (Shaheen 2014).

Due to the free flow of information and the partial immateriality of cyberspace, the capability gap in the cyber domain can be narrowed down and demonstrated in two different, albeit not necessarily excluding, ways:

- Cyberspace as a means of exploitation itself, through the virtual layers (syntactic and semantic), i.e. the lines of code that make interconnected devices perform a certain action. In this context, technical knowledge allows actors to use software capable of attacking certain targets. Cyberweapons, therefore, are not physical; they exist in the different layers of cyberspace and can be sold, copied, altered and disseminated through the network to anyone interested.

- Cyberspace as a communication tool. The global reach of cyberspace allows individuals, groups and institutions with different ideologies, interests and goals to connect with each other.

The multiplicity of actors contributes to a scenario in which cyber mastery can be operated in such a way that intelligence agencies can monitor conversations of heads of state, entrepreneurs, and academics around the globe; terrorist groups can recruit and train dissidents from other countries; activists and social movements of diverse backgrounds and nationalities can coordinate their demonstrations; and hackers can cause physical damage to the strategic infrastructure of a particular state or company, regardless of the country in which the hacker and target are located. Thus, the usual threats from states continue, only now with new threats in the cyber domain.

Choucri argues that deterritoriality empowers and enables new practices for multiple individuals, and, at the same time, it generates new means for state sovereignty. According to Choucri (2012: 14), '[t]he cyber international "landscape" of actors, actions, technology, and power relations is rapidly changing.'

Although the more developed states are able to control the elements of the physical layer of cyberspace (satellites, submarine cables, servers, among others), the narrowing

capability gap in the virtual layer enables the more vulnerable states, dissidents, separatists, terrorists, activists and the military to take advantage of the diffusion of power to effectively engage in cyberspace. It is also a way to compensate for possible weaknesses regarding weaponry and other traditional power capabilities. It is more practicable and cheaper for a group of hackers to commit cyberspace sabotage against a specific power plant than to train men and acquire and operate armoured vehicles in order to destabilise a power plant by using the traditional kinetic means, for example.

Due to the decrease in costs of accessing and operating in cyberspace, the cyber domain is now considered a locus of power relations where multiple actors can pursue their own interests, especially due to cyberspace's asymmetry, where the more sophisticated a state infrastructure is, the more vulnerable it becomes to cyberattacks (Nye Jr. 2010). Although the state remains the legitimate holder of power in today's international relations, in practice, international politics is no longer a monopoly of powerful government actors, as new actors join the complex game of international relations.

Uncertainty

The most elusive of the peculiarities of cyberspace stems from its logic and internal dynamics that hinder the process of identifying and attributing actions to specific actors. In turn, this undermines the accountability processes now trending in international relations that, together with the multiplicity of actors and the interconnectedness of the network, result in cyber uncertainty. When addressing the relationship of cyberspace with traditional military thinking, Kallberg and Cook (2017) determine the following elements as sticking points:

- The absence of object permanence in the cyber domain. Except for the physical layer, objects can be created, erased, moved and manipulated, without the slightest implication of mobilisation, logistics or manoeuvre, as they only exist virtually. It is worth noting that this is a direct consequence of the immaterial aspect of cyberspace.
- Computational execution speed. While tactical decisions can be made quickly and even instinctively, strategic decisions require more time in order to ascertain the several elements, scenarios and possible outcomes. The computational speed of a malignant action in cyberspace limits the decision-making reaction by affecting the capability to communicate with the hierarchical command. This raises issues about the use of artificial intelligence, a debate so complex that it exceeds the limits of this article.
- The absence of a means to measure success. Given its highly complex, interconnected and changing nature, an action in the cyber domain is not easily detected or quantified once its effects are not necessarily instantaneous – particularly in cases of intelligence and target tracing – and they are hidden underneath the complex layers of semantic and syntactic networks.

- Anonymity arising from the multiplicity of actors and the nature of informational flows disassociated from identification in cyber space, combined with the difficulty in measuring the effective success of a cyberattack.

Elements such as absence of object permanence and the computational execution speed do not directly influence the uncertainty aspect. However, they corroborate the previous interpretation of cyberspace as a domain disassociated from space and essential for modern strategic relations. The absence of success metrics and the anonymity cited by Kallberg and Cook are the elements that culminate in the inherent uncertainty of cyberspace.

The difficulty in measuring success in the cyber domain is due to the lack of quantifiable feedback on results, the degree of efficiency, and the absence of a chain of events that culminates at any given time (Kallberg 2016). That is, considering the complex nature of the tangle of interconnections and semantic and syntactic layers of cyberspace, it is difficult to trace a given outcome back to a specific causative action. The results will not always be exact or observable, since the effects are not necessarily kinetic and/or instantaneous.

Anonymity, understood as the impossibility of attributing[12] actions to specific actors in certain places, is inherent in the cyber domain due to the governance processes and the internet architecture itself (Wheeler and Larsen 2003). The importance given to attribution in cyberspace is necessary because it is from the identification of misdemeanours that the legal and political process of accountability begins (Hunker, Hutchinson and Margulies 2008), by demanding the pre-established behavioural standards between states (Grant and Keohane 2005).

Nevertheless, the use of proxies[13] and other technologies can disguise an attack and ultimately assign it to third parties. Recently, the CIA's practice of spreading malware[14] containing parts of the code written in Russian and North Korean was made public. Thus, if CIA malware were detected, the company or agency that was investigating the security breach could erroneously assign it to whomever the CIA wanted to incriminate (Wikileaks 2017).

The diffusion of power adds to the uncertainty, whereas multiple actors, not necessarily state actors, are capable of affecting basic network infrastructures, having access to sensitive information and monitoring specific targets, without necessarily being identified or made accountable. The element of uncertainty appears due to the difficulty of attributing anonymous flows in cyberspace, and this may cause different consequences for international relations, such as a counterattack on possible opponents, who may not necessarily be guilty, leading to an uncontrolled escalation of the conflict. In the absence of responsibility, different actors abuse the anonymous aspect of cyberspace and use it for different purposes, including as a tool for both protection and attack.

According to Cavelty (2015), the difficulties in accountability in the virtual layer of cyberspace lead to a speculative international context. Since accountability is not reliable, contextual responsibility is used in *cui-bono* logic. That is, it is assumed that the person responsible is the player who benefits from the action. Shaheen (2014) points out that the difficulty in assigning responsibility and consequently holding perpetrators accountable

results in low political costs for cyberattacks; this, together with the diffusion of power and proliferation of cyber weapons, gives rise to an instability in the offensive-defensive balance and an increasingly aggressive stance on the part of cyber actors.

Therefore, the element of uncertainty corresponds to the myriad of aspects and technologies pertaining to cyberspace that hinder the process of attribution and consequent accountability, a fact that can lead to the escalation of war and/or incrimination of third parties. Uncertainty is deeply linked to the diffusion of power and the deterritoriality aspect of the cyber domain, resulting in a situation in which multiple actors can act globally without being held accountable for their actions, effectively undermining the process of global accountability.

The fundamental conceptual trinity of cyberspace

With the widespread use of the cyber domain by society in the 21st century, the assumptions of international relations as addressed in this article have to be considered in the light of a new social, technological and political reality.

The arrival of cyberspace as a space of power with characteristics that permeate other domains generates practical challenges to international relations. In fact, because the peculiarities of cyberspace allow for ways of interacting between actors that had not previously been considered in the *status quo* of IR scholarship, these challenges can potentially cause theoretical setbacks for the field.

In this regard, the FCT works as an analytical tool that facilitates the understanding of the complexities originated by cyberspace as a new international relations domain. The FCT responds to these contemporary relations between state and non-state actors in cyberspace as a strategic domain, and as such, realises its peculiarities and internal logic.

The possible difficulties arising from the symbiotic relationship developed between cyberspace and society in the 21st century can be analysed individually if the assumptions are promptly confronted with the peculiarities that make up the elements of the FCT. However, the adversities imposed by cyberspace on international relations are not individualised; they occur through the combination and overlapping of deterritoriality, multiplicity of actors and uncertainty. In this context, the FCT can be applied, albeit superficially, to some theoretical IR paradigms that emphasise certain precepts, and can potentially challenge them.

Analysing the historiography of IR scholarship, Schmidt (2013) traces an evolutionary process comprised of phases, debates, or historical events, which culminates in the historical-methodological approach corresponding to the IR field, which, until this day is shaped by a western view, grounded in the pioneering spirit of English and American scholars. According to Schmidt (2013), one of the main effects of Thomas Kuhn's work on the IR scientific community was the academic frenzy among authors to establish their respective theories as the paradigms proper to the scholarship. In this context, Schmidt claims that the realist paradigm emerged as the initial exponent with which different the-

oretical approaches aligned or disagreed, resulting in the establishment of new paradigms to be challenged, which characterises the paradigmatic plurality of the IR academic field.

Even before the advent of cyberspace, the perspectives of the exponents of the main theoretical trends of IR are the ones considered when defining it. As globalisation advances, they can be viewed in the context of cyberspace, so that when analysed from the paradigmatic perspective of IR, the peculiarities of cyberspace align with different schools of thought.

The political prominence that the individual assumes in the liberal (Kant 2018) and neoliberal (Keohane and Nye Jr. 1987) discourse can be observed from the point where deterritoriality and the diffusion of power in the global network allow independent actors and groups to act in the cyber domain. This is not only through soft power, organising demonstrations and sharing ideals – as noted in the Arab Spring – but because there is a new distribution of hard power, since individuals can exploit the vulnerabilities caused by introducing critical infrastructure in cyberspace. Thus, in a cursory analysis, liberal paradigms have a certain theoretical inclination to understand the cyber phenomenon more holistically.

Because it is a more recent paradigm, the constructivist approach is predominant in the literature common to cybernetics and IR. The constructivist view tends to focus on how cyberspace assists in the expansion of defining and transforming ideals, which contributes to changes in the social *status quo*. The process of viewing cyberspace and identifying certain activities as threats is not the result of a material determination, but of an intersubjective interpretation of the domain (Reardon and Choucri 2012). Thus, like the liberal approach, the constructivist approach comprises deterritoriality and multiplicity of cyberspace actors.

However, while liberal and constructivist theoretical paradigms (Onuf 1979; Wendt 1992) are based on the co-operation and accountability of international actors, state or otherwise, dependence on this system can be challenged since actors can act anonymously in cyberspace, without the correct attribution to the actions or at some point implicating those responsible.

On the one hand, the globalised aspect and the independence of the individual contribute to the liberal and constructivist understanding of cyberspace, albeit inevitably challenged by the uncertainty principle; on the other hand, realist approaches that accept the anarchic character of international relations tend to present a theoretical predisposition for the recognition of this same anarchic character in the uncertainty of cyberspace.

Nevertheless, the concept of territory as a zone of power with increasing border rigidity, present in the works of Carr (2001), Morgenthau (2001), and Aron (2003), can be challenged by the deterritorialised logic of the virtual cyberspace layer and by the interconnectivity of territories. This could happen because of immaterial flows in transit through the electromagnetic spectrum, capable of affecting the physical layer and other infrastructures within the target territory.

The Stuxnet case and the destabilisation of Iranian nuclear power plants illustrate the state's ability to exploit the virtual layer of cyberspace. Thus, traditional state threats use

cyberspace anonymity and deterritoriality to cross borders virtually, free from legal and diplomatic consequences, as they will be hard to identify and be held responsible. From this perspective, the costs of conducting an attack are significantly reduced, which make the offensive-defensive balance unstable and contributes to a context of increasing aggression in cyberspace (Shaheen 2014).

The realist emphasis on the state as the sole international player, due to its monopoly of power, is also challenged in cyberspace when considering the detrimental effects that individuals can generate, whether for political, ideological and/or criminal purposes. The Wannacry[15] ransomware – supposedly developed by independent[16], financially-motivated hackers – has spread across basic multi-country infrastructure, causing millions of dollars in damage, and disrupting critical services (Thompson and Mullen 2017). Essentially, exemplifying how non-state actors can act globally and cause damage to traditional power holders.

The proliferation of cyber threats capable of exerting both soft and hard power erodes the sense of security and reliability in cyberspace-dependent infrastructures and systems, resulting in the strategic valorisation of cyberspace and the need for its securitisation, as demonstrated in the defence documentation previously stated.

Incidents such as those mentioned above and the peculiarities of the cyber domain, in general, challenge the different theoretical predispositions of the multiple IR schools of thought. In this context, approaches based on the territorial conception as a source of state power are challenged by the deterritorialised flows in which multiple, not necessarily state actors, are able to pursue their interests. On the other hand, schools guided by the principles of co-operation and accountability are tested by the principle of uncertainty and difficulty in attributing authorship in cyberspace.

Such theoretical considerations are beyond the scope proposed by this work and demand an in-depth analysis on this theme. However, they illustrate the permanence of the theoretical and paradigmatic debate alluded to by Schmidt (2013), after the advent of cybernetics, and how the FCT can be applied in order to clarify how the fundamental precepts of the main paradigms of the IR scholarship include the advent of social relations in cyberspace, given that global cyberattacks, espionage, monitoring, and other incidents that pose challenges at the political and theoretical levels tend to become more frequent in an interconnected society.

It is important to emphasise that the works of different exponents of the IR academic field were established before the advent or more widespread operationalisation of cyberspace. Expecting the respective authors to understand a social and political phenomenon in cyberspace proportions would be unfair to them.

Final considerations

Through a brief bibliographic review, the present work sought to conceptualise cyberspace through academic and governmental sources, promoting a holistic and strategic view of how this new domain challenges international relations. With this in mind, the FCT was

developed, a tool that analyses the traditional conceptions of territory, monopoly of power by the state, and accountability, in the light of cyberspace peculiarities, illustrated by the elements of deterritoriality, multiplicity of actors and uncertainty.

Cyberspace, as a power domain, engenders challenges arising from its idiosyncrasies to society in general, demanding new ways of thinking and interacting in the international context. In order to mitigate such challenges and help in the general understanding of the cyber phenomenon and its impacts on international relations, the FCT enables the theoretical-analytical reappraisal of the fundamental precepts of IR from an analytical perspective that comprises the cyber domain together with the other domains. Thus, the FCT is relevant in helping to understand the cyber phenomenon in today's social relations, recognising the potential for theoretical-analytical limitations of the IR literature.

In light of the FCT, some principles of the realist, liberal and constructivist theories are weakened, even if superficially and/or as a consequence of their time. Constructivist and liberal views are challenged as actors – state or otherwise – use the principle of uncertainty to pursue their interests with no accountability for their actions,[17] as per the anarchic view of the realist approach. In contrast, the flows of the virtual cyberspace layer permeate the rigid territoriality and border control characteristic of realism, engendering new avenues of power hitherto unanticipated by leading realist theorists. In addition, as the diffusion of power generates operational capacity for multiple actors, the realist conception of the state as the sole holder of power is drained.

On the other hand, liberal and constructivist approaches benefit precisely from the action of multiple actors, co-operating and contributing to the construction of new relationships, processes, and identities on a global scale, favoured by digital flows. Nevertheless, the grounding of these approaches on principles of global accountability is undermined when various actors resort to the principle of cyber uncertainty to avoid the accountability process.

The conclusions thus far contain a superficiality because of the constrictions in this work, which led to the holistic application of the FCT in order to illustrate its use. Therefore, a possible new research agenda could be an in-depth application of the FCT on specific theoretical trends, in order to obtain a more detailed investigation of the effects of cyberspace on the theory or theories in question.

Another possible research agenda concerns the interrelationship of cyberspace with the air and space domain. As these domains are relatively newly operationalised and have profound implications for the future, an analysis of their interrelationship is relevant and could contribute to the understanding of such domains as strategic, each with their own logic.

Finally, by considering defence studies as a branch of IR studies (Diniz 2016), it is expected that the challenges posed to international relations will unfold into defence studies and military relations. In this context, the FCT could also be useful in helping to understand the complexity of the cyber domain.

Acknowledgments

This article is part of the project 'Science, Technology and Innovation in Defense: Cybernetics and National Defense,' approved by Public Notice 27/2018, Support Program for Teaching and Scientific and Technological Research in National Defense – PRO-DEFENSE IV.

Notes

1 The title comes from the three elements that are part of the analytical tool and is inspired by the Clausewitzian Trinity, summarised as i) violence; ii) chance; iii) subordination of war to politics. For more information, see Clausewitz (1982) and Aron (1986).

2 It is important to note that the operationalisation of outer space raises theoretical and practical issues similar to cyberspace. However, the subject requires further examination in itself, which would deviate from the paper's aim. Hence, the term 'traditional domain' herein used refers to land, air and sea domains.

3 Referred to here as a synonym of violence as in 'physical intervention of an individual or group against another individual or group (or against oneself)' and inherent in the power of the state: 'Violence is a characteristic feature of political power or government power' (Stoppino 1998: 1291-1293). It is also pertinent to note that the legitimacy of the monopoly of violence by the state has been questioned previously (Bull 2002).

4 The widely available access to information, global communications and advances due to the digitalisation of aspects of everyday life represent a rupture of previous social, economic and geographical constrains that limited human interactions.

5 The 2016 edition of the LBDN was only approved by the National Council in December 2018, as per the legislative decree PDS 137/2018, published in the Official Journal on 17 December 2018.

6 The logic of zonal territoriality also applies to maritime and air domains in the form of national/international waters and airspace respectively. The spatial domain and its exploration also pose challenges to the zonal logic of territory, a subject that, although relevant, is beyond the scope of this article.

7 Reticular logic refers to a more traditional comprehension of networks, that is: the interconnectivity between different nodes within a network. Differently from the zonal logic that encompasses a large spatial area.

8 This statement has exceptions such as China and North Korea, who notoriously restrict their populations' access to cyberspace through government controls in companies. However, these players still operate in the cyber domain, carrying out attacks such as the one perpetrated by North Korean hackers against the Sony Pictures movie studio (Peterson 2014) and the debatable (Weaver 2018) Chinese attack on the supply chain of computer chip makers of companies like Google and Apple (Robertson and Riley 2018).

9 It is important to emphasise that cyberspace and internet are not synonyms. Cyberspace is an operational and electromagnetic domain; the internet is a network of computers inserted in this domain (Cepik et al 2014).

10 Birdwell (2011) addresses strategic and operational similarities and differences between cyberspace and space domain in more depth.

11 Understood as cybernetic power, that is, one's ability to obtain the desired effects in and/or through cyberspace (Nye Jr. 2010).

12 The concept of responsibility in cyberspace comes from the following perspective: 'determining the identity or location of an attacker or an attacker's intermediary' (Wheeler and Larsen 2003: 1).

13 Refers to the use of servers located in other countries. Thus, country X can attack and make it look as if the real perpetrators are in country Y, for example. Additionally, it can also imply a larger group (or state) utilising the services of hackers or smaller groups.

14 The most common types of 'malicious software' are viruses or worms, which are capable of causing damage

and self-replicating in computer networks and systems (Goldani 2005).

15 Malware, which encrypts files on a device and requires a ransom payment for their release.

16 Although there is a debate regarding a possible involvement of North Korea (Bossert 2017), its attribution is mainly on a *cui-bono* logic.

17 Although there have always been actions conducted with 'plausible deniability,' cyberspace makes these activities much more pervasive and available to more actors.

References

Aron, Raymond. 1986. *Pensar a guerra, Clausewitz: a era européia*. Brasília: Universidade de Brasília.

_____. 2002. *Paz e Guerra entre as nações*. 1st Edition. Transl. Sérgio Bath. Brasília: Editora Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo.

Ayres Pinto, Danielle, Riva Sobrado de Freitas and Graciela Pagliari. 2019. 'Fronteiras virtuais: Um debate sobre segurança e soberania do Estado.' In Danielle Jacon Ayres Pinto, Maria Freire and Daniel Chaves (eds), *Fronteiras Contemporâneas Comparadas: Desenvolvimento, Segurança e Cidadania*. Macapá: Editora da Universidade Federal do Amapá, pp. 39-52.

Birdwell, M Bodine and Robert Mills. 2011. *War Fighting in Cyberspace: Evolving Force Presentation and Command and Control*. Air University, Maxwell AFB, Al Air Force Research Institute.

Bossert, Thomas P. 2017. 'It's official: North Korea is behind WannaCry.' *The Wall Street Journal* [online], 18 December. At https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 [Accessed on 24 April 2019].

Bull, Hedley. 2002. *A Sociedade Anárquica*. Brasília: Editora Universidade de Brasília.

Castells, Manuel. 2003. *A Galáxia Internet: Reflexões Sobre a Internet, Negócios e a Sociedade*. Rio de Janeiro: Zahar.

Carr, Edward H. 1981. *Vinte Anos de Crise: 1919–1939*. Brasília: Editora Universidade de Brasília.

Cepik, Marco, Diego Rafael Canabarro and Thiago Borne. 2014. 'A securitização do ciberespaço e o terrorismo: uma abordagem crítica.' In André de Mello Souza, Reginaldo Mattar Nasser and Rodrigo Fracalossi de Moraes (eds), *Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI*. Brasília: IPEA, pp. 161-186.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge: MIT Press.

Clausewitz, Carl Von. 1982. *On War*,Vol. 20. Transl. J Graham. London: Penguin.

Coelho Neto, Agripino Souza. 2013. 'Redes e Territórios (Networks and Territories).' *Mercator* 12 (28): 19-34.

Diniz, Eugenio. 2016. 'Breve ensaio sobre Estudos de Defesa como atividade científica.' *Revista Brasileira de Estudos de Defesa* 2 (2): 21-28.

Federal Ministry of the Interior [Germany]. 2011. *Cyber Security Strategy for Germany*. Berlin: Federal Ministry of the Interior.

Ferreira Neto, Walfredo Bento. 2018. 'Territorializando o "Novo" e (Re)territorializando os Tradicionais: a cibernética Como Espaço e Recurso de Poder.' *Revista Brasileira de Estudos Estratégicos* 4: 85-113.

Haesbaert, Rogério. 2002. *Territórios Alternativos*. São Paulo: Editora Contexto.

_____. 2004. *O Mito da Desterritorialização: do 'Fim dos Territórios' à Multiterritorialidade*. Rio de Janeiro: Bertrand Brasil.

_____. 2007. 'Território e multiterritorialidade: Um debate.' *GEOgraphia* 9 (17): 19-46.

Hildebrandt, Mireille. 2013. 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in Cyberspace.' *University of Toronto Law Journal* 63 (2): 196-224.

Hunker, Jeffrey, Bob Hutchinson and Jonathan Margulies. 2008. *Roles and Challenges for Sufficient Cyber-Attack Attribution*. Hanover: Dartmouth College, Institute for Information Infrastructure Protection.

Internetworldstats.com. 2019. *World Internet Users Statistics and 2019 World Population Stats*. At https://www.internetworldstats.com/stats.htm [Accessed on 15 August 2019].

Kallberg, Jan. 2016. *Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations*. West Point: Army Cyber Institute, West Point.

Kallberg, Jan and Thomas S Cook. 2017. 'The unfitness of traditional military thinking in cyber.' *IEEE Access* 5: 8126-8130. At https://ieeexplore.ieee.org/abstract/document/7896576 [Accessed on 5 September 2019].

Kant, Immanuel. 2018. *A Paz Perpétua e Outros Opúsculos*. Transl. Artur Morão. Lisbon: Leya.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Keohane, Robert O and Joseph S Nye Jr. 1987. 'Power and interdependence revisited.' *International Organization* 41 (4): 725-753.

Kremer, Jan-Frederik and Benedikt Müller (eds). 2013. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin and Heidelberg: Springer.

Krippendorff, Klaus. 2004. *Content Analysis: An Introduction to its Methodology*, 2nd Ed. Thousand Oaks: Sage Publications.

Kuehl, Daniel T. 2009. 'From cyberspace to cyberpower: Defining the problem.' In Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security*. Washington, DC: National Defense University Press.

Kuhn, Thomas S. 2018. *A Estrutura das Revoluções Científicas.* 13th Ed. São Paulo: Perspectiva.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: Rand Corporation.

Lobato, Luisa Cruz and Kai Michael Kenkel. 2015. 'Discourses of cyberspace securitization in Brazil and in the United States.' *Revista Brasileira de Política Internacional* 58 (2): 23-43.

Ministry of Defence [Brazil]. 2014. *Doutrina Militar de Defesa Cibernética – MD 31-M07*. At https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf [Accessed on 10 January 2018].

_____. 2016. *Defense White Paper.* At https://www.defesa.gov.br/arquivos/2017/mes03/livro-branco-de-defesa-nacional-consulta-publica-12122017.pdf [Accessed on 10 January 2018].

Morgenthau, Hans J. 2003. *A Política entre Nações*. Brasília: Universidade de Brasilia.

Nye Jr, Joseph S. 2012. *O Futuro do Poder*. São Paulo: Benvirá.

_____. 2010. *Cyber power*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Office of the Chairman of the Joint Chiefs of Staff [USA]. 2019. *DOD Dictionary of Military and Associated Terms*. [ebook] Washington, DC. At https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2019-08-06-101717-717 [Accessed on 15 August 2019].

Peterson, Andrea. 2014. The Sony Pictures hack, explained. *The Washington Post* [online], 18 December. At https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ [Accessed on 15 August 2019].

Onuf, Nicholas G. 1979. 'International legal order as an idea.' *American Journal of International Law* 73 (2): 244-266.

Raffestin, Claude. 1993. *Por uma Geografia do Poder*. Transl. Maria Cecília França. São Paulo: Editora Ática.

Rattray, Gregory J. 2009. 'An environmental approach to understanding cyberpower.' In Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security*. [online]. Washington, DC: National Defense University Press, pp. 253-274. At https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/ [Accessed on 19 August 2019].

Reardon, Robert and Nazli Choucri. 2012. 'The role of cyberspace in international relations: A view of the literature.' Paper prepared for the 2012 ISA Annual Convention San Diego, USA, 1 April.

Robertson, Jordan and Michael Riley. 2018. 'The Big Hack: How China used a tiny chip to infiltrate U.S. companies.' *Bloomberg.com,* 4 October. At https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies [Accessed on 19 August 2019].

Santos, Milton. 2002. *A Natureza do Espaço: Técnica e Tempo, Razão e Emoção* (Vol. 1). São Paulo: Edusp.

Schmidt, Brian C. 2012. 'On the history and historiography of International Relations.' In Walter Carlsnaes, Thomas Risse and Beth A Simmons (eds), *Handbook of International Relations*. London: SAGE Publications Ltd, pp. 3-22.

Shaheen, Salma. 2014. 'Offense–defense balance in cyber warfare.' In Jan-Frederik Kremer and Benedikt Müller (eds), *Cyberspace and International Relations.* Berlin and Heidelberg: Springer, pp. 77-93.

Sheldon, John B. 2011. 'Deciphering cyberpower: Strategic purpose in peace and war.' *Strategic Studies Quarterly* 5 (2): 95-112.

Souza, Marcelo J L de. 1995. 'O território: sobre espaço e poder, autonomia e desenvolvimento.' In Iná Elias de Castro, Paulo Cesar da Costa Gomes and Roberto Lobato Corrêa (eds), *Geografia: Conceitos e Temas*. 2nd Ed. Rio de Janeiro: Bertrand Brasil, pp. 77-116.

Stoppino, Mário. 2018. 'Violência.' In Bobbio, Norberto, Nicola Matteucci, Gianfranco Pasquino, Carmen C Varriale, João Ferreira and Luís Guerreiro Pinto Cacais (eds), *Dicionário de Política*. 11th Ed. Brasília: Editora Universidade de Brasília, pp. 1291-1298.

The Federal Government of Germany. 2016. *White Paper 2016: On German Security Policy and the Future of The Bundeswehr*. Berlin: Federal Ministry of Defence.

The State Council Information Office [China]. 2019. *China's National Defense in the New Era*. Beijing, China: Foreign Languages Press Co. Ltd. At http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc [Accessed on 5 August 2019].

The White House. 2017. *National Security Strategy of the United States of America*. Washington, DC.

Thompson, Mark and Jethro Mullen. 2017. 'Ransomware: Attack hits 150 countries, Europol says world is in "disaster recovery mode."' *CNNMoney* [online]. At https://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/ [Accessed on 5 August 2019].

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

Weaver, Nicholas. 2019. *The China SuperMicro Hack: About That Bloomberg Report*. Lawfare [online], 4 October. At https://www.lawfareblog.com/china-supermicro-hack-about-bloomberg-report [Accessed on 7 September 2019].

Wendt, Alexander. 1992. 'Anarchy is what states make of it: The social construction of power politics.' *International Organization* 46 (2): 391-425.

Wheeler, David A and Gregory N Larsen. 2003. *Techniques for Cyber Attack Attribution* (IDA Paper P-3792). Alexandria: Institute for Defense Analyses.

Wikileaks. 2019. *WikiLeaks – Vault 7: Projects*. Wikileaks.org [online]. At https://wikileaks.org/vault7/ [Accessed on 26 January 2019].

About the authors

Breno Pauli Medeiros is a Ph.D. student of the Military Science Postgraduate Program (PPGCM) of the Brazillian Army Command and General Staff College (ECEME). He holds a CAPES Scholarship and is member of the project 'Science, Technology and Innovation in Defense: Cybernetics and National Defense,' approved by Public Notice 27/2018, Support Program for Teaching and Scientific and Technological Research in National Defense – PRO-DEFENSE IV. He holds a Bachelor's degree in Geography from the Fluminense Federal University (UFF) and a Master's degree in military sciences from PPGCM, where he defended the dissertation 'Cyberspace and International Relations: Towards the Construction of a New Paradigm?' from which this article was adapted. He serves as assistant academic coordinator of the thematic area 'Cyber Defense' of the Military Observatory of Praia Vermelha (OMPV).

Luiz Rogério Franco Goldoni holds a Master's and Doctorate in Political Science from the Fluminense Federal University (UFF). He is Professor of the Postgraduate Program in Military Science (PPGCM) at the Brazillian Army Command and General Staff College (ECEME), teaching the following courses: 'Defense Logistics,' 'Management and Public Policy in Defense' and 'Cyber Defense.' He serves as academic coordinator of the Program's research field 'Defense Management: Public Policy, Economy and Industry' and is researcher on the project 'Science, Technology and Innovation in Defense: Cybernetics and National Defense,' supported by CNPq (Public Note 27/2018, Support Program for Teaching and Scientific and Technological Research in National Defense – PRO-DEFENSE IV). He is coordinator of the thematic area 'Cyber Defense' of the Praia Vermelha Military Observatory (OMPV).

A Trindade Conceitual Fundamental do Ciberespaço

Resumo: Este artigo baseia-se na premissa de que a crescente interação humana no ciberespaço eleva-a ao nível do domínio estratégico e, como tal, levanta desafios teóricos e práticos para as relações internacionais. Baseia-se em uma reflexão epistemológica sobre os pressupostos fundamentais dos paradigmas que permeiam as relações internacionais. O principal objetivo é conceituar o ciberespaço como domínio estratégico no século XXI, bem como desenvolver uma estrutura analítica que forneça evidências e investigue a resiliência dos fundamentos das atuais relações internacionais. Mais especificamente, os seguintes preceitos: i) soberania baseada na territorialidade, ii) monopólio estatal do poder e iii) responsabilização entre atores internacionais. Nesse sentido, a abordagem se refere à documentação de defesa e a fontes científicas, a fim de alcançar uma definição que caracterize o ciberespaço, considerando seus aspectos técnicos, científicos e estratégicos. Ao mesmo tempo, o trabalho bibliográfico sustenta o desenvolvimento da ferramenta analítica conhecida como Trindade conceitual fundamental do ciberespaço, com base nas características do domínio ciberespaço: i) desterritorialidade, ii) multiplicidade de atores e iii) incerteza.

Palavras-chave: ciberespaço; cibernética; território; prestação de contas; Relações Internacionais.

Received on 7 May 2019, and approved for publication on 6 January 2020.