DOI 10.21544/1809-3191.v25n2.p 517-543

THE CYBER ISSUE AND REALIST THINKING

Marcio Rocha[1]
Daniel Farias da Fonseca[2]

ABSTRACT

This research aimed to analyze to what extent the realist theory contributes to explain the Cyber Issue and the occurrence of virtual conflicts between states today. The study takes place in the context that, in recent years, several states in the International System have been attributing to their Armed Forces the responsibility of Defense not only against physical threats, but also against those originating in cyberspace. This investigation is justified by the contribution with the exiting literature on the cybernetic topic, which is still relatively small today. The study approached what characterized the conflict and the cyberspace, as well as how this phenomenon affects the perception of State Security. A brief review was conducted on realist thinking and its fundamental premises. The research conclusion points to an applicability of the realistic logic for understanding the state conflicts in which cyber activities are present, similar to what already occurs in conventional conflicts in the International System, even though there is a certain resistance on this topic from some scholars of interstate conflicts, adherents of realist thinking.

Keywords: Cyber issue. Realism. Defense and Security. Strategic Studies.

[1] PhD. Fluminense Federal University (UFF), Rio de Janeiro (RJ), Brazil. E-mail: marcioochamr@yahoo.com.br / Orcid: https://orcid.org/0000-0003-0948-6863.7856-5640

[2] Master's degree. Fluminense Federal University (UFF), Rio de Janeiro (RJ), Brazil. E-mail: danireload@gmail.com

INTRODUCTION

This research aimed at analyzing how the realist theory contributes to explain the Cyber Issue and the occurrence of virtual conflicts between states today.

It is a fact that the development and intensive use of advanced data transmission and processing technologies, leading to a popularization and massification of its use, such as the Internet, and combined with the globalization process, made cyberspace[3] an environment with numerous conflicts between political groups, criminal groups, companies in general and also between states. As cyberspace is something still recent, understanding its meaning is still in development. But it is also a fact that there is still no control or dominance over cyberspace by a particular country or group of countries. This leads us to understand that, in a scenario of competition, conflict, or even war, being able to invade the cyberspace of a particular institution or country would allow us to know more about it and, if possible, to obtain its control, which would result in a strategic advantage for those who are able to do so. Currently, there is no denying that information or knowledge control is a strategic asset for any organization, company or state.

In this sense, it is essential, especially for states, to protect their information and critical infrastructure. Due to the development and use of increasingly advanced transmission and data processing technologies, states now use and depend on computer networks to send and receive data, and to promote knowledge management.

Critical infrastructures specifically, may be understood as those that are vital to the survival of the state and on which it greatly depends for its operation, such as hydroelectric plants, communication and telecommunication systems, air traffic control systems, banking systems, etc. To better explain the meaning of critical infrastructure, the Canadian Government's definition was used:

> Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services

[3] Cyber is an abbreviation of the word "cybernetic", which refers to something or somewhere that has a large concentration of technology, especially networks, internet and computers. An interesting fact about the etymology of the word "cybernetic" is that it originates from the Greek word "κυβερνήτης", which means "the art of governing" or also the "art of sailing".

> essential to the health, safety, security or economic well-being of [the population], and the effective functioning of government. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence (CANADA, 2009, p. 2).

Janczewski and Colarik (2008) argue that the use of these data transmission networks has led to an increase in the efficiency and performance of companies and states, but has also caused security problems due to the increase in the automation of processes and the concentration of the most important information and data on computers.

> The use of these systems and networks means that there now is a major concentration and centralization of information resources. Such a consolidation creates a major vulnerability to a host of attacks and exploitations. Over the past 35 years, electronic economic espionage has resulted in the theft of military and technological developments that have changed the balance of power and continue to threaten the safety and stability of the world. (JANCZEWSKI; COLARIK, 2008)

That is, the authors point to the existence of vulnerabilities in the computer systems in the network, as well as emphasize that these vulnerabilities have been exploited in such a way that changes have occurred in the world balance of power, in an indirect reference to China's ability to promote cyber actions.

The realization of these vulnerabilities, especially those with potential to pose threats to the National Defense of the states, has forced a considerable number of countries to use their Armed Forces to defend the cyberspace of their interests, enabling them to develop both offensive and defensive actions in cyberspace (TABANSKY, 2011).

With this logic, we verified that several states now consider that their Armed Forces, within their Defense attributions, should execute activities to protect their countries not only against physical threats, but also against those from cyberspace (CAVELTY, 2012). What explains these decisions is that, during the last ten years, there has been a considerable increase in the occurrence of cyber-attacks and conflicts. This increase includes those that were led by a state and targeted a country considered to be a potential enemy (MILLMAN, 2018).

In this sense, for some authors, cyberspace may be considered, at present, a new military environment (KRAMER; STARR; WENTZ, 2009). For them, cyberspace would have become the fifth domain of military action, alongside land, sea, air and space.

This situation has had considerable impacts on the military, affecting the scope of its tasks and the way in which they can be carried out, using this environment to conduct cyber operations that would support military action or achieve political objectives (SHELDON, 2011).

Still needing further analysis and better understanding, the conflict between states involving cyber activities already has the attention of scholars and researchers from the two main academic areas focused on the study and research of state conflicts: Strategic Studies and International Relations.

However, there is still some resistance, within these areas, regarding deepening studies on cyber issues and how this impacts the relationship between states. This is mainly due to the predominance of realist thinking among researchers in these two areas, for which the Cybernetics theme would be beyond the scope of this current of thought.

It was in this sense that the research question that guided this study was focused on determining to what extent the realist theory contributes to explain the Cyber Issue, regarding the occurrence of virtual conflicts between states at present.

The study was exploratory and based on a literature review on the subject in question; it is important to notice that this is a recent, complex subject, which still has limitations in theoretical and bibliographic terms. This research is justified by the possible contribution with the scarce literature on the subject, as well as helping to understand the current state conflicts in which offensive and defensive cyber actions were present.

The structure of the investigation was divided as follows: in the first part, an analysis was conducted about the meaning of Cyber Issue, cyberspace and its relation with aspects of the National Defense of some countries; in the second part, aspects of realist thinking, its main characteristics and approaches in the analysis of conflicts between states in the international scenario were addressed; and finally, in the third part, an analysis of cyber conflicts involving states was developed, taking as reference the realist thinking and determining the level of contribution of this current of thought in the approach and explanation of the state conflicts in which cyber activities were verified.

THE CYBER ISSUE

The period of cyberspace emergence may be pointed to as the 1970s, with the creation of the ARPANET[4]. It was the first system that allowed the network connection of computers, allowing them to communicate with each other, thus forming this environment (TABANSKY, 2011). What justified the creation of ARPANET dates back to a US Army need for a robust and long-range military communications network (KREMER; MÜLLER, 2014). Consequently, this network arises to serve and allow the exchange of information between computer equipment, physically distant, even in the event of a nuclear attack, according to the United States optics.

For the purposes of this research, we considered that cyberspace consists of a virtual environment, composed of information, formed by computer networks that transmit it and connect computerized systems, through which information may travel, be stored, accessed and modified (TABANSKY, 2011). One of the main components of this environment is the Internet, i.e. a global communication network created between the late 1980s and early 1990s (CAVELTY; MAUER; KRISHNA-HENSEL, 2007). The Internet was based on the protocols and technologies developed for ARPANET, but its use was directed to the civil environment. The Internet, as well as the cyberspace itself, experienced a period of expansion, popularization and of increased use and presence around the world in the late 20th century.

Cyberspace is widely used worldwide in daily activities performed by both the civilian population, companies in general and governments. Whether through the use of the Internet, or Information and Communication Technologies (ICT), it is increasingly present in our daily lives (KREMER; MÜLLER, 2014).

Due to the importance and benefits provided by cyberspace, and as a consequence of this phenomenon, experts began to see that there

[4] ARPANET – The Advanced Research Projects Agency Network (ARPANET) was a communications network (initially exclusively for military use), created to enable communication between different US military bases, located on its territory or not, and their computer systems, facilitating the transmission of information, the coordination of their actions, and increasing the reliability of these transmissions (KREMER; MÜLLER, 2014).

would be a potential for dangers and threats to arise from the use of this virtual environment (RIBEIRO; RIVERA, 2014). It was believed that some of them, such as hacking and the spread of computer viruses, could negatively affect the essential activities of states, especially with regard to their security.

The debates and concerns arising from this prognosis of insecurity gave rise to what we record as the Cyber Issue in this study. Therefore, for the purposes of this research, the understanding of Cybernetics refers to the potential problems and consequences for society and state, provided by the intensive use of advanced technologies that support the transmission and processing of data of interest to institutions, companies, irregular or terrorist groups, and states. This process led to a popularization and massification of its use, as well as the consequent loss of control over it, allowing its harmful use by people, diverse groups and even by states. The Cyber Issue is directly related to the potential negative impacts that the resulting cyber threats may have, mainly, on State Security and Defense.

We understand by cyber threats offensive and intrusive virtual actions that have great potential to impact or compromise the protection of states, whether physical or virtual. This impact may occur through theft of strategic and confidential information, and the conduction of virtual attacks and intrusions against critical infrastructures, the use of which is essential for conducting State Defense-related activities. In this case, such acts may culminate in their permanent and physical destruction, denying and disabling their use, whether temporarily or indefinitely. These actions may include disruption of communication systems, global positioning, banking systems, and the generation and distribution of drinking water, fuels and electricity, etc. (TABANSKY, 2011).

The lack of control and widespread use of cyberspace allows these effects to be obtained by conducting acts of espionage, sabotage, and attacks; possible through cyberspace. These actions are usually carried out through the invasion of computerized equipment or computer networks to manipulate stored information or to interrupt information transmission. Among these actions, the cyber-attack stands out, due to its destructive potential, as well as the opportunity it offers to conduct cyber conflicts.

Cyber-attack may be defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computers or information networks and/or programs that reside or transit through these systems or networks" (CAPLAN, 2013, p. 2). This type of attack is intended to cause harm to others by disrupting — temporarily or permanently — or by changing the regular operation of a target system. This includes copying, deleting, or altering data that is stored in it, in others connected to it, or that only travel through it (TABANSKY, 2011).

In practice, cyber-attacks may be used to generate material or immaterial damage to its target, impairing its performance. It also makes it possible to negatively impact the security of a state by performing virtual intrusions that interfere with its full functioning and that of its bodies or institutions.

Among these consequences, we highlight the actions of the Armed Forces, which became highly dependent on the use of cyberspace for their daily operations and related to the protection of the country and the preparation to participate in possible military conflicts (MANESS; VALERIANO, 2016).

In the case of the Armed Forces, cyberspace dependency is related to the need and complex activity of obtaining and transmitting real-time information about battlefield conditions, and the essential coordination of the activities of troops and military equipment of different military units involved in battle. This dependence also means that the Armed Forces have become significantly susceptible to cyber threats and the impacts they may have on conducting military operations.

When we relate the performance of the Armed Forces and the cyberspace, we have to consider that a cyber conflict might be restricted only to actions performed in the virtual environment, without involving the use of traditional military actions. However, it may also occur parallel to a war conflict in physical environments, with the aim of supporting it (TABANSKY, 2011).

The term cyber warfare is generally used to refer to a possible type of conflict that can occur through cyber space. Cyber warfare may involve the confrontation of one or more states, as well as diverse political or criminal groups, and is based on exploiting security breaches in this environment to harm the potential adversary. However, there is still no consensus widely accepted by researchers in this field and by military strategists, about what would in reality constitute a cyber war. The same question exists as to whether or not to consider whether it would be possible for a type of war to actually occur through cyberspace. For these reasons, this study has addressed cyber conflicts in general, but without going into the merits of whether or not they may constitute a new type of war.

Recent facts point out that cyber conflict may offer advantages to the state capable of executing it compared to traditional military conflict. This is mainly related to the low cost of these activities and the difficulty of determining the authorship and identity of the people responsible for it, as well as their occurrence. What stands out is that the virtual character of this type of conflict makes it possible for the person responsible to mask or hide their true identity, whether it is formed by an individual, a group, or a state.

The most developed countries are potential targets for cyber-attacks and conflicts. The more technologically advanced a country is, the more it depends on cyberspace. Thus, the use of cyberspace may be a military advantage to a militarily inferior adversary, which, in theory, might be a relatively inexpensive and effective means of minimizing military asymmetry, being capable of causing significant damage to a more powerful adversary.

Currently, there is no international body that has any kind of control over the Internet as a whole (CAVELTY; MAUER; KRISHNA-HENSEL, 2007). It, which is a central component of cyberspace, was elaborated in a decentralized manner, without the existence of a single global entity responsible for managing it (TABANSKY, 2011). Thus,

> the Internet is therefore a primary example of an unbounded system, a system characterised by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and lack of complete information about the network. (CAVELTY, MAUER and KRISHNA-HENSEL, 2007, p. 27)

Thus, cyberspace is characterized by a condition of anarchy, that is, the absence of an authority that is hierarchically superior to the states and has the power to impose its will on them (KREMER; MÜLLER, 2014). The condition of anarchy is one of the main precepts of realist thinking and also one of the main factors in enabling the elaboration of the explanatory logic provided by this current of thought. This logic is the basis for explaining the actions and behaviors adopted by states during and before military conflicts that may occur between them in an international environment marked by the phenomenon of anarchy.

It is noteworthy that this current of thought is not the only theoretical approach, or line of thought, related to the analysis of

International Relations. We could use the thinking of the English School, Neoliberalism, the Copenhagen School Securitization Theory, or Constructivism. However, using the realist theory offers a more appropriate approach to this study. When applied to the performance of states in cyberspace, it allows us to gain broader and more general considerations, whose scope is associated with more ontological issues, that is, with a more general theory (ACÁCIO; SOUZA, 2012).

Realism identifies some specific features of the international scenario and points to how they may influence state behavior. In systems that are governed by the same aspects, it could be employed to draw similar conclusions.

Cyberspace has a primordial characteristic that is also present in the International System (IS): anarchy. For this reason, it becomes possible to apply this theory to analyze the behavior of states in cyberspace.

According to Reardon and Choucri:

> realist theories of international relations are most applicable to issues related to cyber security and cyber warfare. Realist theories can help to explain how states use cyber technologies to advance their interests in security, and how they may respond to other states' cyber capabilities. (REARDON; CHOUCRIL, 2012, p. 6).

For this reason, we discuss below the main features and the logic that guides realist thinking.

REALIST THINKING

The Realist School of International Relations emerged in the 1920s as a systematized form of study and scientific analysis of International Relations and in a post-World War I context. Its focus is to understand the dynamics, characteristics and possible consequences of interaction between states in the global political arena, in particular, the conflicting relations between them. The aim of realist thinking is to develop scientific theories and knowledge that allow us to understand the rationality that influences conflicts between states and, mainly, to understand and explain what their causes would be.

The realist theory, like others, is based on a set of simple assumptions that are used to try to simplify and explain a complex and multifaceted reality (LAKE, 2008). It was believed that, through a systematic study of the phenomenon of war, it would be possible to determine the conditions necessary to prevent them, thus enabling the existence and guarantee of peace between states (WALTZ, 2002). Its approach, unlike pacifist currents, was not the promotion of broad global disarmament as a means of peace. In their view, this would be a Utopian peace, doomed to failure (CARR, 2001).

For the realists, war would be a recurring phenomenon in the International System that could afflict or involve any country, varying only the reason and time at which they could occur. Realist thinking has three main premises, which form the core and basis of its thinking and analysis. These factors guarantee to this current of thought its explanatory power on the dynamics of action and behavior of states in the International System. These premises are: 1) the centrality of states in the international environment, or the belief that they would be the main actors in this environment; 2) that they seek and prioritize to satisfy their own interests; and 3) that this environment is marked by its anarchic character.

The first feature, which regards the state as the main actor in the context of International Relations, is based on the belief that states are the only actors who have a level of power, especially that related to military power, which allows them the ability to project power over others and impose their will on them.

For realists, power is composed of certain aspects called power resources or capabilities. However, in many of their analyses, the resources and capabilities of a state are considered to be themselves a type of power (BALDWIN, 2012). They believe that the main capability that the state must maintain and enhance is its military capabilities, also called Military Power.

According to Edward Carr:

> The supreme importance of the military instrument lies in the fact that the last ratio of power in International Relations is war. Every act of the state, in the power aspect, is directed toward war, not as a desirable weapon, but as a weapon that may be needed as a last resort. (CARR, 2001, p. 143, our translation)

Having adequate military capability would be the last resort that states may turn to in order to confront their potential enemies, or to impose their will on others. This may be as much through the use of violence as through the mere threat of force imposed.

The second characteristic highlighted by realist thinking refers to an alleged selfishness of states seeking to achieve or maintain their interests. That is, they would rather prioritize the fulfillment of their own political goals than help other states.

This feature is based on the fact that the political class of a state, and consequently of its diplomats, would be pressured by the people to attend mainly to the national interest and to promote national development, including through negotiations at the international level.

The third characteristic highlights the absence of an authority at the international level that is hierarchically superior to the states, which has the ability or the power to impose its will on them, being able to exercise some control over their actions.

As Aron emphasizes, in an anarchic environment, the mere existence of other countries and their relationship may pose a potential threat to themselves (ARON, 2002). This stems from the lack of clarity and certainty of the intention of these states towards others. In this scenario, we find that, if a nation were to declare war on another country, there is no institution that has the function, or responsibility, or clear and definite ability to prevent this act of war.

In realist thinking, there will always be the possibility that a war could occur at any time, as soon as a country decides to resort to this act against any of the others.

However, anarchy cannot be regarded as a direct cause of war, but as a permissive cause of war (Wendt, 1992). In other words, anarchy allows war to take place, since there is no entity capable of preventing interstate armed confrontation (WALTZ, 2001).

In this scenario, states would be solely responsible for their own security and capable of facing potential enemies. According to Baylis and Wirtz:

> In the absence of world government, realists note that states have adopted a 'self-help' approach to their interests and especially their security. In other words, they reserve the right to use lethal force to achieve their objectives […] (BAYLIS; WIRTZ, 2002, p. 7).

This approach may be understood as the conception that, in order to survive, each state must first rely on itself (ARON, 2002). This attitude, due to the distrust of other states, reinforces the selfish character attributed to them by realists.

In this context, the incentives for the existence some form of cooperation between states may be very low. What justifies this stance of the states lies in the absence of an institution with the authority and capacity to impose a punishment on anyone who violates what is established by international society.

According to Wohlforth:

> When no authority exists that can enforce agreements— "anarchy"—then any state can resort to force to get what it wants. Even if a state can be fairly sure that no other state will take up arms today, there is no guarantee against the possibility that one might do so tomorrow. Because no state can rule out this prospect, states tend to arm themselves against this contingency. With all states thus armed, politics takes on a different cast. Disputes that would be easy to settle if states could rely on some higher authority to enforce an agreement can escalate to war in the absence of such authority. The signature realist argument is therefore that anarchy renders states' security problematic and potentially conflictual, and is a key underlying cause of war. (WOHLFORTH, 2008, p. 135).

Thus, in an anarchic environment, where states seek to satisfy their own interests, there is a constant possibility of war (WALTZ, 2001). Or, according to Raymond Aron:

> All international politics involves a constant collision of wills, since it consists of relations among sovereign states which claim to rule themselves independently. So long as these units are not subject to external law or to an arbiter, they are, as such, rivals, for each is affected by the actions of the others and inevitably suspects their intentions. (ARON, p. 100, 2002)

This situation directly influences the behavior of states, causing them to feel constantly insecure, which results in the quest to enhance their safety. At the same time, they also seek to prepare for the possible occurrence of a conflict.

Also, according to Morghentau:

> The political objective of military preparations of any kind is to deter other nations from using military force

> by making it too risky for them to do so. The political aim of military preparations is, in other words, to make the actual application of military force unnecessary by inducing the prospective enemy to desist from the use of military force. (MORGENTHAU, 2003, p. 57)

Military preparations may be understood either as an effort by the state to defend its interests against those of other nations, or to make it capable of pursuing its own interests internationally. These interests and needs include ensuring their own survival as well as the safety of their citizens. In practice, a state that has greater power than others may be able to subordinate them to its will. If the main concern is state security, it may use this power to discourage threats or attempted attacks against it.

The pursuit of "security" by powerful states allows them to pursue power policies (CARR, 2001). Since their power over other countries is likely to change over time, this contributes to their constant competition for power.

Or, according to Raymond Aron:

> If we suppose that security is the final goal of state policy, the effective means will be to establish a new relation of forces or to modify the old one so that potential enemies, by reason of their inferiority, will not be tempted to take the initiative of an aggression. (ARON, p. 128, 2002).

Competition for power enhancement between states is called the Security Dilemma by the realists, that is, the situation in which the increase in power of a state may lead its neighbors to seek to carry out the same action. So, in this situation, countries close to this one would fear that this action might signal a possible preparation to use it against any of them in the near future. In this way, the others start to fear for their safety and seek to reinforce it, by replicating this same act, of seeking to increase their power.

Considering that the main aspect of the state power lies in their military power, then investment and the ability to produce warlike knowledge and technologies becomes essential for their survival. These technologies directly impact the level of military capability and, consequently, the power of these actors.

Military technologies, in general, influence the ability of military forces to act, being able to increase the efficiency and scope of their performance. Often the difference between the technological level of the armed forces of two states may be decisive in the outcome of wars. According to Hans Morgenthau, "the fate of nations and civilizations has often been determined by a differential in the technology of warfare for which the inferior side was unable to compensate in other ways" (MORGENTHAU, 2003, p. 237).

However, since the second half of the twentieth century, states have increasingly made efforts to achieve their political goals through the use of diplomatic and economic means, not through the use of force. The main reason for this is due to the high costs to perform this type of action, which fall on the one who chooses to use force.

Thus, the decision to use power or not usually involves a rational analysis of the cost-benefit of this action. This analysis involves both this type of action — the use of power — and the comparison between it and other possible courses of action that are feasible to be used to achieve the same political objective.

Even so, there are still considerable reasons for states to reserve large amounts of resources to invest in preparing, improving the efficiency and performance of their Armed Forces. This is mainly due to the possibility of exerting power over others through the mere threat of the use of violence and its instruments. If the target of this action believes that it can be accomplished, it may give in and do the will of the one who had the ability to promote the threat. However, in order to make this threat credible, it is necessary to have a military power greater than the threatened country has.

Nowadays, as mentioned earlier, there have also been occurrences of conflicts between states in the cyberspace, as well as the conduct of military operations supported by virtual actions.

The ability to develop offensive and defensive actions in the cyberspace may be considered today as another instrument of state power. Thus, the state capacity to perform cyber actions in support of military operations, considering the anarchic character of cyberspace, enables the application of realistic thinking about virtual conflicts between states, either about their occurrence or about the reasons that could lead to it.

In the following section, we will analyze the approaches that realist thinking dedicates to understanding cyber issues today.

THE CYBER ISSUE IN REALIST THINKING

Advocates of realist thinking generally argue only for the impact that war technologies may have on war activities, as well as on understanding the reasons that can lead a state to war. Thus, technologies applied to the Internet and cyber space as a whole are often overlooked by realists in their analysis. The same has been true for cyber conflict analysis, as well as for the possible threats and impacts that may arise from the cyber environment where they occur.

The possibility of a state gaining or using some kind of power within or through cyberspace is disputed by realists. For them, a virtual resource could not in itself influence or be used to influence the behavior of countries. Thus, it could not be considered as a new type of state power.

This type of conflict would be secondary and of minor importance, according to realists, when compared to conventional warfare, which can be carried out in the physical environment. They even question whether virtual offensive and defensive actions could actually constitute a conflict.

In the realist perspective, this is due to the primacy of the use of physical military means to allow a state to project power over one or more of its potential adversaries, either through the imposition of military defeat or the mere threat of declaring war. Moreover, they question the very use of this term, as well as the designation of war, for any kind of state-to-state interaction that might occur through cyberspace.

The classic realist definition of power, linked to military and other aspects that are related to traditional forms of it, does not allow to consider the existence of its new forms (KREMER; MÜLLER, 2014).

Some realists consider the use of virtual offensive actions to be mere punctual instruments in a traditional war, similar to traditional acts of sabotage. The main focus of these realists emphasizes respect for traditional forms of state power and security, which are traditionally related to their own military might. Thus, the use of cyber means could not be able to replace traditional conflicts nor be used by itself. At most, cyber actions would enhance the conventional type conflict.

Thus, regardless of the possible impacts that cyberspace may have on these aspects, realists do not believe that it is necessary to revise their theories and precepts to understand security in the digital age (JORGE, 2012). Also, according to this author:

> The realists, presumably, would counter the challenge of the information revolution (...). These trends are seen as secondary phenomena, which may affect the domestic policies and structures of states, but which do not weaken the anarchic system of international politics, and thus do not affect the primacy of the state as the supreme political unit. (JORGE, 2012, p. 19, our translation)

In practice, the caveat of cyber realists is that they use a more restrictive definition of the concepts of Security and Power. In theory, these concepts would not allow to include aspects related to cyber space, or other types of threat, that could affect the sovereignty of states in the international arena. For realists, the maintenance and violation of a state's security mainly concerns aspects related to threats from conventional military forces. Therefore, executing these threats by other means deserves less importance in their studies.

However, a change of posture is already noticed in the speech of some realists when the subject is cybernetics. Or, according to Kremer and Muller, there is currently a common tendency for governments to view threats arising or related to cyberspace as challenges related to international and national security (KREMER; MÜLLER, 2014). That is, adherents of realism who wish to apply this theory to try to explain cyber conflicts are beginning to emerge. They believe that the potential that this kind of conflict may have in the future, involving confrontations between states, justifies this application.

Despite all the realists' restrictions on cybernetics, as mentioned earlier, this does not mean that this theory is unable to explain this new reality, or that it may be an inappropriate means to do so. The existence of similarities between the characteristics attributed by the realists to the international environment and the characteristics present in cyberspace, make it possible for realists to consider, in the future, including the study of threats originating in the virtual space as impacting the relationship between states.

It is possible to see this change in posture by Jan-Frederik Kremer and Benedikt Müller when they claim that it would be relevant for realists to study the virtual environment, especially the dynamics of states within it. Moreover, actions taken within or through it may affect the distribution of countries' capacities, their relative power and thus their survival in the International System. In their view, cyberspace would constitute a new arena where states and their interests could collide, including those related to ensuring their own security or weakening a potential adversary.

When analyzing realistic authors who addressed cyberspace, Acácio and Souza concluded that:

> authors who might be associated with Realist thinking regarding cyberspace generally think of this field as a new operational domain for states to act in, where states should project more and more power and gain more and more influence vis-à-vis other states. (ACÁCIO; SOUZA, p. 8, 2012)

In this sense, it appears that other authors face the study of the use of cyberspace to obtain or use any kind of power as a concrete possibility. For them, this environment would allow the existence of a new form of this phenomenon, which has been called Cyber Power, which may be defined as follows:

> Cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain (NYE, p. 3, 2011).

According to Nye, these features include the Internet, networked computers, intranets, radio waves, fiber-optic cables, satellite-based forms of communication, and information and communication technologies (NYE, 2011).

As an example of actions that integrate and allow Cyber Power to be exercised, we can mention the following: cyber-attacks, cyber espionage, cyber sabotage, and cyber conflict. Some recent phenomena allow us to verify that some states are already using one or more of these actions to achieve their own benefits in relation to other countries and through the use of specific actions in cyberspace.

Two examples of cyber activities involving conflict between states, which have been reported in literature, currently refer to the United States, Israel and Iran, and the other to Russia and the Republic of Georgia.

In the first case, the United States and Israel are assigned to sabotage the Iranian nuclear program's uranium enrichment centrifuges in 2010, when a cyber-attack was carried out and resulted in the physical destruction of the centrifuges.

This cyber action would have been carried out in order to avoid the option of military action with the same purpose. It was seen as a less risky and costly action than employing military troops. It has enabled the achievement of a long-standing US political objective, the weakening of Iran's nuclear program. This program was viewed by the US government as a threat to their security and interests (JORGE, 2012).

In the second case, which took place in 2008, a series of cyber-attacks were carried out against Georgia, allegedly by Russia, while these two countries were facing a military conflict.

According to some experts, a first wave of cyber-attacks would have taken place against Georgian communication and information systems shortly before the Russian military campaign began (HAGEN, 2012). During its early days, there was a second wave of attacks, but this time more and more sophisticated (SHAKARIAN; SHAKARIAN; RUEF, 2013; HAGEN, 2012).

This series of attacks interfered with communication between Georgia and the outside world during the conflict with Russia. It has had an impact on Georgians' ability to access and transmit information, effectively isolating them from the outside world (SHAKARIAN; SHAKARIAN; RUEF, 2013; HAGEN, 2012). It also adversely affected the communication systems used by Georgian troops, interfering with their use. This would have made it difficult for these troops to coordinate and act, thereby impairing their performance on the battlefield.

According to some experts, these attacks would also have been part of an intelligence operation. They would have allowed the person responsible for the attack to access computerized government systems and the information stored on them. This would have made it possible to steal and accumulate political and military information stored in these systems (HAGEN, 2012).

Many authors consider that it was used by Russia to support the conduct of its military operations and that it would have been one of the factors contributing to the military defeat of its victim (SHAKARIAN; SHAKARIAN; RUEF, 2013). This case was the first time in history that large-scale cyber-attacks were conducted in conjunction with a major military combat operation, both having the same target (LANGNER, 2016; SHAKARIAN; SHAKARIAN; RUEF, 2013).

The above examples, along with numerous others already reported in literature, might be considered strategic military-cyber operations, and raise the idea that state actors use such an environment as a new alternative to the realist Morgenthausian assumption of demonstration of power (VILAR-LOPES, 2017). Thus, cyberspace may be considered as "a new political arena in which states can act, where they need to, in order to project power and influence over other actors" (FERREIRA et al., 2015, p .03).

These examples point out that, in cyberspace, states would have incentives to seek a certain level of cyber power. The reasons for this concern regard both the possibility of achieving political objectives and increasing the level of their state security. Moreover, the search for cyber power could be due to the perception that this type of power could give comparative advantages over those who do not have such ability, both in the military and in the political field.

Considering the possible threats present in cyberspace, and according to realist thinking, the context of anarchy, also present in cyberspace, may contribute to the states seeking to obtain the capacity to project power in the virtual arena, and this stance may be explained by uncertainty on the intentions of other actors.

Unlike threats in the physical world, there are no physical or natural boundaries in cyberspace. Thus, regardless of the physical distance between two potential enemies, in the virtual arena the information and resulting threats that may flow between them are only seconds away. In this situation, a virtual Security Dilemma is established, in which uncertainty about the real intentions and possibilities of a potential adversary forces states that perceive threats to their interests to take action to increase their own cyber power.

Thus, it can be considered that the behavior of states within cyberspace may be analogous to the one they perform in the International System, within realist conceptions. That is, they are always influenced by the search for increasing their own security and a consequent increase of its power in front of the other actors. This is mainly due to the existence of similarities between the physical and virtual environments, whichever the characteristic of anarchy, leads states to develop their potential to use power and its instruments to subordinate others to their will, so as to minimizing the possibility of having their safety compromised by another actor, as well as influencing a discouragement for cooperation between them.

It is noteworthy that, since the 1990s, the number of countries that have delegated to their Armed Forces the task of protecting them within the cyberspace has been increasing. This is partly due to the belief that these institutions are better structured and have better potential to ensure adequate protection in this area. In this case, and not coincidentally, there has been a persistent discussion about the concept of cyber warfare, of considering virtual aggression as a possible act of war, besides possible responses by states that could be considered legal and appropriate to this type of action.

Thus, the evidence indicates that the cyber issue has affected and influenced the behavior of states in the international system, especially in relation to the search for a cyber power compatible with the state interests to be preserved or conquered. This influence may be explained and analyzed by the realist theory, making this theory a valuable instrument for understanding this new reality involving state conflicts.

FINAL CONSIDERATIONS

It was possible to verify, in relation to the behavior of the states, the existence of significant evidences that they decided, consciously or influenced by other factors, to adopt a similar attitude to the one that they already adopt in the International System, according to the realist approach, regarding the domain and use of cyberspace.

However, an adequate understanding of the actions and consequences for the states, resulting from the Cyber Issue, still depends on further research and reflection on what this phenomenon represents, considering that these activities are recent. In this regard, we highlight the investments and efforts of more advanced countries in the development of advanced technologies related to data transmission and processing, hardware, software, human resources training, research centers, etc. and that may ensure advantages in cyberspace.

However, despite these efforts, the Cyberspace still shows vulnerabilities and, in some way, may pose risks to what states consider essential to their security, that is, the vulnerability of their critical infrastructures to offensive cyber actions by potential opponents. Therefore, the Cyber Issue is also a source of insecurity and of conflicts between states. In this context, the Cyber Issue has become a factor that influences states to constantly search for greater capacity in the cyber area, i.e. obtaining cyber power, both offensive and defensive.

The conflicts originated by the Cyber Issue involving states, and considering the characteristic of "anarchy" in these activities, allows us to have a relationship with what happens with the states within the International System. Thus, it becomes possible to apply realistic logic to the understanding of state conflicts in which cyber activities are present, as well as to understand the logic and behavior of states in the cyber environment.

However, the study showed that realists still offer some resistance to value the activities and consequences related to the Cyber Issue, since they consider that, in the scope and importance that the realist theory attributes to the Military Power, those factors involving the state and the Cyberspace would still be relegated to the background.

The lesson the research offers us is that, at present, obtaining and maintaining a Cyber Power adequate to the threats present in cyberspace is no longer an option, but a requirement against the state interests to be preserved in terms of security and defense, which requires us to deepen our studies and reflections on all aspects related to the Cyber Issue.

A QUESTÃO CIBERNÉTICA E O PENSAMENTO REALISTA

RESUMO

Esta pesquisa teve como objetivo analisar em que medida a teoria realista contribui para explicar a Questão Cibernética e a ocorrência de conflitos virtuais entre os Estados na atualidade. A pesquisa situa-se no contexto de que, nos últimos anos, vários Estados no Sistema Internacional passaram a atribuir às suas Forças Armadas a responsabilidade de Defesa não somente contra ameaças físicas, mas também contra aquelas com origem no espaço cibernético. O que justifica a pesquisa é a contribuição com a literatura existente sobre a temática cibernética que, na atualidade, ainda é relativamente reduzida. O estudo abordou o que caracteriza o conflito e o espaço cibernético, bem como esse fenômeno impacta a percepção de Segurança dos Estados. Foi realizada uma breve revisão sobre o pensamento realista e de suas premissas fundamentais. A conclusão da pesquisa aponta para uma aplicabilidade da lógica realista para a compreensão dos conflitos estatais em que atividades cibernéticas estejam presentes, de modo análogo ao que já ocorre em conflitos convencionais no Sistema Internacional, mesmo existindo uma certa resistência de alguns estudiosos dos conflitos interestatais, adeptos do pensamento realista, quanto à temática cibernética.

Palavras-chave: Questão Cibernética. Realismo. Defesa e Segurança. Estudos Estratégicos.

REFERENCES

ACÁCIO, Igor Daniel P; SOUZA, Gills Lopes M. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?. In: Encontro Anual da Anpocs, 36. Lindóia, São Paulo, 2012.

ARON, Raymond. Paz e Guerra entre as Nações. 1. ed. Brasília: Editora Universidade de Brasília, 2002.

BALDWIN, Stephen. Power and International Relations. In: Carlsnaes, Walter; RISSE, Thomas; SIMMONS, Beth. Handbook of International Relations. 2. ed. London: Sage Publications, 2012.

BAYLIS, John; WIRTZ, James. J. Introduction. In: BAYLIS, John; et al. Strategy in the contemporary world: an introduction to strategic studies. 1. Ed. Oxford: Oxford University Press, 2002.

CANADA. Sécurité publique Canada. Stratégie nationale sur les infrastructures essentielles, Ottawa, 2009. Available at: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-fra.pdf. Access on: Jan. 20, 2017.

CAPLAN, Nathalie. Cyber War: the Challenge to National Security. Global Security Studies, v. 4, n. 1, p. 93-115, 2013.

CARR, Edward Hallett. Vinte anos de crise: 1919-1939 - Uma Introdução ao estudo das Relações Internacionais. 2. ed. Brasília: Editora Universidade de Brasília, 2001.

CAVELTY, Myriam Dunn; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia. Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. 1. ed. Hampshire: Ashgate Publishing, 2007.

CAVELTY, MyriamDunn; MAUER, Victor; KRISHNA--HENSEL, Sai Felicia. The militarization of Cyberspace: why less may be better. International Conference on Cyber Conflict, 4. 2012.

CRAIG, Anthony J. S; VALERIANO, Brandon. Realism and Cyber Conflict: Security in the Digital Age. In: ORSI, David E; AVGUSTIN, J. R; NURNUS, Max. Realism in practice: an Appraisal. 1. ed. S.l: E-International Relations, 2018.

DAHL, Robert A. The Concept of Power. Behavioral Science, v. 2, n. 3, p.

201-2015, jul. 1957.

FIGUEIREDO, Eurico de Lima. Estudos Estratégicos como Área de Conhecimento Cientifico. In: Revista Brasileira de Estudos da Defesa, v. 2, n. 2, p. 107-128, jul. 2015.

JANCZEWSKI, Lech J; COLARIK, Andrew M. Cyber Warfare and Cyber Terrorism. Hershey, PA: IGI Global, 2008.

JORGE, Bernardo Wahl Gonçalves de Araújo. Das "Guerras Cibernéticas". In: Anais do XI Ciclo de Estudos Estratégicos: Segurança e Defesa cibernética. Rio de Janeiro, 2012.

KRAMER, Franklin D; STARR; Stuart H; WENTZ, Larry K. Cyberpower and National Security. 1. ed. Washington: Potomac Books, 2009.

KREMER, Jan-Frederik; MÜLLER, Benedikt. Cyberspace and International Relations: Theory, Prospects and Challenges. Ed. 1. New York: Springer, 2014.

LAKE, David A. The State and International Relations. In: Reus-Smit, Christian; Snidal, Duncan. The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2008.

MANESS, Ryan C; VALERIANO, Brandon. The Impact of Cyber Conflict on International Interactions. Armed Forces & Society, v. 42, n. 2, 2016.

MILLMAN, Rene. Nation state cyber-attacks on the rise: detect lateral movement quickly. SC Media UK, 2018. Available at: https://www.scmagazineuk.com/nation-state-cyber-attacks-on-the-rise--detect-lateral- movement-quickly/article/746561/. Accessed on: Apr. 11, 2018.

MORGENTHAU, Hans J. A política entre as Nações: A luta pelo poder e pela paz. Brasília: Editora da Universidade de Brasília, 2003.

NYE JR, Joseph S. Power and National Security in cyberspace. In: LORD, Kristin M; SHARP, Travis. America's Cyber Future: security and prosperity in the information age. Washington: Center for a new American study, 2011.

REARDON, Robert; CHOUCRIL, Nazli. The Role of Cyberspace in International Relations: A View of the Literature. In: ISA Annual Convention, 5. San Diego, California, 2012.

RIBEIRO, Vinicius G; RIVERA, César G. A inserção da segurança cibernética na agenda de segurança dos EUA no Século XXI. Século XXI, v. 5, n. 2, p. 135-150, 2014.

SHAKARIAN, Paulo; SHAKARIAN, Jana; RUEF, Andrew. Introduction to cyberwarfare: a multidisciplinary approach. Waltham: Elsevier, 2013.

SHELDON, John B. Deciphering Cyberpower: strategic purpose in peace and war. In: Strategic Studies Quarterly, v. 5, n. 2, p. 95-112, 2011.

TABANSKY, Lior. Basic Concepts in Cyber Warfare. Military and Strategic Affairs, v. 3, n. 1, p. 75-92, 2011.

VILAR-LOPES, Gills. Relações Internacionais cibernéticas (CiberRI): o impacto dos estudos estratégicos sobre o ciberespaço nas Relações Internacionais. In: Congresso Latinoamericano de Ciência Política, 9. Montevideo, 2017.

WALTZ, Kenneth J. O Homem, o Estado e a Guerra: uma análise teórica. 3. ed. New York: Columbia University Press, 2001.

WENDT, Alexander. Anarchy is what States make of it: the Social Construction of Power Politics. International Organization. v. 46, n. 2, p. 391-425, 1992.

WOHLFORTH, William C. Realism. In: REUS-SMIT, Christian; SNIDAL, Duncan. The Oxford Handbook of International Relations. Oxford: Oxford University Press.