Russia, BRICS and Cyber Power: Evoking Synergies under Conjectures of Deviation

Danielle Jacon Ayres Pinto[1]
Larlecianne Piccolli[2]
Riva Sobrado de Freitas[3]

Abstract

When one thinks about powerful and influential traditional actors of the International system, Russia cannot be ruled out of this select group. Despite the oscillations by which the State had been through in the post-Cold War period, the international community witnessed, since the beginning of the 21st century, the recovery of its *status quo* as an influential power among both the developed countries and, mainly, the developing countries, and the BRICS is perhaps the greatest expression of this rise. As the dynamics of power within the system become more flexible on the threshold of the 21st century, moving from a traditional range of military resources to covering new demands linked to new technologies, especially the internet, Russia seeks to use them as a resource of power. Thus, this paper aims to understand how cyber resources takes part of the Russian strategy to rebuild its power in the International System and how significant these resources are to the new understanding of the State capacity of the Russian Federation. It's then believed that cyber resources act as a profitable power tool for Russia's reentering the international arena. It is supported by the concept of "strategic deterrence" assumed in the country's Military Doctrine (2014), which sustains military (conventional and nuclear) and non-military tools (political, economic, scientific measures).

Keywords: Russia. Power. Cyber Resources.

Introduction

The end of the Cold War seems to be a much more significant timeframe for international politics than just the ending of the bipolarity between the United States of America (US) and the Union of Soviet Socialist Republics (USSR). This historic moment marked the construction of a new way of understanding the world reality from the social, political, economic and security points of view.

Throughout the 1990s, the world experienced an exponential improvement in its interactivity, but at the same time it moved towards a homogenization process that promised to be the solution to the inequalities so far faced worldwide. Thanks to globalization, every person

[1] Associate Professor at Federal University of Santa Catarina, UFSC – Brazil. Contact: djap2222@yahoo.com or danielleayres@gmail.com

[2] Ph.D. candidate in International Strategic Studies at Federal University of Rio Grande do Sul. Contact: larle@hotmail.com

[3] Associate Professor in Post-Graduation at University of Oeste de Santa Catarina – UNOESC. Contact: rivafreit@gmail.com

would be equal, with the same possibilities and challenges. As warned by Manuel Castell (2011), Boaventura de Sousa Santos (2010), Joseph Stiglitz (2003) and many others, this scenario did not happen. What in fact occurred was an increase in violence, inequality and the continuity of the political processes that preserved the promotion of benefits to the most powerful countries of the International System.

However, despite the fact that the globalization did not fulfill its promise, it would still bring to the system the rise of new actors who no longer needed to hide under the umbrella of the system's traditional powers. These actors emerged, prioritizing a new rhetoric of power and using new power resources to sustain it. Thus, in 1997, we witnessed the BRICS[4] (Brazil, Russia, India, China and South Africa) appear as the promise of a new power pole coming from the peripheral countries and bringing to the system a new way of interaction. Alongside the BRICS, society will see the growing influence and dependence that the advancement of digital technologies is bringing on people's daily lives. And, naturally, such resources will become a new important aspect to building the State’s power in the international sphere.

However, it is a fact that Russia, the central theme of this article, cannot effectively be considered as a new power pole. Its history and influence on the system are noticeable, yet the collapse of the USSR and its reorganization as the Russian Federation imposed a new way of interacting with the system, as well as a new perception of what space it intended to occupy in international politics. This new state perspective, as a Russian Federation, put that country as a kind of new power pole, being part of the select group of those States who have decision-making capacity in the International system. Russia also acts as a potential State, which reappears and regains its importance in the international arena by envisioning new strategic dimensions as the foundation of its external actions.

Before this scenario, the article proposes that we should think about how Russia, a central power in the bipolarity of the Cold War, rose in the 21st century to become an exponent of power. It should also be considered as to how cyber resources became a part of the new strategy of international insertion of that State. Our proposal is to analyze the recovery of Russia's *status quo* in the 21st century and how it is directly related to the BRICS and to new technologies as power resources. Based on the concept of “Strategic Deterrence”, adopted by

[4] It is an English acronym for Brazil, Russia, India, China and South Africa. It was first mentioned by the British economist Jim O'Neil in a 2001 study for Goldman Sachs called “Building Better Economic BRICs”. The British economist pointed that, regarding their economic development, those “BRICs” countries were qualified as emerging markets.

the 2014 Russian Military Doctrine, a preliminary guiding hypothesis can be assumed: by prioritizing conventional and unconventional military means to build its reinsertion into the system, Russia deems cyber technology as an important power resource, making use of it in the international power struggle throughout the 21st century.

Power: from the Cold War end to the 21st century

To think of power in international politics is usually to associate coercive actions and resources with a strategy that increasingly seeks to satisfy State demands within the international sphere. This rhetoric seemed to prevail in the international system throughout the 20th century, especially during the Cold War and its arms race context.

However, as argued by Byung Chul-Han (2019, p. 12) “the coercive model does not live up to the complexity of power. Power as coercion consists in imposing one's own decisions *against* the will of the other”. With the end of bipolar cleavage, the coercive rhetoric is losing ground, mainly because there is no longer *the other*, the enemy, once the world is now intertwined in a single globalized society.

This is the context that led Joseph Nye to introduce his perception of *soft power* in the 1990s debate on international politics and power. This concept does not imply to coerce the counterpart but to convince it, through cultural resources, political values, and foreign policy actions, (Nye, 2004) that it benefits from following the preference of the State that exerts power–and it certainly could be the case, but it is, in fact, not guaranteed.

Thus, Nye translates soft power as follows:

> A country may obtain the outcomes it wants in world politics because other countries-admiring its values, emulating its example, aspiring to its level of prosperity and openness-want to follow it. […] This soft power – getting others to want the outcomes that you want – co-opts people rather than coerces them. (Nye, 2004: 5).

In sum, example and identity gain more importance than the effective ability to coerce and compel others to do something that a powerful state wants. In a connected and borderless world, as proposed by globalization, where there is no *other* but in fact an integration, the logic of power changes. New cyber technologies, especially the internet, emerged in this perspective as a means of bringing people and countries closer together. The resource that was born to be military spread out to civil society in the post-Cold War period and now determines the way in which society develops and communicates, thus becoming an essential resource for human life (Ayres Pinto; Pagliari, 2019; Kuehl, 2009; Flournay; Sulmeyer, 2018).

Nevertheless, another historic event would change this perception of power that arose in the 1990s: the September 11 attack on the World Trade Center in New York. This attack undermined the perception of the non-existence of the *other*, showing that instead of Western values and culture being praised, they were actually devalued and attacked due to constant attempts by the US to control other States and utilise warlike behavior against these aforementioned States in the 1990s.

The American response to the September 11 attack was a return to a coercive, threatening, will-imposing, and invading country model of power, using violence as a *modus operandi*. However, the world no longer effectively bears this kind of bellicose interaction because of the increasing costs of coercion, both from an economic point of view and, mainly, from the relational point of view. The effective interdependence of the system actors made coercive actions increasingly objectionable and thus unhelpful in meeting the demands of the actors. An example of this is the US military action in Afghanistan and Iraq post 2001 and the high political and economic costs imposed to the Americans without the expected earning—the elimination of those it considered its enemies.

Faced with this scenario, a dilemma emerges: the traditional resources of power cannot be abandoned, meanwhile, on the basis of coercive logic, as they no longer make the same effect as they would have done previously. At this point, Joseph Nye (2011) would sharpen his understanding of power in the 21st century by providing his perception on the concept of *smart power*[5]. The first idea is to dispel the misperception that *smart power* is an improved *soft power*. According to Nye (2011: XIV) "Smart Power is not simply 'soft power 2.0'".

For the author, this new perception involves more than power resources—it concretely includes an effective capacity to mold an international insertion strategy that understands the dynamics of interdependence in the system. In this sense, the author affirms that:

> A smart power narrative for the twenty-first century is not about maximizing power or preserving hegemony. It is about finding ways to combine resources into successful strategies in the new context of power diffusion and 'rise of rest' (Nye, 2011: 207-208).

For Nye (2011) there are two new post-September 11 dynamics in the system: a transition of power (new state actors are achieving more influence) and a diffusion of power

[5] The concept of smart power was coined by the lawyer and international analyst Suzzane Nossel in a 2004 for Foreign Affairs article. The researcher defines this concept as follows: "Smart power means knowing that the United States' own hand is not always its best tool: U.S. interests are furthered by enlisting others on behalf of U.S. goals, through alliances, international institutions, careful diplomacy, and the power of ideals" (NOSSEL, 2004, p.138). But this will be an analysis exclusively focused on the USA, and Nye's perception will have a broader dimension.

(new *non*-state actors are earning the ability to exercise power). This trend is directly linked to new technological resources and their lower costs.

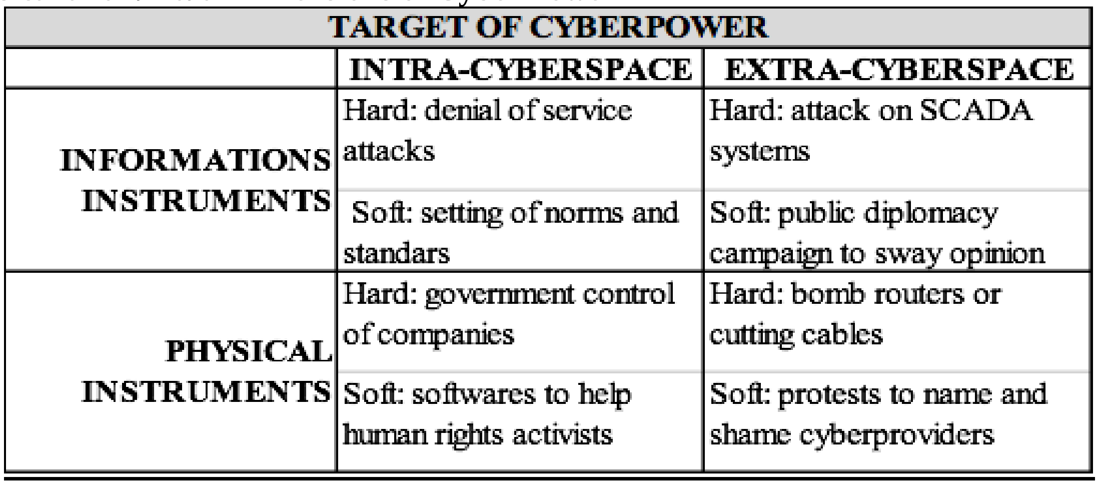
In this context of transition and diffusion of power, cyber resources become essential, as stated by Richard Haass:

> The principal characteristic of twenty-first-century international relations is turning out to be nonpolarity: a world dominated not by one or two or even several states but rather by dozens of actors possessing and exercising various kinds of power. This represents a tectonic shift from the past. [...] the proliferation of information is as much a cause of nonpolarity as is the proliferation of weaponry (Haass, 2008: N/A).

Hence, cyber power becomes an effective resource for the new system dynamics, and its concept can be defined as the "ability to use cyberspace to create advantages and influence events in others operational environments and across the instruments of power" (Nye, 2010: 4). The logic of power does not change; what differs is the consideration of technological resources as means for the exercise of power, both in the virtual world as well as in the non-virtual world. Therefore, the States that possess such resources need to understand how to use them and also the role they play in the strategy of insertion into the international system. As was mentioned before, considering its official documents, the Russian Federation seems to have understood the importance of defining such precepts for its own insertion strategy.

However, within a more explanatory approach, it is important to observe the table established by Joseph Nye to determine cyber power resources:

Physical and Virtual Dimensions of Cyber Power



TARGET OF CYBERPOWER		
	INTRA-CYBERSPACE	EXTRA-CYBERSPACE
INFORMATIONS INSTRUMENTS	Hard: denial of service attacks	Hard: attack on SCADA systems
	Soft: setting of norms and standars	Soft: public diplomacy campaign to sway opinion
PHYSICAL INSTRUMENTS	Hard: government control of companies	Hard: bomb routers or cutting cables
	Soft: softwares to help human rights activists	Soft: protests to name and shame cyberproviders

Source: Nye, 2010: 5.

In this sense, it is reasonable to realize that not only the control and dissemination of information but also the use of cyber systems to damage critical infrastructures (which are extra-cyberspace) are possible actions in this new logic of power in the 21st century.

Accordingly, those that are determined by States as *cyber* resources (or as composing resources of this sphere of action) can be used in an insertion strategy not only as coercive means but also in a logic of co-optation. What seems to be decisive for the course of action is the actual political, economic and security costs involved and how states can afford them.

Bearing in mind the above theoretical framework, next we will proceed with analyzing how Russia, through its strategic documents—especially its 2014 Military Doctrine—defines the use of these cyber resources and also what role the BRICS play in this Russian strategy.

Russia and the new power resource: cyber power enters the country doctrinal conceptions

Analyzing Russia's strategic positioning in the 21st century international system inevitably entails understanding–even briefly–the unfolding systemic chaos that plagued the country in the 1990s. As aforementioned, in a context of redefinition and rearrangements of power in the international system, the political-economic system and the Russian social fabric deteriorated, weakening the country's position in the new established order. The State reorganization experienced since the year 2000 indicates a reinsertion in the international system. Such a process benefited, on the one hand, from the maintenance of its great power status (based on its strategic nuclear military capabilities) and, on the other, by the new power dynamics that emerged in the post-Cold War period.

The decline and subsequent dissolution of the USSR was caused by a combination of political, economic and military factors exacerbated by Gorbachev's reformist policies (Perestroika and Glasnost) and nationalist mobilizations in the Soviet republics. The Belavezha Accords marked the end of the USSR, the Cold War and the bipolarity of the international system. A period of transition began and it was initially characterized by the US hegemony in the scenario of a globalized capitalist world where Russian insertion took place in a nefarious way.

The 1990s was a disastrous and traumatic period in Russia. Economic decline plagued the country with GDP falling by almost half in the early years.

On the political sphere, the “democratic” government of President Yeltsin has gradually presented itself as a failed and controlling administration, conducting absurd episodes such as the bombing of the Duma (Parliament) to dislodge political opponents. The country's erratic privatization process has promoted the formation of groups of billionaires who squandered national heritage while the population drowned in poverty. The Russian society witnessed a major decline in the size of the population, as well as in the life expectancy of the population.

Further issues were seen due to high unemployment rates, uncontrolled growth in the number of mafias, crime, violence and conflict–the last ones being demonstrated by both Chechen Wars in 1994 and 1999 (Visentini, 2017).

In short, what was seen in the 1990s in Russia was a breakdown of the State and a lack of administrative capacity generated an internal systemic chaos that was soon reflected in the external position of the country. In this regard, a wholly Western-oriented foreign policy kept relations with the United States as a priority in the hope that rapprochement with Western institutions would provide the necessary support for the resumption of economic growth and political stabilization. It was not long before Moscow showed its discontent with the contradictory Western aid unveiled in invasive policies consolidated in the Kosovo military onslaught and in the NATO expansion process.

The new millennium renews the framework of competition through the resurgence of centrifugal forces that, on the one hand, remove the predominance of power from the unipolar core and, on the other, reshape the conceptual core of power by encompassing new tools for its execution in the international arena. Thus, after a period of predominance of unipolar configuration of the international order, we are in the process of consolidating a restructured international system which is now multipolar. Among the new poles of power, Russia reappears in a position of political, military and economic importance, thereby safeguarding its interests in this new configuration of the system (Piccolli, 2012; Piccolli, Dall'Agnol, Pereira, 2018).

Thus, after the turmoil of the 1990s, Moscow began to rebuild its political unity and reestablish itself in economic terms which allowed the country to orient a project for its reinsertion in the international system. The governments of Vladimir Putin and Dmitri Medvedev were able to manage the political stability (achieved through a process of state centralization and strengthening of executive power) and economic growth (driven by hydrocarbon exports), which were fundamental to achieving their goals in the face of the new world order. Likewise, the governments were mindful of the changes in the capacity building of States, expanding its range of tools to a niche beyond traditional capabilities. For that matter, it started to consider the role of cyber resources as a source of power in the international arena.

In the course of the 2000s, the construction of cyber power resources is noticeably concurrent with the development of the country's security strategy documents which, after all, are a reflection of the evolution of the risks and threats arising from the external realm–and of Moscow's stance towards these. It follows that the doctrinal meaning of the term "strategic deterrence" consolidates Moscow's assimilation of the reality of an international system whose security dynamics encompass a diverse range of capabilities, including cyber power.

The recent versions of the country strategy papers, Military Doctrine (2014), National Security Strategy (2015), Foreign Policy Concept, and Information Security Doctrine (2016), generally signal Moscow's perception of a security environment characterized by:

> increasing global competition, the tension in the various areas interstate and interregional interaction, values and rivalry development patterns and processes of economic instability political developments at the global and regional levels background of the complications of international relations.[…], unresolved […] conflicts [to which there] is a tendency to force their resolution, in including in the regions bordering on the Russian Federation. [...] (Russia, 2014, §9, §10).

For Moscow the existing "architecture [of] international security does not provide equal security for all States" (Russia, 2014, §10). In sum, its evolved in a tendency toward a scenario of complication of international relations

Moscow still points to the West's inability to govern world politics and the economy (Russia, 2016, §4). The papers argue that attempts to impose Western values (as a result of the globalization process of the 1990s) as a means of democratization and growth for other countries, as well as an attempt to contain the emergence of alternative power centers, incite the instability of international systems, impacting on numerous regional conflicts. In other words, Russia points out that the current security instability is a product of the Western, and more specifically the United States', unwillingness to share its dominant role in the system– which means not accepting the already settled polycentric/multipolar reality. In this sense, Moscow is well aware of the role played by the use of cyber resources in government destabilization processes when it points out that, while the use of technological resources contributes to the economic development and better functioning of state institutions, they embody a range of new threats.

> The possibilities of transboundary information circulation are increasingly used for geopolitical goals, goals of a military-political nature contravening international law or for terrorist, extremist, criminal and other unlawful ends detrimental for international security and strategic stability [...] [A] number of foreign countries are building up their information technology capacities to influence the information infrastructure in pursuing military purposes (Russia, 2016, 10-11).

From this finding, Moscow assumes that the use of cyber power in the sphere of national security is characterized for the: growing use by certain States and organizations of information technologies for military and political purposes, including for actions inconsistent with international law and seek to undermine the sovereignty, political and social stability and territorial integrity of the Russian Federation and its allies, and pose a threat to international peace, global and regional security (Russia, 2016, §15).

The argument above, brought by the Russian Information Security Doctrine, verbalizes the propositions encompassed by the other strategic documents of the country regarding the political destabilization movements in the surroundings of the Russian territory. Moscow explains that such movements, like the Color Revolutions, make direct use of communication and information technologies for military purposes, acting against the sovereignty, political independence and territorial integrity of States (Russia, 2014, §12, 1- n. 13). The documents, albeit indirectly, allude to the similarity between the Color Revolutions and the Ukrainian Crisis, but mainly to the possibility of such movements spreading to the Russian domestic sphere. For the Russians, these movements are the basis of contemporary military conflicts which use indirect and asymmetrical operations, such as the use of political forces and public associations with external funding.

For this purpose, the State must be prepared to deal with these new threats through non-military channels, meanwhile it must also secure its traditional military means, considering the chances of escalating conflicts and real threats to State integrity and sovereignty. In this respect, they reserve themselves the right to incur in military means to deter non-military actions and/or conventional military aggression that threats Russian security, whether occurred in its territory or in the territory of allies, endangering the very existence of the State. In the same document, they postulate the right to use nuclear weapons in response to a nuclear or even non-nuclear attack of mass destruction against themselves and/or their allies (Russia, 2000, §8; Russia 2010, §22; Russia, 2014, §27). This is the logic behind the doctrinal meaning of "strategic deterrence" postulated in the Military Doctrine (2014): to have an effective link between military and non-military capabilities for the defense of the country. The concept is elucidated as:

> a coordinated system of military and non-military measures carried out consecutively or simultaneously for the purpose of deterring military action by the opposing State (or coalition of States) involving strategic damage to the other party […]. Strategic Deterrence is aimed at stablishing a political-military situation [...] in order to influence an adversary within a predetermined framework or to de-escalate the military conflict […] Strategic deterrence measures are carried out continuously in both peacetime and conflict. [...] Non-military measures include actions in several spheres, such as political, diplomatic, legal, economic, ideological, scientific and technical. [...] Military measures include: intelligence and information actions; demonstration of military presence and military strength; actions to ensure the safety of State economic activity; peacekeeping operations; air defense; protection and defense of the State border in air, sea and land

> space; [...]; to make (or threaten to) precise (including nuclear) attacks (MD, 2019: online).

There can be seen to be a linearity of strategic documents regarding the defensive character of the Russian actions in the system, either through the use of traditional military capabilities (conventional and nuclear weapons) or through the use of new power resources and tools, such as cyber capabilities. Regarding the latter, it must be made clear that there are significant differences in Russian and Western approaches to cyber power which makes understanding between the parties very difficult. As an example, it can be mentioned the controlling of the flow of information in cyber networks. For Russians, the circulation of information perceived as threats to society, strategic interests and state sovereignty is dealt as a security issue, with the government having the power to limit such threats. This is a reality that does not happen in the West, where the free circulation of information through networks prevails (Giles, 2012). Giles also make aware of the fact that Russia's vision of “information warfare” is not restricted to the circulation of information, having a far “more holistic concept than its literal translation suggests, carrying cyber operations implicitly within it alongside disciplines such as electronic warfare (EW), psychological operations (PsyOps), strategic communications and Influence” (Giles, 2012, p. 74).

Since the collapse of the USSR and the restructuring of Russian capabilities, the use of cyber power resources has gone through a process of consolidation in the doctrines that embody Russia's strategic positioning. Some alleged Russian military action in the Georgian conflict (2008) have characteristics that give evidence of the use of cyber resources in the conduct of the conflict. It was also considered as a rehearsal for a more intense conflict with the West. David Hollis (2011) points out that Russian military actions were combined across four dimensions: air, land, sea and cyberspace. The Russian Forces were actually accused by the Georgian government of assaulting more than fifty-four websites in the neighboring country (linked to communication, finance and even government websites). The alleged actions by Moscow were aimed at hampering communications and limiting the decision-making process in Georgia. Hollis (2011) states that the Russian strategy was not intended to attack critical infrastructures but rather to hold sufficient capacity to enable them to do so.

From the lessons learned from the alleged Russian actions, it should be noted that the lack of mastery of cyberspace has altered Georgia's ability to conduct communication strategies at the national level. In turn, the Russian capabilities allowed an integration between the different dimensions of the Armed Forces, with the cyber power and the outer space command capabilities being essential in this case, serving for inter-force communications and also as a destabilizing tool of enemy forces in the conflict.

In summary, there can be notice that Moscow is aware of the importance of using cyber resources to secure their status in the international political arena. To this end, it uses a defensive rhetoric, characteristic of its international strategic insertion design.

BRICS and Cyber Resources: An Alternative Power Scenario for Russia?

As presented above, 21st century Russia clearly understands two important issues regarding its dynamics in the international system: (1) that it is a relevant actor and will regain its power *status quo* on the international stage; (2) that non-military (or non-traditionally military) resources, such as cybernetics, are central to this Russian ambition.

However, it can be seen that, when Russia thinks about its international insertion processes, it has an effectively independent method of strategic planning, bringing to themselves the demands of such insertion. So, in this perspective, where would be the BRICS' place, especially when we talk about cyber power?

The BRICS appear as an effective zone of importance in the late twentieth century, when the foundation of this importance was directly related to the capacities of economic growth and development (Davydov, 2018; Abdenur, 2017) that those countries seemed to possess in the opinion of Goldman & Sachs analysts.

In this perspective, the BRICS engaged in dynamics of confrontation with the hegemonic power that the USA had in the international system. The proposal was not to confront and replace this *hegemon*, but rather to create alternative power spaces where developing and poorer countries saw the possibility of gains in the BRICS. At the same time, increasing the relative power of the countries can be considered to be part of this acronym.

But the relationship was strictly based on an economic and cooperative dynamic in international organizations, in order to face insertion challenges together. In the dynamics of power resources and international security challenges, their joint action did not unfold as being effective. Their interaction in this area appeared at official meetings held by the BRICS. Yet the focus was always on a more generalist debate which privileged a perception of how to understand security issues and weigh them on the international agenda, rather than actually creating an alliance between countries to promote a cooperative security process. Topics such as cybercrime, terrorism and others were dealt with at conferences such as Fortaleza in 2015, but they were nothing more than debates about conjunctures, not effectively turning into joint actions (Abdenur, 2017).

On the other hand, when we think of Russia, China and cyber power, what we see is a battle in international space for the control of two distinct action dynamics over this new security dimension. The first one is the USA and Europe seeking to determine how cyberspace will work. The second dimension is Russia and China trying to show themselves as exponents in this space, bringing new understandings and technologies, thus emerging as effective cyber power poles (Forsyth, 2013).

In this sense, when thinking of Russia, BRICS and cyber power, it is not possible to see an effective collaboration of these actors in order to create a cohesive group that determines and conducts cyber-dimension security actions.

What we see is Russia being effectively centered on becoming a power pole in a multipolar system and using the cheapest, and least physically destructive, cyber resources to support its strategy. The BRICS in this dynamic appear more as a possible area of influence than effective cooperative partners (Davydov, 2018).

Final Remarks

In this brief essay, we sought to clarify the transition from traditional military capabilities to a wider range of resources, such as the Internet, and how Russia is adapting to the use of such capabilities as a power resource in the international arena. Therefore, from the analysis of the Russian military doctrine documents, the evolution of cyber power was considered as a mechanism for rebuilding its power in the international system of the new millennium, serving as a useful tool for Moscow.

It is believed that, if at first Moscow would use available *soft power* resources for a multifaceted insertion, when restructuring its State capacity it has employed those we assume here as the precepts of *smart power* to counter external offensives on its surroundings and also to assume its position of power in a new multipolar world order.

However, this strategy turns to a Russian international insertion that privileges its independence in the international system. Hence, the BRICS in this scenario is much more a space for the exercise of Russian power than for effective cooperation in cyber security. However, given the volatility of the international system, caution is needed in the analysis so definitive conclusions on the topic are left open. Likewise, from this first essay arises a vast agenda of topics to be researched in the scope of the proposed theme, postulating continuity to the work developed.

References

Abdenur A.E. 2017. "Can the BRICS Cooperate in International Security?" *International Organisations Research Journal*. 12(3): 73–93.

Ayres Pinto, Danielle Jacon; Pagliari, Graciela de Conti. 2019. "The Innovation of Power: The Cyberdefense as an Opportunity to Construct State Capacity in the International Arena". *Annuals of ISA International Convention Toronto*. Available at http://web.isanet.org/Web/Conferences/Toronto%202019-s/Archive/81ad4c59-8825-4fad-9ba3-61d8d2593ecd.pdf . [Accessed on September 30, 2019]

Castell, Manuel. 1999. *A era da informação: economia, sociedade e cultura. A sociedade em Rede*. Volume 1. São Paulo: Editora Paz e Terra

Daydov, Vladimir. 2018. *Latinoamérica y Rusia – Rutas para la cooperación y el desarollo*. Buenos Aires: Clasco.

Flournay, M.; Sulmeyer, M. 2018. "Battlefield Internet – a Plan for securing Cyberspace". *Foreign Affairs*. 97(5): 40-46.

Forsyth (Jr.), James Wood. 2013. "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace*". Strategic Studies Quartely*. 7(1): 93-113.

Giles, Keir. 2012. "Russia and Cyber Security." *Nação e Defesa*. 133: 69-89.

Han, Byung-Chul. 2019. *O que é poder?* Petrópolis: Editora Vozes.

Hass, R. 2008. "The age of no polarity. Foreign Affairs." 87(3): maio-junho, 47.

Hollis, David. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal.* Available at https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf . [Accessed on September 30, 2019].

Kuehl, Dan. 2009. "From Cyberspace to Cyberpower: Defining the Problem". In Kramer, Franklin; Starr, Stuart; Wentz, Larry. *Cyberpower and National Security*. Washington: National Defense University Press.

Nye (Jr.), J. S. 2004. *Soft Power: The means to success in World Politics*. New York: Public Affairs.

Nye (Jr.), J. S. 2010. *Cyber Power*. Cambridge: Belfer Center for Science and International Relations.

Nye (Jr.), J. S. 2011. *The future of Power*. Nova Iorque: Public Affairs.

Piccolli, Larlecianne, Augusto César Dall'Agnol, and Tito Barcellos Pereira. 2018. "Documentos de Política Externa e de Segurança da Federação Russa após 2014: principais mudanças e implicações." *Mural Internacional.* Vol.9 (1): 69-83.

Piccolli, Larlecianne. 2012. “Europa enquanto condicionante da política externa e de segurança da Rússia: o papel da defesa antimíssil”. *Dissertação* (Mestrado em Estudos Estratégicos Internacionais) - Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre.

Russia. 2010. *The Military Doctrine of the Russian Federation*. February 20. Available at: http://www.sras.org/military_doctrine_russian_federation_2010. [Accessed on September 26, 2019]

Russia. 2014. *The Military Doctrine of the Russian Federation*. December, 25. Available at: https://rusemb.org.uk/press/2029. [Accessed on September 26, 2019]

Russia. 2015. “Russian National Security Strategy”. Available at:
http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf . [Accessed on September 26, 2019]

Russia. 2016. *Doctrine of Information Security of the Russian Federation.* December 5. Available at http://www.scrf.gov.ru/security/information/DIB_engl/ [Accessed on September 26, 2019]

Russia. 2016. *Foreign Policy Concept of the Russian Federation*. November 30. Available at http://www.mid.ru/foreign_policy/official_documents [Accessed on September 26, 2019]

Sousa Santos, Boaventura. 2010. *Reconhecer para libertar: caminhos do cosmopolitismo multicultura*. Rio de Janeiro: Editora Civilização Brasileira.

Stiglitz, Joseph E. 2003. *A Globalização e seus malefícios*. São Paulo: Editora Futura.
Visentini, Paulo. 2017. *Os Paradoxos da Revolução Russa - Ascensão e queda do socialismo soviético (1917-1991)*. Rio de Janeiro: Alta Books.