

# The Grand Strategy: changes in ways and means due to Information Operations and the threat to the interests of Brazil and Argentina

*La Gran Estrategia: cambios de formas y medios por las Operaciones de Información y la amenaza a los intereses de Brasil y Argentina*

**Abstract:** The objective of this work is the analysis of the Grand Strategy of the States by the capacity of Information Operations. Initially, the analysis focuses on the traditional role of ways, means, and ends with military power in the constant interaction between States, the threat to its existence. In a second moment, the changes in the ways and means of transnational threats and the global commons will be detailed, under the effect of globalized technology and concepts vulnerable to the gray zone and the narrative. In a third point of analysis are the ways and means of the grand strategy of the main world states in multidomain and influence, which implies an extensive use of Information Operations in a great competition. Finally, the conclusions point out that the maintenance of the national interests of countries such as Brazil and Argentina require the adaptation of multi-domain military strategic doctrine with extensive use of Information Operations as the basis of its grand strategy.

**Keywords:** grand strategy; information operations; global commons; multidomain; transnational threats.

**Resumen:** El objetivo de este trabajo es el análisis de la Gran Estrategia de los Estados por la capacidad de Operaciones de Información. Inicialmente, el análisis se centra en el papel tradicional de los modos, medios y fines con el poder militar en la interacción constante entre los Estados, la amenaza a la existencia del mismo. En un segundo momento, se detallarán los cambios en los modos y medios de las amenazas transnacionales y los *global commons*, bajo el efecto de la tecnología globalizada y conceptos vulnerables a la zona gris y la narrativa. En un tercer punto de análisis se encuentran los modos y medios de la gran estrategia de los principales estados mundiales en multidominio e influencia, que implica un uso extensivo de las Operaciones de Información en una gran competencia. Finalmente, las conclusiones apuntan que el mantenimiento de los intereses nacionales de países como Brasil y Argentina requiere la adecuación doctrinaria estratégica militar multidominio con amplio uso de las Operaciones de Información como base de su gran estrategia.

**Palabras Clave:** gran estrategia; operaciones de información; global commons; multidominio; amenazas transnacionales.

**Márcio Saldanha Walker** 

Exército Brasileiro. Ministério da Defesa.  
Brasília, DF, Brasil.  
walker22ms@yahoo.com.br

**Horacio Sánchez Mariño** 

Ministério de Defesa. Escola Superior de  
Guerra Conjunta das Forças Armadas.  
Buenos Aires, Capital Federal, Argentina.  
hsanchezmarino@esgcfaa.edu.ar

**Received: Sept 7<sup>th</sup>, 2022**

**Approved: Apr 14<sup>th</sup>, 2023**

COLEÇÃO MEIRA MATTOS

ISSN on-line 2316-4891 / ISSN print 2316-4833

<http://ebrevistas.eb.mil.br/index.php/RMM/index>



## 1 INTRODUCTION

National security issues may not have a worldwide consensus of the anarchic organization of states, but the threats exist. The grand strategy of states links explicit values to ends, ways, and means. However, the solutions are not clear, and the Information Operations capability is presented as part of a military grand strategy to deal with the new phenomena of realistic multidomain warfare. Brazil and Argentina are geopolitically the largest countries in South America, but this does not represent a defense potential, as the technological advancement of information capabilities challenges defense capabilities in relation to the interests of world powers.

The contemporary study of grand strategy includes debates about its definition. The grand strategy can be understood as part of foreign policy, while others believe that it covers foreign policy, military doctrine, and tactics. The conventional assumption is that grand strategy links explicit values of ways and means. However, there is a lack of consensus on the meaning, as it allows to incorporate economic and institutional dimensions into the ends or to extend the analysis to non-traditional threats, such as climate change, pandemics, and economic security (BALZACQ; DOMBROWSKI; REICH, 2019).

In general, the analysis of a country's traditional grand strategy is twofold in ways, the first being a national and global security approach, focused exclusively on military force, relationships, and threats. In a second view, it has a conception of strategy that distinguishes between foreign and defense policy, and does not fully cover diplomatic, economic, social, and cultural issues (MILANI; NERY, 2019).

However, the realistic organization of the armed forces, directed at state threats and ends, is constantly threatened by the changing course of transnational events. The essence of traditional military power is challenged by new actors who merged the media with the population and transcended state borders. Technological advances and new domains of warfare created an information fog in the face of state actors such as the United States, United Kingdom, Russia, and China with new strategic multidomain tools and non-state actors with new information threat techniques.

The strategic scenario of Brazil and Argentina, regional geopolitical actors in the South Atlantic continent, shows that the ways of threat are more complex than the previous ones, as they will have to face threats of a subtle, multipolar, and undefined nature in terms of information and influence. Threats can be both state and transnational, physical or not, as a phenomenon with gaps and common interests. In this scenario, world powers have updated their defense policies by other means and included concepts related to the military power of information. The military power of regional states is challenged to actualize the multidomain force competition interaction between states. So how is the traditional grand strategy of ends affected by the changing ways and means of multidomain information?

The following will analyze how traditional state interests may be challenged by the universe of multidomain military competition in a grand strategy of Information Operations that may affect the interests of Brazil and Argentina.

## 2 THE REALISTIC DEFENSE AND THE ENDS OF MILITARY POWER

The philosophical origin of the geopolitical military power of a state lies in its own realist identity of ends. “State is a human community which, within a given territory (the ‘territory’ is a distinctive element), claims (successfully) for itself the monopoly of legitimate physical violence” (WEBER, 1967, p. 83; our translation). Realist theories of international relations underlie the existence of states and the permanent game of competition for space and power.

From a geopolitical realist perspective, the projection of power factors (military, economic, political, psychosocial) is conceived so that all interaction between actors in the world geopolitical system is subject to a game of power interests, and that their action tends at least to maintain or improve their relative position on the world board to the expense of other actors.

According to Hobbes, the essence of the State consists of: “an entity whose acts unite a large crowd, by mutual covenants, made among themselves, is instituted by each as the author, for the purpose of using the strength and means of all, as it may judge proper, to secure the common peace and defense” (2005, p. 141; our translation).

For the geopolitical realism of the ends, the referent object of security will be the territorial integrity of the State, since it is the State that can, on the basis of its position in the system, preserve the interests of the nation and with them the welfare of society. The central objective of a State’s security policy must be to have all the indispensable means and resources necessary to preserve the interests of the nation, in order to maintain the integrity of the State’s priority interests and to free them from threats (MØLLER, 1996).

Each State organizes in ways its coercive power to guarantee the internal order of its institutions and to maintain its *status quo* in relation to the influence of other States, its defense. In the rationalist approach, States are the actors who hold power and seek means to realize their material and concrete interests in the face of an anarchic international environment, with the power aspects aimed at guaranteeing their *status quo ante bellum* (MORGENTHAU, 2003). Thus, the defense of the State has always been related to the existence of a military power that sustains it.

The construction of the political order of states, internal or external, can be known by the characteristics of some authors who defined it, such as Hobbes in the absolute state, Locke with parliamentary monarchy, Montesquieu with the limited state, Rousseau with democracy, Hegel with constitutional monarchy (BOBBIO, 1996). In all situations the state has its essence in the constitution of military power, even in democracy, “in the general sense of power and the possibility of imposing one’s own will on the behavior of others, domination can take the most diverse forms” (WEBER, 1964, p. 696). This is because the State’s interest predominates, in terms of its survival as a sovereign State.

In the context of sovereignty, the ways of the formation of the absolute State are achieved through a double process of concentration and centralization of power over a given territory. Concentration means the power to make laws, jurisdictional power, the power to use internal and external force, and the power to impose taxes. Centralization refers to the process of elimination or disallowance of lower legal systems, such as cities, corporations, private companies, which survive due to the tolerance of the central power (BOBBIO, 1996).

However, the nature of the state is to survive in a competitive world and sovereign power can be threatened by other means on the multidominant scale of military power. The use of power, with ways and means to guarantee sovereignty or interfere with that of other states, can be classified by the definition of geopolitician Bernard Cohen (2015): great power, first order states with the capabilities and ambitions to expand their influence beyond the regions in which they are situated (United States, Russia, China, Germany, and Japan); regional power, second order states in competition and their geopolitical reach is regionally confined (France, United Kingdom, India, Brazil, Iran, Turkey, and Australia); third order states, they have only a single type of capability to influence their neighbors (Ukraine, North Korea, Colombia, Chile, and Argentina); the other states are in fourth or fifth order.

Because of the essence of states and the nature of international relations driven by ends, conflicts of state interests will continue to trouble the international scene. The realist view is that any attempt to guarantee a system of collective security in the world, with the annulment of military power, is destined to fail because of the impossibility of freezing the *status quo* in a competitive international system between states (MORGENTHAU, 2003). From a realist perspective, the projection of power factors will be increasingly characterized by a multidomain performance of military power. The projection of power factors (military, economic, political, psychosocial) is seen in its integrity, but mainly realistic. Any interaction between the actors of the global geopolitical system is subject to a game of interests of the powers because it is understood as the power to dictate laws, the jurisdictional power, the power to use force inside and outside.

Given the above, the realist school of defense remains important in the current strategic context of Brazil and Argentina and the military power of the States that considered great power as the axis of action of international actors. However, can the realist vision, sovereign boundaries, people's security, and military aspects keep up with the changing ways and means of information and transnational multidomain scenarios?

### **3 THE TRANSNATIONALIZATION OF THE WAYS AND MEANS OF THREATS**

Since September 11, 2001, the geopolitical status of threats to states is uncertain. New phenomena such as globalization and the transnationalization of the means are threatening the boundaries beyond absolute states. As for the ways, the traditional strategy needs to be replaced by a grand strategy that demands the participation of different actors in different areas of the power structure in the formulation of these state policies. According to Buzan (1991), threats are not only military, but also political, economic, environmental, and social, which may determine a holistic approach to threats, beyond the traditional concept of military defense of the State.

According to Nina Silove (2018), there is a general tendency to use the term grand strategy inconsistently. She identifies three uses of grand strategy which she calls grand plans (a deliberate and intentional plan of action), grand principles (conceptual coordinates), and grand behaviors (an established pattern of behavior or practice). Silove's formulation is significant to the purpose of the ways in highlighting the relationship between the articulated ends of a state,

its strategic planning and its behavior in attempting to implement the grand strategy. Thus, the change in transnational social behavior caused by information via means may affect the traditional form of grand strategy.

Liang and Xiangsui (1999, p. 130) already said that there is a war by other means combined with threats beyond state boundaries, which will assemble and mix with each other more means to solve a problem in a wider range than the problem itself. For realists, when national security is threatened, the response is not simply a matter of selecting military means. However, today, considering the issues of information warfare, the meaning of the word “country” in terms of nationality or geography is no more than a small or large link in human society.

Countries are increasingly affected by regional or global organizations, such as the European Union, ASEAN, OPEC [...] and the largest of all, the United Nations. In addition to these, a large number of multinational organizations and non-state organizations of all shapes and sizes, such as multinational corporations, trade associations, peace and environmental organizations, the Olympic Committee, religious organizations, terrorist organizations, small hacker groups, etc., are present in the countries. These multinational, non-state and supranational organizations form a global power system that is emerging. (LIANG; XIANGSUI, 1999, p. 130; our translation)

The crises that will arise in future scenarios will be more complex than previous ones, as threats will have to be confronted by other ways and means of a subtle, multipolar, and undefined nature, without the need to categorize a nation’s state of war or peace (VERGARA; TRAMA, 2017). This phenomenon of conflict that is neither war nor peace was defined as a gray zone where it is not easy to distinguish between who, what or how states relate to each other. The distinction between security and defense has become blurred. As Cha points out “globalization creates an interpenetration of international and domestic affairs [...] this ‘inter-mestic’ approach to security policy is related to the transnationalization of threats” (2000, p. 397; our translation). In this scenario, state interests are relativized by the narrative, and there is a constant invisible competition for space and power.

Examples of ways and means of transnational threat include competition for spaces outside a national jurisdiction, known as global commons (SANDLER, 1992). The possibility of a global consensus of global powers on common spaces is questioned by the authors. Brzezinski (2012) explains that the United States will have difficulty leading the protection and good faith management of the global commons, such as climate change, because it does not have the necessary power in the face of the geopolitical interests of Russia and China. In information warfare, the analysis of geopolitical resources transcends the geographic space under the dominion of States, extending the study to common areas, or without defined spatial domain, and the means of military action cover a multidomain nature.

The management of the global commons: sea, space, water security, and the environment, is a current issue, which proposes an international agenda related to the ends. Antarctica

is an example of common spaces, which contain transnational interests. Seven countries made sovereignty claims since the Antarctic Treaty of 1959: United Kingdom – Australia – New Zealand – France – Norway – Argentina – Chile. However, Antarctica technically belongs to no one and, according to the Defense Strategy (AUSTRALIA, 2020), the environment may include conflicts between states and the conduct of covert military activities in the gray zone of conflict. The threats challenge the Antarctic Treaty by the struggle for sovereignty, the non-militarization of Antarctica, and the commitment to keep the Protocol on Environmental Protection (1991) that provides protection of the environment and prohibits mining and oil extraction.

Meanwhile, by the means of information warfare, the ways of threats can come from the understanding that large areas with natural resources are catalogued as global common for the environmental just cause of mankind. This would be the case of the Amazon between Brazil, Venezuela, Colombia, Ecuador, Peru, and Bolivia; or the Argentinean and/or Chilean Patagonia, with a partial British presence (BORRELL, 2020). South America includes a great variety of biogeographic regions threatened by the interests of other states, its main resources being: energy, fresh water, food and the epicontinental sea. The continent has the largest extension of jungles and rainforests in the world, richest in biodiversity (KOUTOUDJIAN; CURTI, 2015). In a context of common regional threat, Paraguay, Argentina, Brazil, and Uruguay have the largest water reserve, the Guarani Aquifer, beyond the common interests in the South Atlantic continental shelf (KOUTOUDJIAN; CURTI, 2015).

According to Van Creveld (2007), another important group of transnational threats by other ways and means are terrorists, guerrillas, and thieves, a situation that benefits from the difficulty of reaching a consensus on the definition of national security and defense, but which are built on charismatic rather than institutional bases and motivated by fanaticism or ideologies. As low-intensity conflicts grow in the future, intermingling with the possibility of traditional state conflicts, they will produce a collapse in Clausewitz's triune structure of defense: government, people, and army. The difference between front and back of the state, as civilians and military, will disappear under transversal and information threats. The United Nations Development Program, in its 1994 report, "is based on addressing threats from both military and non-military sources, such as interstate conflicts, human rights violations, terrorism, organized crime, drug trafficking" (OROZCO, 2006, p. 176; our translation).

Another common area of competition is cyberspace, which represents a great opportunity to define other ways and means in the strategy. "Cyber incidents and attacks are now a source of threat in the globalized world, due to their ability to access diplomatic, governmental and military information systems" (VERGARA; TRAMA, 2017, p. 14; our translation). There is a war of narrative and influence. The attacks are continuous and permanent, without methods, scope, and consequences (VERGARA; TRAMA, 2017). "Cyberattacks present a new and growing threat, which international law and most current national laws are unable to cope with" (VERGARA; TRAMA, 2017, p. 88; our translation). The interconnected domain environment expanded the possibilities in space and time of information threats, determining the fusion of the multidomain jurisdictional fusion of state interests. Attacks do not respect the

limits of the land, air, and maritime domains of military conflicts, expanding the possibilities of relativization of borders, actors or interests that take advantage of the cyber domain.

In a great competition of ways and means, states and non-state actors are rapidly expanding their investment in cyberspace. Threats operate among populations with whom they often share a cultural or ethnic identity, making it difficult to distinguish between threat and non-threat. The information environment increased in multidomain complexity of military employment and the control of will and influence can affect decision makers. Because of the widespread availability of technology, the information environment became an even more important consideration for military planning, because armed forces depend on these technologies (ESTADOS UNIDOS, 2016). Military technology yields to expanding possibilities of artificial intelligence and unmanned weapons are increasingly used. The control of influence and the power of information became part of the strategic considerations of the most recent global commons and transnational threats of the 21st century, following the restructuring and recovery of power between Western and Eastern states, with the expansion of the role of China and Russia on the international chessboard of military competition.

Therefore, in information warfare, the threats will be not only from great powers and regional adversaries, but also from extremists, violent and criminal non-state actors, and from threats such as climate change, infectious diseases, cyber-attacks, and disinformation that do not respect national borders (ESTADOS UNIDOS, 2021). The transnational character of threats' ways and means requires the expansion of the concept of traditional use of military power, evolving towards a concept of a multidomain weapon that should imply a grand strategy. So, what would be the best strategy for state security?

#### **4 THE GRAND STRATEGY AND THE CHANGE OF WAYS AND MEANS THROUGH INFORMATION OPERATIONS**

The realistic identity ends of the states considered world leaders lead the countries to a permanent competition for common interests. In the realist vision, military means and ways are no longer sufficient. The idea of a grand strategy requires the participation of different actors in the formulation of state policies, incorporating the phenomenon of information into the pluralism of actors.

The information strategy experiences the integration of other means of Cyber Warfare capability with Intelligence, Information Operations, Cyberspace, Electronic Warfare, and Space Operations as part of a Multidomain Task Force as Strategy concept (THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, 2021). To exercise its internal sovereignty, or even to maintain its *status quo* in the face of non-state threats, each country uses the Grand Information Operations Strategy in different ways and goes beyond state military boundaries. In the grand strategy, the ways used are comprehensive, encompassing a diverse range of instruments of national power rather than focusing on a single type of instrument (LAYTON, 2012).

Brazil and Argentina made little progress in understanding the scope of the multi-domain grand strategy of information and the change of ways and means. In the context of global competition, peripheral countries may be under the constant influence of great power

interests. At present and in the future, the global commons and the relativization of the possession of territories, such as the Amazon Rainforest and areas of the South Atlantic and Antarctica, are in dispute. The multidomain conflict establishes a challenge of influence and interests, involving the application of military instruments in a holistic and integrated manner.

The cyber environment is the common space of competition and the most active in the multidomain, it has no borders and is a transnational threat, making states think about defense structures. However, it is not the only military instrument of information warfare. The Western approach, such as Brazil's or Argentina's, to cyber defense typically focused on ways and means with technical responses, without considering the interface with information warfare. "This approach is entirely suitable for some persistent or background threats, but is not always sufficient for a broader, more holistic approach such as that taken by Russia" (GILES, 2016, p. 22; our translation).

As an example, for the US, successful military contributions in the multidomain require sustained integration in ways and means of conventional, irregular, and special operations capabilities (ESTADOS UNIDOS, 2020c). The Russian Federation (RF) and the People's Republic of China (PRC) use all the instruments of their national power to undermine and remake the international system to serve their own interests (ESTADOS UNIDOS, 2020a). United Kingdom is militarily employing Information Operations in integral defense, increasing the escalation of competition, and the rise of crisis and conflict (REINO UNIDO, 2021).

According to the US Strategy there is irregular warfare by other ways, between state and non-state actors to influence populations and affect legitimacy. The traditional grand strategy incorporated the importance of the participation of actors additional to the military. This type of warfare favors other means, indirect and asymmetric approaches, although it can employ the full range of military and other capabilities in order to erode an adversary's power, influence and will. Information Operations, unconventional warfare, stabilization, foreign internal defense, counterterrorism, and counterinsurgency are also included. The means of related activities, such as psychological operations, cyberspace operations, combating threat networks, threat financing, civil-military operations, and security cooperation also shape the information environment and other areas of competition and conflict centered on the population (ESTADOS UNIDOS, 2020c).

According to US strategic scenarios, the world's powers are competing on artificial intelligence and quantum computing, which could shape everything from the economic and military balance between states to the future of work, wealth and inequality within them. Next generation (5G) telecommunications infrastructure will set the stage for all aspects of Information Operations. The ways and means of emerging technologies remain largely ungoverned by laws or rules designed to focus rights and values, managing the risk that competition will lead to conflict (ESTADOS UNIDOS, 2021).

Therefore, the Russian concept of ways and means carries computer network operations together with

psychological operations, strategic communications, intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, weakening of communications,



degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities. (MSHVIDOBADZE, 2011, our translation)

Information and psychological warfare will come above all forms and methods of operations in future wars to achieve superiority in troops and arms control and to erode the morale and psychological spirit of the opposing side's armed forces personnel and population. Indeed, information warfare and psychological operations provide a large part of the basis for victory. (CHEKINOV; BOGDANOV, 2015, p. 44; our translation)

Russia conducts information confrontation activities between states and other actors in the information space with “the aim of causing damage to information systems, processes and resources, critical structures, [and] undermining political and social systems in order to destabilize society and the adversary state as a whole” (NOGOVITZIN, 2009, p. 12; our translation). Confrontational information is a broader concept than information operations, encompassing the action of other actors in society, which means a multifaceted, multifactorial struggle involving “social systems, classes, nations [and] states through diplomatic, political, informational, psychological, financial, economic, armed conflict, and many other forms of influence” to achieve strategic and political objectives (SLIPCHENKO, 2013, p. 53; our translation).

China conducts activities in the information gray zone and expands into the Indo-Pacific, Antarctic, and Arctic.

These activities involve with military and non-military forms of assertiveness and coercion aimed at achieving strategic goals without provoking conflict. In the Indo-Pacific, these activities have ranged from militarisation of the South China Sea to active interference, disinformation campaigns and economic coercion. (AUSTRALIA, 2020, p. 5)

China is widely seen as the closest competitor to the United States in the international artificial intelligence market. China's 2017 Next Generation Artificial Intelligence Development Plan describes as a strategic technology that has become a focus of international competition. Such technologies could be used to counter espionage and assist military targets. In addition, open-source publications indicate that China is developing a set of artificial intelligence tools for cyber operations (ESTADOS UNIDOS, 2020b).

In the United Kingdom the means of Information Operations are in the Integrated Operational Concept of the Ministry of Defense, which emphasizes the need for integration across all combat domains, with different actors, while also incorporating cyber capability under what is called Multidomain Integration. According to the UK strategy, CP 411: “Our armed forces must have the tools and capabilities they need to lead, influence, partner, deter and when necessary to fight to ensure the whole of the UK and its interests are protected” (REINO UNIDO, 2021, p. 11). For Layton (2012), the United Kingdom has a major strategic change in

ways that also involves the development of resources and their allocation, a complex combination that must generate the legitimacy and soft power needed to be successfully implemented from peacetime.

Based on the examples, it can be concluded that the grand strategy means of Information Operations has an expansive and integrative scope of other actors' ways that encompasses the development of a society's economic, demographic, biological, environmental, and social resources. The allocation of these resources and military power are the application of national unified power.

The role of information and information technologies in strategic competition and military operations is evolving considerably, challenging the technological capabilities of countries such as Brazil and Argentina. In the early 2000s, the growth of the Internet occurred, becoming a tool that shapes public opinion and influence politics, economics, and military decision-making. New information technologies will increase the volume of means, accuracy and speed of sharing, processing, and analyzing data. Discussions on advanced information technologies that would have a significant effect on the character of military operations will, in the near future, transform conventional military conflicts into a great information war.

## 5 CONCLUSION

The analysis presented here allows us to understand how the international strategic scenario is seriously affected by the multidomain capability of Information Operations. The State, as a realistic major player, faces the challenge of developing a major strategy for competition in the information dimension. The development of a grand strategy requires examining how ends, ways, and means actually operate within contrasting contexts. The realist view where national interests are defined in terms of military power on the international stage is no longer sufficient. The idea of a grand strategy requires the participation of different actors in the formulation of State policies, incorporating the phenomenon of information into the pluralism of actors.

The first part of the analysis on the ends allowed us to conclude that the existence of the State still needs to be guaranteed by military power, although adapting it to the possibilities of the ways and means of the future. Inter-state threats remain a very current issue and deserve attention in the military strategy of competition for natural resources and territorial spaces. The realist theory of the existence of the State is fundamental to understand that the referent object of security will be the territorial integrity of the State, since it is the State itself that can, based on its position in the system, preserve the interests of the nation and with them the welfare of society. The institutional process of the State through which the strategy is formulated needs to integrate the ends to a combination of resources (material and social) that can and will be used as instruments in the implementation of a grand strategy.

The second point of conclusion is that there is a change in the ways and means of threats and that these are not only military and between states. There is a great mutation that considers the existence of new actors, interconnected and internationalized threats, being part of a great multidomain information war. However, each country shapes the ways and elements

of material and social resources in very different ways. Threats permeate institutions and require an integral role for the means of national participation. According to the strategic scenarios, the world's powers are competing in the multidomain and transnational threat is the competition for spaces outside national jurisdiction, called global commons. There is great difficulty in defining military boundaries in information warfare, expanding the possibilities of ways and means in disputes in the gray zone of conflicts and involving different non-military sectors.

The third conclusion is that the means of Information Operations are among the main strategies of the States to face the problem, beyond the military operational field. Within the components (ways, means, and ends) of grand strategy, the use of other non-kinetic military ways and means in US, UK, Russian, and Chinese strategy, such as cyber warfare, psychological operations, electronic warfare and communication, are combined with national means to shape grand strategy. In this scenario, the challenge for countries such as Brazil and Argentina is to better understand how information confrontation operates in multidomain warfare, the perspectives for effective international governance of the information domain, and the ways in which information confrontation can be used as an instrument of soft power.

Finally, the ends of realistic interstate threats continued, changes in the ways and means of state and non-state threats are here to stay in the global commons. State borders are no barrier to technology and the transnationalization of information. The military power of Information Operations means can add great defense capability to the State and that is why they are being implemented at the grand strategy level of the great power States. The maintenance of realistic national interests of countries such as Brazil and Argentina require the adequacy of military strategic multidomain defense doctrine, with extensive use of Information Operations as the basis of their grand strategy.

## **AUTHORSHIP AND CONTRIBUTIONS**

All authors participated equally in the development of the article.

## REFERENCES

AUSTRALIA. **2020 Defence Strategic Update**. Canberra: Australian Government Department of Defence, 2020.

BALZACQ, T.; DOMBROWSKI, P.; REICH, S. **Comparative Grand Strategy: A Framework and Cases**. Oxford: Oxford University Press, 2019.

BOBBIO, N. **Estado, gobierno y sociedad**. México: Fondo de Cultura Económica, 1996.

BORRELL, J. J. Dimensiones del espacio geopolítico como categorías de análisis en materia de recursos naturales. **Casus Belli**, Buenos Aires, n. 1, p. 73–101, 2020. Available from: <https://fe.undef.edu.ar/publicaciones/ojs3/index.php/casusbelli/article/view/9>. Access: May 3. 2023.

BRZEZINSKI, Zbigniew. **Strategic Vision: America and the crisis of global power**. New York: Basic Books, 2012.

BUZAN, B. **People, States and Fear: an Agenda for International Security**. Boulder: Lynne Rienner Publishers, 1991.

CHA, V. Globalization and the Study of International Security. **Journal of Peace Research**, London, v. 37, n. 3, p. 391–403, 2000. Available from: <https://journals.sagepub.com/doi/10.1177/0022343300037003007>. Access: May 3. 2023.

CHEKINOV, S. G.; BOGDANOV, S. A. “Прогнозирование характера и содержания войн будущего: проблемы и суждения” (Forecasting the nature and content of wars of the future: problems and assessments), *Voennaya Mysl’* (Military Thought), No. 10, p. 44-45, 2015.

COHEN, S. B. **Geopolitics. The geography of international relations**. Lanham: Rowman & Littlefield, 2015.

ESTADOS UNIDOS. **FM 3-13: Information Operations**. Washington, DC: Headquarters, Department Of The Army, 2016.

ESTADOS UNIDOS. **Advantage at Sea**. Prevailing with Integrated All-Domain Naval Power. Washington, DC: Marine Corps and Coast Guard, 2020a. Available from: <https://media.defense.gov/2020/Dec/16/2002553074/-1/-1/0/TRISERVICESTRATEGY.PDF>. Access: May 3. 2023.

ESTADOS UNIDOS. **Emerging Military Technologies**: background and Issues for Congress. Congressional Research Service. Washington, DC: Congressional Research Service, 2020b. Available from: <https://crsreports.congress.gov/product/pdf/R/R46458>. Access: May 3. 2023.

ESTADOS UNIDOS. **Summary of the irregular warfare annex to the national defense strategy**. Washington, DC: Department of Defense, 2020c. Available from: <https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF>. Access: May 3. 2023.

ESTADOS UNIDOS. **Renewing america's advantages**. Interim National Security Strategic Guidance. Washington, DC: The White House, 2021.

GILES, K. **Manual de guerra de información russa**. Roma: NATO Defense College, 2016.

HOBBS, T. **Leviatan**. O la materia, forma y poder de una república eclesiástica y civil. México: Fondo de Cultura Económica, 2005.

KOUTOUDJIAN, A.; CURTI, S. **La geopolítica de sudamérica en los últimos años**. Buenos Aires: Ad-Hoc, 2015.

LAYTON, P. The idea of Grand Strategy. **The RUSI Journal**, London, v. 157, n. 4, 2012. Disponible: <https://rusi.org/explore-our-research/publications/rusi-journal/idea-grand-strategy>. Acceso en: 3 maio 2023.

LIANG, Q.; XIANGSUI, W. **La guerra más allá de los límites**. Beijing: Pla Literature & Art Publishing House, 1999.

MILANI, C. R.; NERY, T. Brazil. In: BALZACQ, T.; DOMBROWSKI, P.; REICH, S. **Comparative Grand Strategy: a framework and cases**. Oxford: Oxford University Press, 2019.

MØLLER, B. Conceptos sobre seguridad: nuevos riesgos y desafíos. **Desarrollo Económico**, Buenos Aires, v. 36, n. 143, p. 769–792, 1996. Available from: <https://dialnet.unirioja.es/servlet/articulo?codigo=2651089>. Access: May 3. 2023.

MORGENTHAU, H. J. **A política entre as nações: a luta pelo poder e pela paz**. Brasília, DF: Editora UnB, 2003.

MSHVIDOBADZE, K. El campo de batalla en tu computadora portátil. **Radio Free Europe/Radio Liberty**, Praga, 21 mar. 2011. Available from: <http://www.rferl.org/articleprintview/2345202.html>. Access: May 3. 2023.

NOGOVITZIN, A. In: Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, **Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation**. Santa Monica, CA: RAND Corporation, 2022. Disponible: [https://www.rand.org/pubs/research\\_reports/RRA198-8.html](https://www.rand.org/pubs/research_reports/RRA198-8.html). Acceso en: 3 maio 2023.

OROZCO, G. El concepto de la seguridad en la Teoría de las Relaciones Internacionales. **Revista CIDOB d'Afers Internacionals**, n. 72, p. 161-180, 2006. Available from: [https://www.cidob.org/es/articulos/revista\\_cidob\\_d\\_afers\\_internacionals/el\\_concepto\\_de\\_la\\_seguridad\\_en\\_la\\_teor%C3%ADa\\_de\\_las\\_relaciones\\_internacionales](https://www.cidob.org/es/articulos/revista_cidob_d_afers_internacionals/el_concepto_de_la_seguridad_en_la_teor%C3%ADa_de_las_relaciones_internacionales). Access: May 3. 2023.

REINO UNIDO. Parliament by the Secretary of State for Defence by Command of Her Majesty. **Defence in a competitive age**: CP 411. London: Ministry of Defence, 2021. Available from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/974661/CP411\\_-\\_Defence\\_Command\\_Plan.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-_Defence_Command_Plan.pdf). Access: May 3. 2023.

SANDLER, T. After the Cold War, secure the global commons. **Challenge**, Abingdon, v. 35, n. 4, p. 16–23, 1992. Available from: <https://www.tandfonline.com/doi/abs/10.1080/05775132.1992.11471599>. Access: May 3. 2023.

SILOVE, N. Beyond the Buzzword: The Three Meanings of “Grand Strategy”. **Security Studies**, Abingdon, v. 27, n. 1, p. 27–57, 2018. Available from: <https://www.tandfonline.com/doi/full/10.1080/09636412.2017.1360073>. Access: May 3. 2023.

SLIPCHENKO, V. Information Resources and Information Confrontation. **Army Digest**, Moscou, n. 10, p. 52–57, 2013.

THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. **The military balance 2021**. London: Routledge, 2021.

VAN CREVELD, M. **La transformación de la guerra**. La más radical reinterpretación del conflicto armado desde Clausewitz. Buenos Aires: Jose Luis Uceda, 2007.

VERGARA, E. D.; TRAMA, G. A. **Operaciones Militares Cibernéticas**: planeamiento y Ejecución en el Nivel Operacional. Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2017.

WEBER, M. **Economía y sociedad**. Esbozo de sociología comprensiva. Madrid: Fondo de Cultura Económica, 1964.

WEBER, M. **El político y el científico**. Madrid: Alianza Editorial, 1967.