10.21544/2359-3075.v28n2.d

# INTERNATIONAL LAW AND THE CYBER DEFENSE OF SOVEREIGNTY IN THE BLUE AMAZON: AN APPROACH IN THE LIGHT OF THE TALLINN 2.0 MANUAL

Alexandre Peres Teixeira[1]
Liziane Paixão Silva Oliveira[2]

**SUMMARY**

The first Tallinn Manual on International Law Applicable to Cyber Operations was published in 2013 and only referred to wartime cyber operations. The second Manual, published in 2017, also considered cyber operations carried out in peacetime. Given the importance of regulating cyberspace for naval warfare, this article aimsto analyse the rules suggested by the emerging International Law Applied to Cyber Operations, for activities carried out in the context of naval operations. In this way, the research employs the bibliographic review method, based on primary and secondary sources, such as the UN Group of Governmental Experts (UNGGE) report, the Tallinn Manual
2.0 and scientific articles on the subject. It is worth noting that the Tallinn Manual 2.0 promoted the meeting of the emerging International Law Applicable to Cyber Operations with the consolidated law of naval warfare. This encounter generates legal insights that must be evaluated with extreme care.
Keywords: International Cyber Law; Cyber Warfare; Naval Operations.

[1] Graduate Program of the Centro de Ensino Unificado de Brasília (UNICEUB), Brasília -DF, Brazil. E-mail: alexandreperes@yahoo.com.br - ORCID https://orcid.org/0000- 0002-5349-8039..

[2] 2 Graduate Program of the Centro de Ensino Unificado de Brasília (UNICEUB), Brasília -DF, Brazil. E-mail: lizianepaixao@outlook.com - ORCID http://orcid.org/0000-0002- 6266-6073.

## INTRODUCTION

With the growing dependence of states on the technical-scientific informational environment[3] , the cyber dimension has also come to be used for harmful interactions between them, as well as between non-state actors and states, and consequently as a tool for geopolitical confrontations, which exacerbate the simple geographical bias and have a strong influence on the various manifestations of state power. The phenomenon of globalization[4] has served to exacerbate these interstate movements.

For Saldan (2012), international peace and security and the political/legal/institutional stability that comes from them are the pillars for improving and exercising human rights (HR), fundamental freedoms, the self-determination of peoples and the political/economic/social/cultural development of societies. Therefore, the dynamics of International Relations are governed by diplomatic and legal rules, built up over the course of history, with the intention of promoting peaceful coexistence between peoples and seeking peaceful ways of resolving disputes.

As the oceans have always been a determining environment for the geopolitics of the planet, with the arrival of the information age came the possibility of this geographical space becoming ripe for malicious cyber actions against the sovereignty of coastal states.

In the case of Brazil, with its immense coastal area known as the "Blue Amazon"[5], the planning of a cyber defense capable ofdeterring any actor intent on attacking Brazilian sovereignty through the use of cyber warfare is of fundamental importance.

However, to what extent can cyber defense actions be carried out

3 The concept of the technical-scientific information environment is related to the process of spatial formation and integration brought about by digital techniques, as well as the way in which it modifies space. PENA, Rodolfo Alves. Information age. Mundo Educação, 2013. Available at: http://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Accessed on: Feb. 12, 2020.

4 On the changes to the elements of the classic concept of sovereignty read: OLIVEIRA, Liziane Paixão Silva. Sovereignty in the face of globalization. Revista do Programa de Mestrado em Direito do UniCEUB, Brasília, v. 2, n. 1, p. 202-225, jan./jun, 2005.

5 According to Vidigal (2006, p. 18), the Azure Amazon is the Atlantic expanse that protrudes into the Amazon.
Beyond the coastline and oceanic islands, and corresponding to around half of Brazil's surface area, it has been called the Blue Amazon. Blue because it compares to Green because of its size and biodiversity. VIDIGAL, Armando Amorim Ferreira; BOAVISTA, Marcílio. Blue Amazon: the sea that belongs to us. Rio de Janeiro: Record, 2006.

on the basis of international law? Even though this is an extremely new topic, can it be considered that there is already a legal basis that regulates cyber operations carried out between states in maritime environments?

With regard to the initial work that may one day result in standardization, the publication of the Tallinn Manual 2.0 on International Law Applied to Cyber Operations[6] in 2017, as well as the 2013 Tallinn Manual, represent a first step on the road to the formation of an international doctrine capable of inspiring the various legal systems around the world.

The result of NATO's efforts to pacify the use of cyberspace, these Manuals are the first sources of organized international legal doctrine dealing with operations in the cyber domain. Although they are not mandatory, they have the legal nature of soft law and have the potential to influence the practice and opinio iuris of states, in the context of a legal framework that is beginning toform around this important issue. With regard to Naval Operations in a situation of armed conflict,

the Tallinn Manual 2.0 states that the parties to a conflict do not lose their rights as the flag state[7] of a ship, coastal state or port state, nor are they released from their duties and obligations under international law, except in cases where the provisions of the United Nations Convention on the Law of the Sea (UNCLOS), as lex generalis, are overridden by the rules of the International Law of Armed Conflict (ILAC), which constitute lex specialis for times of war, many of which are described in the San Remo Manual of International Law Applicable to Armed Conflicts at Sea[8] .

---

6 According to Stockburger (2016), the International Committee of the Red Cross (ICRC) understands "cyber operations" as those that are carried out against or from a computer or computer system, that are carried out by means of a data flow, that are intended to perpetrate specific actions, such as infiltrating data systems to collect, export, destroy, alter or encrypt data or to trigger, alter or manipulate processes controlled by the infiltrated computer system. STOCKBURGER, Peter Z. (2016) Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum. American University International Law Review, v . 31, n. 4, 2016. Available at: https://digitalcommons.wcl.american. edu/auilr/vol31/iss4/2/. Accessed on: Feb. 22, 2020.

7 State in which the ship or vessel is registered (CNUDM, art. 91).

8 The San Remo Manual is an international law document prepared with coordination of the Institute of International Humanitarian Law in San Remo in 1994, which deals with the rules for armed conflicts at sea. INTERNATIONAL INSTITUTE OF HUMANITARIAN LAW. Sanremo Manual. Sanremo, Italy, 1994. In: INTERNATIONAL LAW RELATING TO THE CONDUCT OF HOSTILITIES: Compilation
of the Hague Conventions and certain other legal instruments. Geneva: International Committee of the Red Cross - ICRC, 2001.

According to Ribeiro (2013), the United Nations Convention on the Law of the Sea (UNCLOS) standardized the criteria used to delimit the jurisdiction of states in the maritime environment, and is directly related to the expansion of the sovereign rights of coastal states (RIBEIRO, 2013, p. 270).

Although the UNCLOS refers more specifically to a peacetime approach, it also applies to situations of armed conflict. This is done in accordance with the 1994 San Remo Manual, which sets out the rules for war at sea. These rules must be observed between belligerents and between belligerents and neutral states.

For Brazil, which has an immense coastline, the task of taking care of the defense of national assets located in the maritime environment has always been a concern of the Na vy. The sea, with its potential to give rise to disputes for the most varied interests, "inspires care to be translated into concerns about security and defense" (REIS, SANTOS, 2014, p. 216). Thus, not only adherence to international standards, but also the dissemination of such standards to defense operators is of paramount importance for the country's deterrence efforts.

In relation to the international legal norms contained in the UNCLOS, although there are a few differences[9] of interpretation on the part of Brazil, these differences are not sufficient to be exploited in order to disturb Brazilian sovereignty in its jurisdictional waters. However, not just for Brazil, but for many coastal states, the construction of rules that equalize the commands of the UNCLOS with the peculiarities of cyber operations are still a new area, in which it is necessary to building conviction in relation to its content.

The information age has also caused disruption in maritime affairs. There is no doubt that the Information Age has greatly changed the dynamics of the use of the seas, as well as combat at sea. Today's private or state-owned ships are increasingly well-served by technology for the control and maintenance of their propulsion, navigation and combat systems.

9 There are provisions in UNCLOS that give rise to different interpretations. For example, Brazil believes that the innocent passage of warships must be notified in advance to the coastal state, and that military exercises in the Exclusive Economic Zone require prior authorization from the coastal state. These positions are not accepted by the international community. Likewise, some governments believe that the UNCLOS does not prohibit scientific research for military purposes in the EEZ of other states. These are just a few examples of controversies, among others, that may come to cloud sovereignty or sovereign rights in Brazilian jurisdictional waters.

According to Fahey (2017), approximately 87% of the merchant shipping fleet relies on the Global Navigation Satellite System (GNSS), a technology that makes merchant ships "easy targets" for attacks[10] cyber, due to the weak signals used by such systems, which do not have encryption or authentication[11]. The author goes on to say that "cyber vulnerabilities in the maritime domain are expanding at an alarming rate, and, unfortunately, proficiency in protecting against these vulnerabilities is at an extremely slow pace". (FAHEY, 2017, p. 2)

While networked computing and satellite navigation systems offer tremendous advantages to the Naval Forces and the commercial transportation sector, they also create potential vulnerabilities, which often evolve faster than the ability to combat them.

The advance of technology has brought comfort, security and sophistication to the maritime environment, but it has also brought enormous vulnerabilities, which can be exploited both in peacetime and in times of armed conflict. Thus, a perfect understanding of the emerging international legal basis for operations in cyberspace is extremely important if we are to be able to cope with this scenario.

The purpose of this article is to identify and analyze specific points of the Law of the Sea and naval warfare, from the perspective of the emerging International Law Applied to Cyber Operations, addressed by the recently created Tallinn Manual 2.0. In order to place the reader in the state of the art of the debate on the genesis of International Cyber Law, it will be necessary to briefly contextualize the concept of sovereignty from the perspective of this newest branch of Public International Law.

In this way, the suggested approach will contextualize the broader aspect of state sovereignty, with reference to the Westphalian paradigm, referring to an analysis of the reflections of the grey areas created by the Tallinn Manual 2.0, which are related to the exercise of this sovereignty, especially in what affects naval warfare. By addressing the points of convergence between maritime law, International Law of Armed Conflicts

10 BHATTI, Jahshan; HUMPHREYS, Todd. Hostile control of ships via false GPS signals: Demonstration and detection. In Viga Tion: Journal of the Institute of Navigation, v. 64, n. 1, p. 51-66, 2017.

11 As a result, GNSS systems are susceptible to "spoofing" - false signals sent to the ship's GNSS receiver, usually via a software-defined radio receiver (SDR), designed to disrupt or misdirect navigation. This vulnerability is not merely speculative. FAHEY, Sean. Combating "cyber fatigue" in the maritime domain. Washington, Humanitarian Law & Police, 2017, p. 3. Available at: https://blogs.icrc.org/law-and-policy/2017/12/07/combating_cyber-fatigue-in-the- maritime-domain/. Accessed on: Feb. 22, 2020.

at sea and the emerging International Cyber Law, the work also aims to contribute to the debate related to the use of cyberspace in the context of naval operations. In the first section of the article, the paradigm of state sovereigntyand its weakening in the Information Age will be briefly discussed. The first section of the article will briefly discuss the paradigm of state sovereignty and its weakening in the Information Age; the second section will analyze some of the concepts intheUnited Nations Convention on the Law of the Sea (UNCLOS) and their relationship with the Tallinn Manual 2.0; the third section will discuss the concepts of Naval Warfare and their correspondence in the emerging International Law Applied to Cyber Operations; and finally there will be a brief conclusion.

## THE PARADIGM OF STATE SOVEREIGNTY AND ITS WEAKENING IN THE INFORMATION AGE

### *The weakening of the Westphalian paradigm:*

The Information Age has brought with it conflicts whose characteristics challenge international law. Cyberspace is currently presenting itself as a new dimension for relations between states. Some actions that take place in the information environment have the potential to generate aggression and interference in state sovereignty.

Onuf (1991) believes that the evolution of the concept of sovereignty, in order to meet the increasingly complex demands of international relations, has meant that this concept has gradually become more difficult to understand. For his part, Watts (2018) states that applying the concept of sovereignty in a manner coherent and well-founded, has proved to be an immensely difficult task. For both authors, this difficulty has been aggravated in contexts that lack deeply rooted standards or those established by state practice, especially with regard to the territoriality enshrined in the Westphalian paradigm[12]. Unlike physical borders, the cyber dimension of a state has no borders, and this affects the old criteria

12 Ferreira (1958) says that the notion of state sovereignty is closely linked to the notion of the emergence of the state. For most of the Doctrine, the constitutive elements of the Stateare: the People, Sovereignty (or political power, for some) and the Territory. According to the Westphalian paradigm, territory is the material evidence for the exercise of sovereignty by the state. This has been one of the most respected paradigms, both for the construction of the complex international system and for the consolidation of national legal systems. See: FERREIRA, Pinto. Teoria Geral do Estado. 2. ed. expanded and updated. São Paulo: José Konkino Editor, 1958, Volume I.

established for evidence of state sovereignty and jurisdiction. In this way, understanding the classic concept of the state's territorial sovereignty becomes important in order to see the complexity related to adapting this concept to the nuances that accompany the operations carried out in cyberspace.

Celso D. de Albuquerque Mello said that one of the elements of a state is its territory. "The territory is where the state exercises its sovereignty, within the limits established by international law." In this way, the author concludes that "the notion of territory isnot geographical, but legal, since it is the domain of validity of the legal order of a given sovereign state" and this will be the starting point for characterizing the physical and terrestrial portion of a state. Territoriality or "territorial existence" has been a fundamental point for understanding the existence of the state. (MELO, 1992, p. 50)

Identifying a violation of sovereignty based on the use of physical territorial boundaries is much easier than doing so when the violation occurs through a malicious cyber operation. Margulies (2013) believes that "international law, which addresses state accountability for kinetic attacks in the real world, is inadequate to addressstate responsibility for cyber attacks". Not only because of the difficulty of detecting and attributing external cyber attacks, but also because of the ease with which the attacker can covertly control them. (MARGULIES, 2013, p. 2)

For Watts (2018), one of the most difficult and pressing issues of the ongoing effort to adapt international law to the areas

One of the most important questions emerging from international relations is how territorial sovereignty should be considered "in the interconnected, still diffuse; virtual, still material; new, still omnipresent world of cyberspace". Even divorced from the unique and legally challenging context of cyberspace, territorial sovereignty is an extremely complex and enigmatic subject in the realm of international law. "Although it is axiomatically fundamental to almost every subject and rule of international law, the precise legal importation of the concept of territorial sovereignty from the real world to the virtual world becomes frustratingly complicated, contextual and illusory," Watts goes on to say (WATTS, 2018, p. 812).

In fact, cyberspace presents itself as a context in which the application of the principle of sovereignty becomes very difficult, as states offer a confusing array of behaviors, as well as countless justifications for

conduct that occurs in the grey areas that separate legality from illegality, especially those related to territorial sovereignty. In this way, various lines of thought are emerging in response to questions regarding the adequacy of the concept of sovereignty and its application in cyberspace.

Stockburger (2016) believes that one of the biggest challenges facing states in the cyber environment "is that the scope and manner of applicability of international law to cyber operations, whether offensive or defensive, has remained unstable since their advent". Thus, for the author, "there is a risk that cyber practice will quickly distance itself from the agreed understandings of its legal regime". (STOCKBURGER, 2016, p. 549)

For Michael N. Schmitt[13] , general editor of the Tallinn Manual 2.0, "it has become common to characterize cyberspace as a new dimension of war, devoid of international law and subject to catastrophic abuse" and in this terrain the actions of states and non-state actors appear as a major threat, both to international security and peace, and to the internal public order of states. (SCHMITT, 2017a, p.7)

Although it is a topic that has only recently entered the international security agenda, the destructive potential of current cyber threats has already been seen in some concrete cases, such as the cyber-attack suffered by Estonia in 2007; Operation Orchard[14], carried out by Israel in 2007; the Russo-Georgian war[15], in 2008;

the Stuxnet virus[16], which infected an Iranian nuclear power plant

13 Professor of International Law, University of Exeter, Coordinator of the Stockton Center for the Study of International Law, Professor at the U.S. Naval War College; Francis Lieber Distinguished Scholar, West Point Military Academy. Author and Project Director of the Tallinn Manual from 2009 to 2017.

14 In September 2007, Israel carried out an air strike on Syria to bomb an alleged nuclear power plant that was to be built with North Korea; the Israeli government allegedly infiltrated Syria's air defense system, because Israeli planes were not detected by radars, which possibly occurred due to the use of specific programs to circumvent Syrian traffic control systems, which transmitted false signals (Idem, 2012, p. 71).

15 In August 2008, just before the Russian army invaded Georgia, a cyber attack allegedly damaged Georgia's military IT systems, including air defense. See: SHACKELFORD, Scott. Estonia Two-and-A-Half Years Later: a progress report on Combating Cyber Attacks. Journal of Internet Law, Forthcoming, 2009. Available at: https://ssrn.com/abstract=1499849. Accessed on: Feb. 17, 2020.

16 In October 2010, the "Stuxnet" virus, supposedly developed by the Israeli and American governments, was infiltrated, possibly via a USB stick, into the systems of the Bushehr nuclear reactor in Iran, built by Russia, with the aim of rendering centrifuges unusable by increasing their rotation, while normality signals were sent to control. The episode affected the Iranian nuclear project and is therefore widely reported as a kind of cyber warfare attack. The Russian computer security company Kaspersky Labs said in December 2011 that Stuxnet could be the first in a series of cyber weapons (SALDAN, op. cit., p. 72).

in 2010; the hacker attack on Sony Pictures[17] in 2014; the accusation of a breach of President Dilma Rousseff's emails[18] in 2015 by the US National Security Agency (NSA); and the cyberattacks suffered by the United States of America (USA) in 2015 and 2016, which had a strong influence on the 2017 presidential elections[19].

Even against this backdrop, efforts to consolidate legal and technical concepts that can deal with these new threats are still moving very slowly. This is because the operations carried out in cyberspace go beyond conventional geographical boundaries, despite the fact that their physical and logical structures, as well as the operators "are housed in different jurisdictions, interacting in a relationship of interdependent structures whose dynamics do not follow a relationship between physical space and virtual or cyber space" (SALDAN, 2012, p. 27).

The phenomenon, known as cyber warfare[20], became better

17 In 2014, a group of hackers launched a cyberattack on Sony Pictures Entertainment and released, among other things, personal information about the company's employees, including email correspondence and information about executive salaries. HABER, Eldar. The Cyber Civil War. 44 Hofstra Law Review 41, 2015. Available at: https://ssrn.com/abstract=2699644. Accessed on: Feb. 17, 2020.

18 Edward Snowden's leaks, published by many different media outlets around the world, have shown that people's most basic rights may have been continually violated, especially the right to privacy and freedom of expression. It was revealed that the NSA (the agency responsible for electronic surveillance in the USA) had accessed the emails of the then President of Brazil, Dilma Rousseff. See: MONTEIRO, Renato Leite. The Balance between Freedom and Security in the Age of Surveillance: a Brief Analysis of the Recent Intelligent ElectronicSurveillance Scandals. SSRN, 2014. Available at: https://ssrn.com/abstract=2468060. Accessed on: Feb. 13, 2020.

19 In 2015 and 2016, hackers affiliated with the Russian government broke into the servers of the US Democratic National Committee (DNC). The subsequent release of documents damaged the Democrats in the congressional elections, which led to the resignation of the DNC chairman, created tension between Clinton and Sanders supporters and, above all, prominently affected the presidential race. The Russian operations were yet another example of Russia's efficiency in exploiting the "Gray Zones" (ZC) of International Law (IL). SCHMITT, Michael. Grey Zones in the International Law of Cyberspace. Yale Journal of International Law, v. 42, p. 1-21, 2017a. Available at: https://www.yjil.yale.edu/grey- zones-in-the-international-law-of-cyberspace/. Accessed on: Feb. 13, 2020.

20 Raboin (2011) already stated that cyber warfare would change the inherent nature of war itself, defending the conceptual idea that cyber warfare would not only change the armaments of modern warfare, but that it would represent a radical change in the nature of the battlefield. RABOIN, Bradley. Corresponding Evolution: International Law and the Emergence of Cyber Warfare. National Association of Administrative Law Judiciary,
v. 31, n. 2, 2011. Available at: http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5

Accessed on: 17 Feb. 2020, p. 604.

known to the general public after 2007, when Estonia was the victim of a sequence of coordinated and systematic cyber attacks against its critical public and private infrastructures, affecting the lives of millions of people in that country. This followed a controversy involving the relocation of Russian soldiers' bodies and a Russian World War II monument.

The attack was attributed to the Russian government and is one of the first[21] cyber warfare incidents recorded on the planet, according to the Tallinn Manual 2.0, involving sovereign states. As a result of this critical event, the North Atlantic Treaty Organization (NATO) established the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) in Tallinn.

One of the first activities of the NATO CCD COE group of international experts was to carry out a detailed study of how international law could regulate the notion of "use of force" when it is employed by states in cyber operations that take place during an international armed conflict. The result of this initial work was the publication of the Tallinn Manual in 2013.

Following the publication of this first manual, the group of experts set out to study, from the point of view of intentional law, the use of cyber operations, not only in the context of armed conflicts, but also in peacetime. Thus, in 2017, the NATO CCD COE, in partnership with Cambridge University, published the Tallinn Manual 2.0, which, in addition to the studies listed in the first manual of 2013, also includes an approach to cyber operations carried out by states in peacetime, thus covering topics such as Space Use Law, Human Rights, Maritime Law, Diplomatic Law, among other topics related to peacetime.

The production process[22] of this manual followed the same lines as the 1880 Oxford Manual on International Law applied to Land Warfare; the 1994 San Remo Manual on International Law applied to Naval Warfare; and the 2009 Harvard Manual on International Law applied to Air and Missile Warfare.

21 There is a record in the literature that the first attack also originated in Russia and targeted the USA in 1982. See: RICHARD, Clarke; KNAKE, Robert. Cyber war: the next threat to national security and what to do about it. New York: Ecco; Reprint edition, 2010, p. 92; MCLAUGHLIN, Stephen, et al. The cybersecurity landscape in industrial control systems. Proceedings of the IEEExplore, v. 104, n. 5, p. 1039-1057, 2016.

22 SCHMITT, Michael. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017b, p. 1.

For the 2017 manual, an international legal base[23] was considered, comprising 54 treaties, 51 concrete cases and 58 different sources, including articles, reports from UN expert groups and manuals on international law.

The Tallinn Manual 2.0 is divided into four parts. Part I deals with general issues of international law and cyberspace. Part II covers specialized regimes of international law and cyberspace. Part III concerns international peace and security and activities in cyberspace, drawing mainly from the Tallinn Manual 1.0. And Part IV is the remainder of the Tallinn Manual 1.0, which deals with the International Law of Armed Conflict as applied to cyber operations[24].

Currently, the Tallinn Manual 2.0 stands as the most recent work of systematized doctrine on International Cyber Law. Far from being considered a binding document, the manual raises important questions about the areas of international law that are exploited by states that are notorious for carrying out malicious cyber operations. These areas are referred to as the "gray zones of international cyber law".

In fact, applying the principle of sovereignty in cyberspace becomes difficult due to the diversity of states' actions in these zones of the emerging International Cyber Law. In view of this complexity, several scholars have embarked on an analysis of questions relating to the adequacy of the concept of sovereignty and its application in cyberspace. For Johnson and Post (1998), "initial academic attention has addressed the fundamental question of the general relevance of sovereignty to cyberspace, especially whether cyberspace can be considered a post- Westphalian domain," which will have to be reinvented to meet the demands of the information age (Johnson and Post 1996, 1370).

## ***Gray areas of international cyber law and sovereignty:***

As already mentioned, the Tallinn Manual 2.0 can be considered the first source of international cyber law doctrine, alongside the reports issued by the UN Group of Governmental Experts on Information Technology (UM GGE). In this way, the Manual has the potential to guide cyber operations carried out by all the states that make up international society, especially with regard to the construction of international treaties, conventions and bilateral agreements on the subject. In this way, resolving

23 SCHIMITT, 2017b, p. i to v.

24 Id., p. v to xi.

the hermeneutical controversies that exist in the Manual is an important task for the consolidation of International Cyber Law.

A careful reading of the Tallinn Manual 2.0 reveals that, on several occasions, the group of experts did not reach a consensus on the scope of application of certain rules. This has led to what Schmitt (2017) calls the gray areas of the Tallinn Manual 2.0. These zones are, in practice, the differences in understanding and interpretation of certain rules that arose between experts from different European countries during the process of building the Manual.

Mentioning the complex problem related to the gray areas of the Manual, Schmitt (2017) cites the US elections[25] of 2017 as an example, stating that they suffered a serious influence on the outcome as a result of malicious cyber operations perpetrated by Russia. According to him, Russia took advantage of the gray areas of the Tallinn Manual 2.0 to influence the outcome.

directly in the exclusive and inherent functions of the US, carrying out something that, in the light of the Tallinn Manual 2.0, can be considered an illicit intervention.

The main gray areas of the Tallinn Manual 2.0, in Schmitt's (2017) assessment, are related to the concept of sovereignty, because according to an approach by some officials[26] of the US Department of Defense ( DoD), "sovereignty would only be a fundamental principle that does not generate any primary rule in international law" so tha t , in the view of these officials, "there is no prohibition on violating the sovereignty of another state" through a cyber operation. For these officials, "a state's cyber operations are only likely to violate other primary rules of international law, such as 'non-intervention' or the 'prohibition on the use of force'". (SCHMITT, 2017a, p. 5)

It is a well-known fact that sovereignty has both an internal and an

25 Through this strategy, Russia exploits principles and rules of IHL that are poorly demarcated or subject to competing interpretations. In doing so, Russia has drawn attention to the complex issues of state responsibility in relation to the actions of non-state actors, and to the related issue of the control of these actors, which, in the view of international humanitarian law (IHL), can internationalize an IAC. (SCHMITT, op. cit., 2017a, p. 1).

26 More precisely by Gary P. Corn and Robert Taylor , authors of the article "Sovereignty in the Age of Cyber". See: CORN, Gary; TAYLOR, Robert. Sovereignty in the age of cyber. In: THE AMERICAN SOCIETY OF INTERNATIONAL LAW. Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0, v. 111, 2017, p. 207-212. Available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70. Accessed on: May 10, 2020.

external component. The notion of internal sovereignty refers to a state's right to exercise control over people, including legal persons, objects and activities on its territory. For Schmitt (2017), it is indisputable that "this right extends to control over individuals involved in cyber activities, cyber infrastructure located in a state's territory and any cyber activities that take place within or through that territory". (SCHMITT, 2017b, p. 12)

External sovereignty, by contrast, refers to the right of states to engage in international relations, as in the case of diplomacy and the conclusion of international agreements. For example, in the exercise of external sovereignty a state is free to become, or not, a party to a treaty regulating cyber activities. Such sovereignty is also the basis for states' legal immunity. As with internal sovereignty, contesting the existence of external sovereignty is not in question.

Schmitt (2017) goes on to say that there are two important gray areas regarding the concept of sovereignty from the point of view of cyber operations. The first revolves around the argument that "sovereignty is only a fundamental principle that does not generate any primary rule of law".

International". Still according to the author, this approach of "sovereignty as a principle, but not a rule" contradicts the extensive practice of states and opinio juris[27], in the non-cybernetic context, which treats the prohibition of violating the sovereignty of others as a primary rule, in such a way that such a violation would constitute an internationally illicit act.

In a different direction, some scholars such as Corn and Taylor (2017) claim that the nature of cyberspace is incompatible with traditional concepts of geography. It is difficult to define the limits of internal and international space, and to identify the "exact role that the principle of sovereignty plays in the cyber activities of regulatory states" (Corn and Taylor 2017, 207).

The second gray area, from the point of view of state sovereignty, relates to remote cyber operations carried out outside the target state. According to a minority view of the Tallinn Manual 2.0, only malicious operations that generate physical[28] damage in the target state could be considered capable of violating sovereignty.

27 opinio juris is an indispensable element for a given practice to be repeated by states becomes recognized as an international customary norm.

28 The experts who wrote the Manual correctly understood that there is "little practical difference between physical damage to property and rendering it practically inoperable" (SCHMITT, 2017a, p. 3).

For Schmitt (2017), there is no doubt that a remote cyber operation, causing physical damage or injury on the territory of another state, violates the sovereignty of the latter, since the well-accepted notion of territorial integrity and inviolability is at its height when physical consequences manifest themselves. However, most of them concluded that the definitive loss of functionality of cyber infrastructure can also be considered a violation of state sovereignty, even if no physical damage occurs (SCHMITT, 2017a, p. 3). Therefore, both loss of functionality and physical damage, for the Tallinn Manual 2.0, can serve as evidence of a violation of state sovereignty through the execution of a cyber operation.

It is therefore important to understand all the controversy surrounding the concept of sovereignty, in order to move forward and see that, even in the face of controversial points and gray areas, the legal framework has been built that attempts to regulate the use of cyber operations between states, both in times of peace and in times of war, as is the case with naval warfare, which we will discuss later.

In short, when it comes to cyber operations, according to the principle of sovereign equality between states, states are free to make their own decisions. Therefore, the state affected by a malicious cyber action, if it decides to take some action in retaliation, must inform what action it will take. But according to rule[29] 4 of the Tallinn Manual 2.0, sovereignty is characterized as a primary rule and not as a fundamental principle that is capable of supporting primary rules, such as the duty of non-intervention and the right to self-defence. In this way, the Tallinn Manual 2.0 indicates that sovereignty is a "rule of law" from which no derogation is permitted, increasing attention to its non-violation and the importance of understanding what would characterize a violation (Ghappour 2017, 225).

In fact, the application of a "principle of sovereignty" in cyberspace is difficult due to the diversity of states' actions in the gray areas of emerging international cyber law. Because of this complexity, various scholars have embarked on an analysis of the issues relating to the adequacy of the concept of sovereignty and its application in cyberspace. For Johnson and Post (1998), "initial scholarly attention has addressed the fundamental question of the general relevance of sovereignty to cyberspace, especially whether cyberspace can be considered a post- Westphalian domain,"

29 "**Rule 4 - Violation of** sovereignty**: A state must not conduct cyber operations that violate the sovereignty of another state**" (SCHMITT, 2017b, p. 17).

which will have to be reinvented to meet the demands of the information age (Johnson and Post 1996, 1370).

Understanding the new movements in international law is extremely important, since the process of building the legal basis that can regulate the use of cyberspace can be permeated by geopolitical interests, requiring states to be diligent so that their interests are not affected by biased legislation. For the context of naval warfare, this is extremely relevant, since the characteristics that accompany the use of a state's naval power make naval combat an efficient vector for cyber warfare.

## POINTS OF CONVERGENCE BETWEEN THE CNUDM AND THE TALLINN 2.0 MANUAL

This section discusses the main articles of the Tallinn 2.0, which relate to UNCLOS. The UNCLOS concepts covered here, although established for non-war situations, are fundamental to understanding the recently created rules that seek to adapt International Law applied to Cyber Operations to situations of armed conflict at sea.

It should be noted that the rules of the Tallinn Manual 2.0, which refer to UNCLOS, constantly allude to the specific situation of naval warfare, referring to the San Remo Manual.

For Brozoski (2019), a phenomenon that has intensified in the ongoing transformations in the international system is the expansion of states over the seas. According to the author, "the dispute over access to sources of energy and mineral resources and the competition for control of the main international shipping routes continue to form the core of the global competition for power, and today they cover maritime space more incisively" (BROZOSKI, 2019, p.77). In this sense, it is unquestionable that the maritime environment is fertile territory for geopolitical confrontations. Brozoski 2019 goes on to say the following:

> As well as having an extensive maritime jurisdiction rich in natural resources - such as the immense oil deposits in the Pre-Salt - Brazil also hasaremarkable technological wealth for exploiting these riches. If, on the one hand, having the science and technology to exploit these assets is an advantage for

> development and autonomy, on the other hand it is also an additional element that encourages the projection of foreign interests over the country. In our view, understanding Brazil's position on the global geopolitical chessboard today necessarily requires understanding the nuances and effects of the ongoing process of territorialization of maritime spaces, both regionally and internationally. All over the world there have been great efforts to incorporate the oceans into the national legal apparatus. There is a growing and widespread understanding that public policies aimed at industrialization, economic growth and Defence and Security must include the seas more forcefully in their agendas (BROZOSKI, 2019, p.82).

On the way to bringing the national context that encompasses the "Blue Amazon" into line with the national and international legal apparatus, the Law of the Sea[30] provides normative guidance on operations that are carried out at sea or launched from there against territorial spaces. The International Group of Experts (GIP), which worked on the construction ofthe Tallinn Manual 2.0, agreed that the Law of the Sea applies to cyber operations carried out from or through cyber infrastructure located at sea.

Cyber operations can be carried out by ships and submarines (hereinafter collectively referred to as "vessels") at sea, by aircraft flying over the seas, by offshore installations, or by means of submarine communication cables, both in peacetime and during armed conflicts (SCHMITT, 2017b, p. 232).

For Rocha and Fonseca (2019), in a conflict scenario, having the ability to carry out a cyber intrusion into an adversary's asset, having access to knowledge and even control over the actions, means obtaining a strategic advantage (ROCHA, FONSECA, 2019, p. 518). The ability to carry out cyber operations from the sea translates into an unprecedented competitive advantage. However, the ability to defend against this type of operation goes beyond the previous one and signifies the maturity of the state in relation to the new scenario of the information age.

30 Comment 1 of the Tallinn Manual 2.0 (SCHMITT, 2017b, p. 232).

Most of the rules[31] of the customary international law of the sea are reflected in the United Nations Convention on the Law of theSea (UNCLOS). Even states that are not parties to UNCLOS usually respect the terms of the Convention. This section of the article draws heavily on the provisions contained in UNCLOS, which for the GIP reflects customary international law on the subject.

A State[32], however, can consent to another State exercising jurisdiction on board ships flying its flag. This consent can be tacit, through custom, or express, through a formal international agreement (see Rule 19). It should be noted that ships may also be subject to the jurisdiction of the coastal state, depending ontheir location and the type of activity they are carrying out. However, in accordance with Rule 5 of the Tallinn Manual 2.0, According to Rule 10, which deals with "immunity from jurisdiction", if the ship has such immunity, it is protected from the jurisdiction of the coastal state. In addition, individuals involved in cyber operations on board ships are subject to prescriptive jurisdiction[33], the basis of which is set out in Rule 10. (SCHMITT, 2017b, p. 232)

The Law of the Sea[34] is a peacetime regime. Although it is generally applied mutatis mutandis during periods of armed conflict (see Rules 82-83), there are various permissive rules and prohibitions, and some specific nuances that are imposed by the Law applied to Naval Warfare, whose application is between belligerent States andbetween belligerent States and neutral States (The San Remo Manual provides for the rules of naval warfare). Consequently, the parties to an armed conflict do not lose the rights established in the UNCLOS as flag states, port states or coastal states, nor are they released from their duties and obligations, except in situations where the UNCLOS rules are modified or replaced by the particular rules of the law of naval warfare. An example of this is the fact that States involved in an armed conflict at sea may exercise the right of "mere passage[35]" (see rule 49 of the Tallinn Manual 2.0) through

31 Comment 2 of the Tallinn Manual 2.0 (SCHMITT, 2017b, p. 232).

32 Comment 4 of the Tallinn Manual 2.0 (SCHMITT, 2017b, p. 232).

33 Prescriptive jurisdiction, or legislative jurisdiction, has been an established concept in international law. It is one of the ways in which a state can have an impact on people, property or circumstances. According to the American Law Institute, prescriptive jurisdiction is "to prescribe, that is, to make its law applicable to the activities, relations, or status of persons, or to the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or recognition, or by judicial determination" (CHOY, 2019, p.1).

34 Comment 5 of the Tallinn Manual 2.0 (SCHMITT, 2017b, p. 233).

35 Name given to the passage of a belligerent ship through the territorial sea of a neutral

the territorial seas of neutral States, a right which, in peacetime, is referred to as the right of "innocent passage" (see Article 48 of the Tallinn Manual 2.0). The regime of mere passage contains specific nuances related to armed conflict and neutrality that restrict or regulate conduct that would otherwise be permitted under the regime of innocent passage. (SCHMITT, 2017b, p. 233)

From this point on, the rules of the Tallinn Manual 2.0 will be detailed for each legal compartment of the maritime environment. Initially, it is important to understand the context in which a malicious cyber operation could interfere with or violate the sovereignty of a coastal state or even cause damage to its public order. The next step will be to understand how a cyber operation can be used as a weapon of naval warfare, or to the advantage of campaigns at sea.

***Cyber Operations on the High Seas:***

When addressing cyber operations on the high seas, the Tallinn Manual 2.0, in rule 45, which is related to art. 88 of UNCLOS, states that **"cyber operations on the high seas may be conducted only for peaceful purposes, unless otherwise provided by international law"** (SCHMITT, 2017b, p. 233).

For UNCLOS, with rare exceptions, ships on the high seas are subject to the jurisdiction of the flag state[36]. This jurisdiction also extends to cyber operations conducted on board. Depending on the location of the ship, it may be subject to the jurisdiction of the coastal state if it does not have immunity from jurisdiction[37]. According to the Tallinn Manual 2.0, individuals engaged in cyber operations are subject to the extraterritorial prescriptive jurisdiction[38] of the flag state (SCHMITT, 2017b, p. 232).

According to UNCLOS, "the high seas are reserved for peaceful purposes", whichis a cogent rule of international law, and the use of force in this territorial space is prohibited, unless permitted by the

state, provided for in Hague Convention XIII, art. 10.

36 Exceptions are when the following crimes are suspected: piracy, slave trade, unauthorized transmissions, non-apparent nationality and the same flag as the warship.

37 It is the privilege granted to certain foreign persons, by virtue of the positions or functions theyhold,to escape the jurisdiction, both civil and criminal, of the state in which they are located. ACCIOLY, Hildebrando; SILVA, Geraldo Eulálio do Nascimento. Manual of public international law. 12. ed. São Paulo: Saraiva, 1996.

38 Rule 10 of the Tallinn Manual 2.0 (SCHMITT, 2017b).

law itself (UNCLOS, art. 88). Referring back to the Tallinn Manual 2.0, cyber operations are permitted, but cannot violate any rule or law of international law. The principle of freedom of the high seas[39] also applies to cyber operations (SCHMITT, 2017b, p. 233).

This also includes the freedom of all states to launch submarine cables on the high seas, but such action cannot affect the freedom of states to use that space (SCHMITT, 2017b, p. 234). It should be noted that the Exclusive Economic Zone[40] (EEZ) has a special regime, which will be discussed below.

> According to the GIP[41], "military operations that do not involve the use of force fall within the scope of the peaceful use of the sea". However, considering where these operations are carried out, even if they are simple military cyber operations, they may be in violation of a treaty or special multilateral regime, such as the Antarctic Treaty[42]. Carrying out cyber operations at sea is subject to the principle of Due Diligence[43] and can be challenged or prohibited by the coastal state (SCHMITT, 2017b, p. 234).

Also in relation to the use of the high seas, the GIP agreed that the establishment of underwater data centers is lawful. However, in the EEZ or territorial sea, this equipment can only be established with the consent of the coastal state and its operation is subject to the regulation and jurisdiction (see rule 9 of the Tallinn Manual 2.0) of that state[44]. This

39 These rules are binding only on states, so that actions by non-state actors in any part of the sea can be considered illegal under international law or under the domestic law of the coastal state (SCHMITT, 2017b, p. 233).

40 The Exclusive Economic Zone (EEZ), according to the United Nations Convention on the Law of the Sea (UNCLOS), is a strip of land beyond territorial waters, over which each coastal country has priority for the use of the sea's natural resources, both living and non- living.

41 Comment 5 of the Tallinn Manual 2.0, (SCHMITT, 2017b, p. 234).

42 See Decree No. 75.963, of July 11, 1975. BRAZIL. Decree No. 75.963, of July 11, 1975. Promulgates the Antarctic Treaty. Brasília - DF: Presidency of the Republic, 1975.

43 Principle enshrined in international law, according to which the State must take all measures to ensure that its territory is not used for the execution of acts contrary to the law of other States, in this case, cyber operations that could harm another State (SCHMITT, 2017b, p. 30).

44 The consent of the coastal state is required for establishment in its territorial sea, as it exercises sovereignty over that area and its seabed (see Rule 2). As for establishment in

legal proposition tends to favor the principle of state sovereignty with regard to the use of its territorial sea and its precedence in exploiting the EEZ.

Schmitt (2017) states that "the law of naval warfare allows certain cyber operations to be conducted on the high seas in the context of an international armed conflict (IAC) (see Rule 82 of the Tallinn Manual 2.0) whichwould otherwise be prohibited in peacetime". As an example, military cyber operations are conducted in support of a naval blockade (Rule 128 of the Tallinn Manual 2.0). Similarly, a cyber-attack (see Rule 92 of the Tallinn Manual 2.0) against a merchant vessel, which is violating a naval blockade, is lawful if the vessel, even after prior warning, continues to resist capture[45].

It should be noted that only states are bound by rule 45 of the Tallinn Manual 2.0 in their cyber operations. The activities of non-state actors at sea may be illegal and may even be characterized as a crime under international or domestic law, but they do not imply the restriction reflected in this rule, unless such activities can be attributed to a state.

***Visiting rights and cyber operations***

Regarding the right of access, rule 46 of the Tallinn Manual 2.0, which is related to art. 110 of UNCLOS, states that **"a warship, or a ship authorized by the State, may exercise the right of access and board a ship of another State, without itsconsent, if there are reasonable grounds to suspect that such a ship is using cyber means to engage in piracy, slave trade, illicit transmissions, does not appear to be of nationality, or if the ship is of the same flag as that of the warship or State"**[46].

With regard to the use of cyber operations to exercise the right of access on the high seas, the general rules are the same as those established by the UNCLOS, i.e. warships or authorized vessels[47] cannot board private vessels that do not fly their country's flag. The exceptions are for the same cases that exist in UNCLOS, which support physical visits. These

---

the EEZ, see UNCLOS, art. 60, specifically with regard to installations and structures for economic purposes (SCHMITT, 2017b, p. 231).

45 See: San Remo Manual, paragraph 98 (SCHMITT, 2017b, p. 235).

46 (SCHMITT, 2017b, p. 235).

47 The term "authorized vessel" will be used for vessels authorized by the flag state to engage in law enforcement actions and must be duly identified as such (SCHMITT, 2017b, p. 232).

are: piracy, the slave trade, unauthorized transmissions, non-apparent nationality and the same flag as the warship.

In the opinion of a minority of the Tallinn Manual 2.0 group of experts, the simple posting of evidence[48] of any kind of illicit activity concerning the ship on social networks "may constitute reasonable evidence to allow a cyber visit". The action to be taken by the Warship or State Ship will depend on the type of situation (among the 5 mentioned) in which the offending ship may be involved (SCHMITT, 2017b, p. 236).

For the GIP, from the point of view of the intersection between International Law Applied to Cyber Operations and the Law of the Sea, the most relevant illicit actions will be, in order of priority: piracy, unauthorized broadcasting and the non-apparent display of a flag. In the GIP's view, the slave trade is also relevant, but it has a lower priority than the actions mentioned above.

In the case of piracy on the high seas or in the EEZ, according to the Tallinn Manual 2.0, a cyber boarding may be carried out, followed by a physical boarding to seize the ship and arrest the crew. It should be noted that from a technical point of view, a pirate ship can use cyber operations to disable the maneuvering or communications of a target ship. However, in order to legitimize the right of cyber visitation, in any of the 5 situations, there must be founded and reasonable suspicion[49] that the ship to be boarded is engaged in illicit actions (SCHMITT, 2017b, p. 236).

With regard to clandestine transmissions[50], these can be sound, radio or television, but they must be characterized as transmissions for public consumption, with the exception of those for distress calls. In this situation, the warships or state ships that have the right to visit and terminate the transmission are those that are receiving the transmission, or belong to the states that are being interfered with, or the states whose ships are receiving or being interfered with[51] by the clandestine transmissions

48 Members of the ship's crew posting on Facebook, Instagram, or any other known network (SCHMITT, 2017b, p. 236).

49 Suspicion must be based on strong evidence, it cannot be "mere liberality" (SCHMITT, 2017b, p. 237).

50 50 In relation to transmission via the internet, with the dissemination of propaganda via social networks, in order to be considered a violation of the sovereignty of another state, we have to observe whether there is coercion (having a direct influence on the inherent and exclusive functions of a sovereign state), described in rule 4 of the Tallinn Manual 2.0 (SCHMITT, 2017b, p. 237).

51 It should be noted that, for UNCLOS, the purpose of the prohibition contained in the rule is directed at broadcasting frequencies, which are controlled by international

(SCHMITT, 2017b, p. 237).

The Tallinn Manual 2.0 also states that for ships that have no apparent nationality[52], or pretend to have one in the case of a false nationality, it is permissible to use both cyber operations for a virtual approach and a physical approach to check the true nationality. To legitimize the right of access, in this case, it is enough for the ship to have an electronic indication of suspected nationality. It is well known that it is not uncommon these days to mask[53] the Global Navigation Satellite System (GNSS) through cyber operations (SCHMITT, 2017b, p. 238).

It should be noted that the permissibility of "virtual visitation" for the situations listed above did not reach a consensus among the group of experts. The majority position was that virtual visitation was an extension of traditional visitation rights; for these experts, virtual visitation was less intrusive than physical visitation, and therefore more consistent with the rights in question. For the minority group, the virtual visit, despite being less intrusive, has the potential to extrapolate what the UNCLOS advocates, since the visiting ship could have access to a large amount of data that is unnecessary for the realization ofthis right. The fact is that opening up the precedent for states to carry out "virtual visits" on other states' ships could mean inviting espionage (SCHMITT, 2017b, p. 239).

Although it is a position that has not yet found a consensus, due to political issues, without prejudice to what this rule advocates, the right of visit, including forced boarding, can be authorized by a resolution of the United Nations Security Council (UNSC), as is currently the case with the ships of the Maritime Task Force of the United Nations Interim Force in Lebanon[54] (MTF-UNIFIL).

***Cyber operations in the Exclusive Economic Zone (EEZ):***

Rule 47 of the Tallinn Manual 2.0, which relates to Articles 55 and 56 of UNCLOS, states that "a State conducting, in the exercise of its rights

telecommunications laws, that could produce harmful effects on communications in the territory, including maritime territory, of a coastal state (SCHMITT, 2017b, p. 236).

52 Technically, there is the possibility of using cyber operations to hide a ship's nationality in the satellite-based Automatic Identification of Ships System (AIS), or to make the system display a false identification (FAHEY, op. cit., p. 3).

53 Id., 2017.

54 MTF UNIFIL ships are authorized to board any ships, which do not have immunity from jurisdiction, on the high seas, in the EEZ or even in Lebanese territorial waters, by virtue of UNSC Resolution 2373).

and duties, a cyber operation in the EEZ of another State shall have due regard to the rights and duties of the coastal State in its EEZ, and the cyber operation shall be conducted for peaceful purposes, unless otherwise provided by international law" (SCHMITT, 2017b, p. 239).

The EEZ is an area, beyond the limits of the territorial sea, which cannot extend more than 200 nautical miles into the sea, with the baselines[55] of the state as references. In the EEZ, the coastal state has rights and jurisdiction for the purposes of exploration, research, management, conservation of the natural resources of the water column, seabed and subsoil of the zone, as well as for energy production using currents and winds[56]. In the EEZ, states can also exercise jurisdiction over the establishment and use of islands, installations and artificial structures for economic purposes; marine scientific research[57]; and over some incidents of marine pollution carried out by ships[58]. For example, cyber activities that interfere with energy production facilities located in the EEZ, such as wind farms or tidal streamturbines, would fall within the jurisdictional competence of the coastal state (SCHMITT, 2017b, p. 249).

According to the CNDUM, all states enjoy the same freedom in the EEZ as they do on the high seas, with regard to navigation, overflight, laying cables and oil pipelines, as well as any other legal international use related to these freedoms. With regard to the transit of warships, there is an established practice in some navies[59] around the world, whereby states give notice both when they are going to cross the EEZ and when they need to cross the territorial sea of coastal states.

With regard to cyber operations carried out in this part of the sea, there are divergent lines in the Tallinn Manual 2.0, but in general, operations to aid navigation and communications, which are lawful and not malicious, can be carried out, applying the same principle of freedom as on the high seas. In this way, the majority position of the Manual believes

55 CNUDM, Art. 57.

56 CNUDM, Art. 55-56.

57 UNCLOS Art. 56 (1)(b).

58 CNUDM Art. 211.

59 It should be noted that only around 40 countries (mostly developing countries), including Brazil, require prior notification of innocent passage by warships, and only 17 countries, including Brazil, have formally expressed the understanding that the consent of the coastal state is required for activities to be carried out in its EEZ.

that ships and aircraft have the same freedom that they experience on the high seas and this does not unduly affect any of the enumerated sovereign rights of coastal states (SCHMITT, 2017b, p. 240).

In the view of the group of experts, UNCLOS fails when it does not address, or list, any security interests of coastal states, regarding cyber operations in the EEZ. T hus, for the experts, aircraft and ships transiting the EEZ, in terms of carrying out cyber operations, enjoy the same freedom as they would on the high seas, including for military activities[60]. This freedom is subject to due consideration of the exclusive rights of the coastal[61] state. In particular, warships and aircraft capable of carrying out cyber operations are free to operate in the EEZ, without the need for the consent of the coastal state (SCHMITT, 2017b, p. 240).

According to the Manual, in relation to the possibility of carrying out military activities in the EEZ, the group of experts was divided between two positions. The majority position[62] believes that, because UNCLOS does not list security interests in this portion of the sea, states could engage in military activities, such as intelligence gathering by cyber means and also cyber military exercises, without the need for coastal state consent. The minority group[63] believes that in order to carry out typical military activities they need the consent of the coastal state. Both groups agree that scientific research, even if "for the good of humanity", including that conducted by military personnel, requires the consent of the coastal state. This issue has a strong potential for controversy in the future, especially when we consider that the Tallinn Manual 2.0 does not prohibit

60 According to the UNCLOS, these are overflight activities, naval force maneuvers, military exercises, surveillance, military research activities, intelligence gathering and the launching of explosives.

61 According to the UNCLOS, the coastal state has sovereign rights and jurisdiction to prospect, exploit and conserve the natural resources existing there, including the generation of energy through currents. As such, no cyber activity carried out by another state in the EEZ can interfere with these rights.

62 For this group, typical military operations have no influence on their enjoyment of the world.

limited sovereignty of coastal states in this stretch of sea (SCHMITT, 2017b, p. 240).

63 According to this group, Article 58(3) of the UNCLOS emphasizes that due consideration must be given to the rights and duties of the coastal state in the EEZ. For the group, security issues are included in this article. (SCHMITT, 2017, p. 240).

cyber espionage[64] (SCHMITT, 2017b, p. 240).

According to the Tallinn Manual 2.0, the concept of "peaceful use" does not prohibit states from carrying out countermeasures[65] from the EEZ, including cyber countermeasures. This understanding also includes naval warfare operations between belligerent states. Such operations must be in line with the San Remo Manual. If the coastal state is a neutral state, the belligerents must give due consideration to its rights and duties.

***Cyber operations in the territorial sea:***

According to Rule 48 of the Tallinn Manual 2.0, which is related to Article 2 of the UNCLOS, "in order for a ship to enjoy the right of innocent passage through the territorial sea of a coastal State, any cyber operation carried out by the ship must be in accordance with the conditions imposed by that right" (SCHMITT, 2017b, p. 241).

Perhaps the passage through the territorial sea of a coastal state is the most sensitive action, as far as International Law Applied to Cyber Operations is concerned. A series of precautions must be taken, both by merchant ships and state vessels, so that a recognized and consolidated right of passage does not inadvertently become the motivation for a serious diplomatic incident.

According to the Tallinn Manual 2.0, coastal states enjoy sovereignty and full jurisdiction in the strip of sea running from the baseline of the coastline to a distance not exceeding 12 nautical miles[66]. The territorial sea is legally an extension of the territory of the coastal state. Ships of all states, including warships, enjoy the right of innocent passage[67] through the territorial sea of coastal states. Airplanes are not

64 Rule 32 of the Tallinn Manual 2.0 (SCHMITT, 2017).

65 Rule 20 of the Tallinn Manual 2.0 (SCHMITT, 2017).

66 Article 3 of the UNCLOS.

67 The institute of "innocent passage" is provided for in Article 3 of Law 8.617/93: Art. 3 The right of innocent passage in the Brazilian territorial sea is recognized for ships of all nationalities. § Paragraph 1 The passage shall be considered innocent provided that it is not prejudicial to the peace, good order or security of Brazil, and must be continuous and rapid. § Paragraph 2 Innocent passage may include stopping and anchoring, but only to the extent that such procedures constitute common navigational incidents or are imposed for reasons of force or serious difficulty, or are intended to assist persons or ships or aircraft in danger or serious difficulty. § Paragraph 3 Foreign ships in the Brazilian territorial sea shall be subject to the regulations established by the Brazilian Government.

entitled to this right and submarines, in order to enjoy it, must sail on the surface, flying their flag (SCHMITT, 2017b, p. 241).

For the group of experts, the innocent passage regime[68] does not require the consent of the coastal state, however, for warships, some coastal states require prior notification, so that it can be consent to the passage. However, this practice lends itself more to diplomatic deference than to a legal requirement between states. Given the degree of lethality and high technology ofnaval warfare, the approach of such warfare to the territory of a coastal state, without proper coordination, can be considered a serious threat to the coastal state or, at the very least, a serious provocation (SCHMITT, 2017b, p. 241).

Innocent passage can be suspended by the coastal state in specific areas for security reasons, but it cannot be discriminatory[69]. For example, passage may be suspended in order to carry out an exercise employing cyber operations, which could pose a cyber security risk to other ships. Innocent passage cannot become detrimental[70] to peace, to the order or security of the coastal state. The Tallinn Manual draws a parallel with the UNCLOS on this topic, listing a series of actions in the cyber sphere that can turn innocent passage into harmful. They are:

68 The innocent passage regime does not apply to inland waters; for ships with immunity from jurisdiction, diplomatic authorization is usually required to access these waters, as well as the inland waters of archipelagic states (SCHMITT, 2017b, p. 241).

69 The suspension must apply to all States (UNCLOS, Article 25, paragraph 3).

70 The UNCLOS lists the situations in which passage can become harmful, in Article 19(2) :

2. The passage of a foreign ship shall be considered prejudicial to the peace, good order or security of the coastal State if that ship carries out, in the territorial sea, any of the following activities: a) any threat or use of force against the Sovereignty, territorial integrity or political independence of the coastal State or any other action in violation of the principles of International Law set forth in the Charter of the United Nations;

c) any act intended to obtain information prejudicial to the defense or security of the coastal State; d) any act of propaganda intended to undermine the defense or security of the coastal State; e) the launching, landing or receiving on board of any aircraft; f) the launching, landing or receiving on board of any military device; g) the embarkation or disembarkation of any product, currency or person in violation of the customs, fiscal, immigration or sanitary laws and regulations of the coastal State; h) any intentional and serious act of pollution contrary to this Convention; i) any fishing activity; j) the carrying out of research activities or hydrographic surveys; k) any act intended to disrupt any communication systems or any other services or facilities of the coastal State; l) any other activity not directly related to the passage.

> a) Illegal threat to use cyber force against the coastal state;
> b) Exercise or practice involving the use of cyber weapons that are not limited exclusively to the ship and its systems[71];
> c) Cyber operations aimed at gathering information harmful to the security of the coastal state;
> d) Distribution, by cyber means, of propaganda that is harmful to the security of the coastal state;
> e) Launching or receiving aircraft, vessels, or any other military equipment, which are engaged, or have the capacity to engage in cyber operations;
> f) Research or evaluation activities, including those carried out or facilitated by cyber means;
> g) Malicious cyber operations intended to interfere with the communications system or any other facility of the coastal state; and
> h) Any other cyber activity unrelated to navigation or communications that the ship uses for passage (SCHMITT, 2017b, p. 242).

This list is not exhaustive and there may be other situations[72] that are capable of transforming the innocent passage into a harmful one. The context of the situation and the extent of the damage must be fundamental to measuring the harm. For example, if a ship provides wireless internet access to an insurgent group, and this signal is blocked by the coastal state, the ship is carrying out a prohibited operation. In this way, the ideal is for the ship, in innocent passage, to restrict cyber operations on board. Only those operations necessary for the safety of the ship should be carried

71 Refers to the ship's organic cybernetic resources, which are essential for navigation. and communication.

72 The specific situation involving the execution of passive (non-intrusive) assessment of wireless cyber networks during innocent passage was also controversial in the group of experts. The majority position of the group argued that such activity is consistent with innocent passage, as it is passive and non-intrusive. The minority argued that such monitoring would be illegal and conflict with the interests of the coastal state (SCHMITT, 2017b, p. 243).

out. According to the Manual, the group of experts also addressed the situation in which the ship, in innocent passage through the territorial sea of a state, carries out a harmful cyber operation against a third state. The majority position states that "cyber activities carried out during innocent passage, may not harm the security or public order of the coastal state, including relations, rights and duties with other states". Therefore, if the cyber operation against a third state does not affect the security of the coastal state, for the majority group, this operation is allowed. For the minority group, each case must be analyzed on its merits, emphasizing that the purpose of innocent passage is to safeguard the basic interests of the coastal state and not those of third states or non- state actors. For them, a cyber operation against a third state or non-state actor does not directly conflict with the innocent passage regime. Still according to the minority group, in order to assess whether or not the cyber operation can affect the coastal state's relationship with a third state, specific factors must be analyzed, such as: the nature of the operation; the extent to which the operation is overt; and the level of relationship between the coastal state and the third state. It should be noted that the lack of consensus on this issue has the potential toposea serious problem to innocent passage, especially if cyber operations against the third state are classified as espionage or cyber warfare (SCHMITT, 2017b, p. 243).

For the group of experts, any ship on innocent passage can and must carry out all cyber operations that "are necessary for its safety and that of the ships accompanying it, provided that such operations do not jeopardize the peace, public order or security of the coastal state". If a ship, during innocent passage, is the target of a hostile cyber operation, it may take all necessary cyber actions[73] to terminate the hostile action (SCHMITT, 2017b, p. 244).

Ships that do not have immunity from jurisdiction during innocent passage may be required to obey the laws and regulations of the coastal state relating to cyber operations. On this type ofship, the coastal state has civil and criminal jurisdiction for some hypotheses when in the territorial sea. For example, coastal states can create laws related to navigational safety or the protection of submarine cables that restrict

73 This procedure is consistent with international law, including, if appropriate, the use of countermeasures or even the invocation of the principle of self-defense (SCHMITT, 2017b, rules 20 and 71).

certain cyber operations during innocent passage.

While the coastal state has certain civil and criminal jurisdiction over ships without immunity from jurisdiction engaged in non-innocent passage, this jurisdiction does not exist over ships with immunity from jurisdiction. If an immune ship is found to be on a non-innocent passage, the coastal state can demand that it leave its jurisdictional waters immediately. In the opinion of the group of experts, the use of forced cyber operations that are designed to compel the recalcitrant ship with immunity from jurisdiction to leave the territorial sea is a permissible measure available to the coastal state (SCHMITT, 2017b, p. 244).

This rule applies mutatis mutandis to innocent passage through the waters of archipelagic states, through which no maritime routes pass, or where these have not been designated as "routes normally used for international navigation".

***Exercise of Jurisdiction over cyber operations in the Territorial Sea:***

Regarding the jurisdiction of cyber operations carried out in the territorial sea of the coastal state, rule 50 of the Tallinn Manual 2.0, which is related to art. 27 of the UNCLOS, states that "the coastal State may exercise jurisdiction on board ships in its territorial sea in respect of criminal activities involving cyber operations if: the consequence of the crime extends to the coastalState; the crime is capable of causing disturbance to the public order and security of the coastal State or to the good order of the territorial sea; the master of the ship or the flag State has requested such action from the authorities of the coastal State; it is a necessary action to combat international drug trafficking" (SCHMITT, 2017b, p. 24). 246).

As a general rule, article 27 of UNCLOS establishes that the authorities of the coastal state may not arrest crew members, seize ships or conduct investigations on board ships flying the flags of other states during the presence of these ships in the territorial waters of the coastal state, except in the following cases: a) if the criminal offense has consequences for the coastal state; b) if the criminal offense is of such a nature that it may disturb the peace of the country or order in the territorial sea;

(c) if the assistance of the local authorities has been requested by the master of the vessel or by the diplomatic representative or consular official of the flag State; or (d) if such measures are necessary for the suppression

of illicit trafficking in narcotic drugs or psychotropic substances.

Regarding the notion of "extension of consequences" provided for in Article 50 of the Tallinn Manual 2.0, for cyber operations carried out on board a ship passing through the jurisdictional waters ofa coastal state, the group of experts agreed that the coastal state may exercise jurisdiction on board a ship passing through its territorial sea if the cyber operation originating from this ship violates the criminal law of that state and is clearly manifested in its territory[74], including the territorial sea (SCHMITT, 2017b, p. 246).

With regard to the scale of the consequences of the illicit cyber operation, the group of experts was divided. The minority group argues that minimal or trivial consequences would not justify the exercise of criminal jurisdiction by the coastal state. For the majority group, "any degree of violation will suffice for the coastal state to have this prerogative". There was consensus among the group of experts that any cyber operation conducted by a foreign vessel in the territorial sea of the coastal state, which has widespread effects[75] and therefore disturbs the coastal state, would be sufficient to entitle the coastal state to exercise criminal jurisdiction on board the vessel in question (SCHMITT, 2017b, p. 244).

Cyber activities related to illicit drug trafficking are the basis for the exercise of the coastal state's criminal jurisdiction over vessels in its territorial sea. Consider the situation in which a state is monitoring the cyber communications of certain vessels located in its territorial sea, based on data provided to law enforcement authorities. If the authorities identify any communications indicating that the vessel is being used for the illegal transportation of drugs, they can use cyber means to facilitate boarding and stopping the vessel (SCHMITT, 2017b, p. 247).

The Manual also states that if a cyber activity that constitutes a crime under domestic law takes place on board a foreign ship before it leaves the territorial sea, it also justifies the coastal state exercising criminal jurisdiction on board that ship. Unlike criminal jurisdiction,

74 For example, a Distributed Denial-of-Service (DDoS) operation initiated from inside a ship against a coastal state's cyber infrastructure, which violates its domestic law (SCHMITT, 2017b, p. 247).

75 nterference in the public order of the territorial sea can be carried out by carrying out a cyber operation that interferes with the navigation systems of ships in the territorial sea and/or with the communication system between ships and shore-based safety of navigation agencies (SCHMITT, 2017b, p. 247).

the coastal state cannot exercise civil jurisdiction over cyber activities on foreign ships passing through its territorial sea (SCHMITT, 2017b, p. 248).

Bilateral agreements between states can change the dynamics of the application of the rule of jurisdiction in the territorial sea, as well as the situation of armed conflict, in which the neutral state must take all possible measures to guarantee the right of mere passage of warships from belligerent states through its territorial sea. It should also be noted that a UNSC Resolution may allow cyber operations within the territorial sea of a coastal state, even if such operations may de-characterize innocent passage.

***Cyber operations in the Contiguous Zone (CZ)***

Regarding the jurisdiction of cyber operations carried out in the contiguous zone of the coastal state, rule 51 of the Tallinn Manual 2.0, which is related to art. 33 of UNCLOS, states that "with respect to vessels located in the contiguous zone of a coastal State, that State may use cyber means to prevent or remedy violations of its fiscal, immigration, sanitary or customs laws occurring in its territory or territorial sea, including violations committed by cyber means" (SCHMITT, 2017b, p. 248).

States can claim a contiguous zone, which extends from the limit of their territorial sea to twenty-four nautical miles, with reference to the baseline[76]. In the area of the contiguous zone, the coastal state enjoys two prerogatives of authority. The first is the sovereign right to enforce its tax, immigration, health and customs laws against vessels suspected of violating them while in the coastal state's internal waters or territorial sea[77] (SCHMITT, 2017b, p. 248).

If a vessel that has violated tax, immigration, health or customs laws, whether by cyber or other means, is in the contiguous zone, the coastal state can interdict the vessel before its departure or open proceedings[78], respecting international law, to make it return to port for investigation or prosecution. For this situation, the coastal police can use cyber means as part of the interdiction operation. For example, it can control the movement of the offending vessel by cyber means and direct it back to the police vessels (SCHMITT, 2017b, p. 248).

76 UNCLOS Art. 33(2).
77 UNCLOS, Art. 33 (1)(b).
78 CNUDM, Art. 111.

The other prerogative of authority granted to the coastal state in relation to enforcement issues in the contiguous zone is that of prevention[79]

This prerogative allows the coastal state to use cyber means to warn and prevent a vessel in the contiguous zone from violating tax, immigration, health and customs laws (SCHMITT, 2017b, p. 249).

***Cyber operations in international straits and waters of archipelago states***

Rules 52 and 53 of the Tallinn Manual 2.0, which are related to Articles 41 and 46 of UNCLOS, state that: **"rule 52- Cyber operations in straits used for international navigation shall be consistent with the right of transit passage" and "rule 53- Cyber operations in waters of archipelagic states shall be consistent with the right of transit passage"** (SCHMITT, 2017b, p. 249; 250).

Straits are the portions of the sea used for international navigation between a part of the high seas or an exclusive economic zone of one or more states and another part of the high seas or an exclusive economic zone of one or more states.

In this part of the sea, the institute used for navigation is the transit passage institute[80] and it differs from innocent passage on the following points: "transit passage cannot be suspended by any of the coastal states; aircraft also have the right of transit passage; and aircraft and ships can pass in their normal mode (a submarine can pass underwater)" (SCHMITT, 2017b, p. 250).

For the Manual, cyber activities that are inconsistent with the transit passage regime cannot be carried out during the passage. Only "cyber activities related to the safety of the ship's navigation and communications may be carried out". Belligerent cyber operations are not permitted in this passage regime (SCHMITT, 2017b, p. 250).

Ships and aircraft with immunity from jurisdiction that carry out cyber operations that violate the legislation of the coastal state will not be subject to its jurisdiction, but "may be asked to withdraw from the strait"[81]. The flag state of these ships or aircraft can be held internationally liable

79 CNUDM, Art. 33º(1)(a).

80 CNUDM, Art. 34.

81 CNUDM, Arts. 34, 38(3).

for any damage or loss that such operations may cause in coastal states (SCHMITT, 2017b, p. 251). Archipelagic states can designate maritime routes for the passage of international maritime traffic in which ships will also have the right of passage and which must be carried out along the same lines as innocent passage through territorial waters. However, with regard to cyber operations carried out on board, the rules are the same for the transit ticket.

***Submarine communication cables:***

According to Rule 54 of the Tallinn Manual 2.0, which is related to Article 112 of the UNCLOS, "the rules and principles of international law applicable to submarine cables and pipelines shall also apply to submarine communication cables". (SCHMITT, 2017b, p. 252).

It is known that submarine communications cables are subject to damage, wear and tear and to interception for data collection, through technical manipulation[82], which can also be carried out to "jam" or "alter" the data passing through them.

The issue of laying underwater communications cables is of great interest to those countries that do not consider the practice ofespionage in peacetime to be reprehensible in international relations. With the rapid advance of technology, it is assumed that unmanned submersible vehicles are capable of manipulating submarine communications cables.It will also be seen in this section that some of the conclusions reached by the group of experts in the Tallinn Manual 2.0, which is mostly made up of experts from NATO countries, who support espionage as a common practice in times of peace, are not very well accepted by the Brazilian Constitution of 1988.

The sovereign rights of the coastal state with regard to the territorial sea also extend to submarine cables laid on its continental shelves. Such cables have the same legal regime of cyber structures located on the land territory of that state. Therefore, in the territorial sea, coastal states have the right to legislate[83] on the activities of launching, maintaining, repairing and replacing submarine communication cables, as

82 Tallinn Manual 2.0 (SCHMITT, 2017b, p. 254).

83 The archipelago state also has the right to legislate on the laying of submarine communications cables and must authorize the repair of such cables when requested by another state (SCHMITT, 2017b, p. 255).

well as to adopt laws and regulations regarding their protection. However, such laws or regulations may not impose restrictions on innocent passage (SCHMITT, 2017b, p. 253).

In relation to the EEZ or Continental Shelf, any state can lay submarine communications cables[84] as long as it respects the limited sovereignty rights that the coastal state has in that strip of sea. Coastal states cannot prohibit such action. Although the laying of pipelines across the Continental Shelf may be subject to the prior consent of the coastal state, this rule does not apply to submarine communicationscables. Such action can only be prevented by the coastal state if such a measure is considered a "reasonable[85] action to exploit its natural resources" (SCHMITT, 2017b, p. 254).

Landlocked states, in order to exercise their right to the freedom to use the high seas[86], as well as their right to connect their cyber structures to the world, must agree, by means of a bilateral treaty, to the transit of communications cables through the territory of coastal states, so that these cables can reach and leave their territory[87]. (SCHMITT, 2017b, p. 255). There is a well-established practice in international law which recognizes that the right to lay submarine communications cables goes hand in hand with the ancillary rights[88] to carry out all measures. This includes the right to prepare for the identification of suitable routes, as well as the right tomaintenance and repair. States launching such cables also have the right to regular monitoring and inspections.

It is not clear from UNCLOS whether states could establish "protection zones", in which they would restrict the activities of anchoring

84 There was no consensus among the group of experts regarding the conflict of sovereignties that exists when it comes to laying submarine communication cables in the EEZ. For a good part of the group, deference should be paid to the coastal state, but without forgetting that such a launch is directly related to the principle of freedom of the high seas (SCHMITT, 2017b, p. 256).

85 The meaning of the word has not been defined by the group of experts.

86 UNCLOS Art. 125(1) and Art. 124(1)(a).

87 CNUDM, Art. 125 (2-3).

88 UNCLOS only provides for the replacement of old cables from archipelagic states, but the majority opinion of the group of experts was that states have the right to r e p l a c e them, especially in the case of cables that are outside the territorial sea of the coastal state. For these experts, such cables are crucial to the economy and security of the states that laid them. The minority view held that the right to replace old cables only applies to exists for archipelagic states, in accordance with UNCLOS. With regard to the right of maintenance and repair, all agreed that this is granted to states (SCHMITT, 2017b, p. 256).

ships, trawling and sand mining, since these activities constitute threats to the integrity of submarine communications cables.Itshouldbenoted that Australia and New Zealand have submarine communications cable protection corridors/zones in their territorial sea and EEZ. International law provides a legal basis for the establishment of cable protection corridors/zones in the territorial sea only.

"The deliberate damaging of submarine cables, subject to the rules of the TIP, is prohibited." It would be inconsistent to allow states to lay cablesand at the same time allow other states to destroy them. However, it is clear from the manual that "in the case of naval warfare actions, if the commander of the military operation in progress can justify that the damage to the cable constitutes a fundamental part of the maneuver, the action may be authorized"[89]. However, such action must not cause unnecessary suffering to the civilian population or constitute a serious offense against human rights (SCHIMITT, 2017b, p. 256).

The group of experts agreed that the physical manipulation of submarine communication cables for data collection in the waters of archipelagic states and in the territorial sea of the coastal state constitutes a serious violation of the sovereignty of the respective states. They also considered that the use of unmanned underwater vehicles is inconsistent with the regime of innocent passage. In the experts' view, in such cases, only the coastal state and the archipelago state have their sovereignty violated, which is not the case with the state that launched the cable. For the group, manipulation outside jurisdictional waters does not constitute a violation of sovereignty. In the opinion of the author of this article, this understanding opens up a considerable gap for international legal uncertainty and could translate into a frank invitation for espionage between states (SCHMITT, 2017b, p. 257).

## POINTS OF CONVERGENCE BETWEEN THE SAN REMO MANUAL AND THE TALLINN 2.0 MANUAL

This section will address the main issues related to the rules established by the San Remo Manual for naval warfare, from the point of view of the Tallinn Manual 2.0. It should be noted that some concepts have already been covered in the previous section, when we alluded directly to UNCLOS.

89 San Remo Manual, 1994.

The San Remo Manual is basically an adaptation of the DICA rules applied to land combat to the peculiarities of naval warfare. In this way, all the principles that govern land combat, such as Military Necessity, Humanity, Proportionality and Distinction, will be present in the rules for naval combat and will also be respected by the Tallinn Manual 2.0.

The experts of the Tallinn Manual 2.0 were concerned with establishing a special rule dealing with the passage of ships from both belligerent and neutral states through the territorial sea of coastal states, with the aim of establishing a single standard ofbehavior when it comes to carrying out cyber operations The concern of the doctrine in this case is both to safeguard the rights of neutral coastal states and to allow belligerent states to maintain their campaigns without violating the rights of others.

***Cyber operations in the Territorial Sea during an Armed Conflict:***

Regarding the conduct of cyber operations during an armed conflict, Rule 49 of the Tallinn Manual 2.0, which is related to Section I of Part II of the San Remo Manual, states that "during an international armed conflict, a neutral coastal state may not discriminate between the belligerent parties with regard to the conduct of cyber operations in its territorial sea" (SCHMITT, 2017b, p. 245).

For the duration of an International Armed Conflict[90] the rules for armed conflicts at sea (San Remo Manual) and neutrality override UNCLOS. The law of neutrality[91] prohibits belligerent parties from using neutral ports and waters as bases of operations against the adversary. But neutral countries can allow it, but are not obliged to exercise the right of mere passage in their territorial seas by the belligerent countries. They can also impose conditions on this right, which must apply to all the belligerent parties (SCHMITT, 2017b, p. 245).

During the mere passage, warships may not use the waters of neutral countries as a base of operations against their adversaries, or engage in belligerent activities[92]. This includes cyber operations against adversaries. However, cyber activities necessary for the security of

90 Rule 82 of the Tallinn Manual 2.0 (SCHMITT, 2017b, 2017).

91 Hague Convention XIII, art. 9.

92 Military activities related to armed conflict.

the warship may be carried out. According to the Tallinn Manual 2.0, belligerent states cannot conduct aggressive cyber operations[93], from outside neutral waters, against a warship that is merely passing through (SCHMITT, 2017b, p. 245).

Under the 1907 Hague Convention[94], a belligerent country is prohibited from erecting any kind of communications infrastructure within neutral waters to communicate with troops on land. By analogy, the experts understood that this rule also applies to cyber infrastructure.

If a belligerent state decides to carry out a cyber attack or malicious action from within the territorial sea of a neutral state, that state can use countermeasures to stop the illegal act of the belligerent state's ship.

***Use of countermeasures:***

Regarding the use of countermeasures, rule 20 of the Tallinn Manual 2.0 states that "a state may have the right to take countermeasures, whether cyber or otherwise, in response to a breach of an international legal obligation owed by another state" (SCHMITT, 2017b, p. 111).

This rule is extremely important for the neutral coastal state, that in a situation of International Armed Conflict must carry out all actions within its power to prevent its territory from being used by one of the warring parties to gain an advantage over the other.

When it comes to naval warfare, such actions can only be taken by the neutral state that has violated its duty of due diligence. It must be to the extent necessary for the offending ship of the belligerent state to cease its illegal action. The countermeasure does not necessarily have to be a cyber operation; it can be a physical or diplomatic action. The countermeasure may even involve carrying out actions that, under normal conditions, could be considered illegal.

It is important to differentiate between countermeasures and "reprisals[95]" between belligerent states in an international armed conflict.

93 For the group of experts, it is generally difficult for a neutral state to observe an aggressive cyber operation that originates from a belligerent warship outside its jurisdictional waters, but if the neutral state becomes aware of such activities, the law of neutrality imposes that the neutral state must cease such activity. This can be done, but not only, through cyber operations (SCHMITT, 2017, p. 245).

94 Hague Convention XIII, art. 5.

95 Reprisal is a customary practice under the IHL, subject to meeting 5 requirements in order to be considered valid: 1. It is only permitted in the event of a serious violation of

Reprisals between belligerents in an armed conflict consist of one of them taking normally unlawful actions against its adversary, in response to the latter's unlawful actions and with the sole purpose of persuading it to respect the law of war. But reprisals cannot be considered countermeasures because they are carried out between belligerents and maintain a causal link with the Armed Conflict. However, countermeasures can be taken, cybernetically or otherwise, in response to an action taken by one of the parties that violates a legal regime other than the TIP. It should be noted that countermeasures cannot be carried out against a non-state actor, unless it is acting on behalf of a state (SCHMITT, 2017b, p. 112).

In this way, a coastal state will be able to carry out all the actions in its power to stop a malicious cyber operation or even a cyber warfare action being carried out from within its territorial sea.

***The Naval Blockade and Exclusion Zone:***

Rules 128 and 130 of the Tallinn Manual 2.0, which are related to paragraphs 93 and 105 of the San Remo Manual, they advocate the following: **"Rule 128 - Methods and means of cyber warfare may be used for the maintenance of a naval or air blockade, alone or in combination with other methods, provided that they do not result in actions inconsistent with the international law of armed conflict." and "Rule 130 - To the extent that States establish zones, whether in peacetime or during armed conflict, lawful cyber operations may be used to exercise their rights in such zones" (SCHMITT, 2017b, p. 508; 510).**

For the law of naval warfare, a blockade[96] is a method of warfare consisting of a belligerent operation to prevent the entry and/or exit of

theIHL and must have the sole purpose of inducing the enemy to respect the rules of the Law of War; II. Reprisal must only be employed as a last resort; III. The reprisal must be proportional to the violation it is intended to stop; IV. The decision to reprisal must rest with the highest level of government; and V. Reprisals must cease as soon as the adversary begins to respect the law". Reference. ICRC. IHL Data Base. Rule 145. Reprisals.

96 According to the San Remo Manual, the elements that characterize a blockade are as follows: it must be declared and notified; the beginning, duration, location and extent must be stated in the declaration; the blockade must be effective; the Forces maintaining the blockade must be stationed at a distance from the coast determined by military needs; a combination of legal methods and methods of war must enforce the blockade; access to neutral ports, coasts and airports may not be blockaded; the termination, suspension, re-establishment, or other alteration of the blockade must be declared and notified; and the blockader must apply the blockade impartially to aircraft and ships of all States (MANUAL DE SAN REMO, 1996, art. 94 to 104).

enemy or neutral ships and aircraft into specific ports, airports or coastal areas belonging to, occupied by or under the control of a belligerent state. It can be established as part of a military operation targeting an enemy military force or as an economic operation, with the strategic aim of weakening the enemy's military force by degrading its economy. According to Farey (2017), the naval blockade of the future could be run entirely from a laptop.

Given the technological advances in computers and computersystems that equip aircraft and ships, cyber means can be used to establish or reinforce a naval or air blockade. The big question is whether or not the use of cyber means to block neutral or enemy cyber communications to or from enemy territory or areas under its control, known as a "cyber blockade[97], is subject to the law governing traditional blockades in times of Armed Conflict.

A small minority of experts considered that this cybernetic operation would be a mere "electronic blockade", which if would confuse it with electronic warfare. "Most were of the opinion that a naval or air blockade is generally established to create a particular effect[98] that can be achieved with the use of cyber means." The establishment of a traditional naval blockade requires the specification of a particular geographical line that ships will not be able to cross. This raised the question of whether a similar line could be articulated in the declaration of a cyber blockade and whether it would be technically possible to carry out the blockade of all means of cyber communication along this line. The technical advisors stated that it is possible to carry out both actions (SCHMITT, 2017b, p. 506).

One of the difficulties of adapting the rules of the traditional naval blockade to the scope of cyber operations lies in the fact that the naval blockade involves prohibiting access to ports or maritime or coastal areas. Thus, given the relative freedom of navigation of neutral ships, this type of blockade is only effective and legitimate when carried out in a

97 This issue generated a lot of debate in the group of experts and these debates revolved around the applicability of the criteria established for the realization of a blockade, for the cyber context, the technical feasibility of carrying out a cyber blockade, and then the characterization of the rules for the cyber blockade as lex lata or lex ferenda (SCHMITT, 2017b, p. 506).

98 As an example, the blockade that is created to achieve negative economic effects on the enemy economy, since economic activity is largely conducted by communication via the internet, the majority group of experts concluded that it would be reasonable to apply the law of blockade in military operations planned to block cyber communications in a territory under the control of the enemy (SCHMITT, 2017b, p. 505).

way that does not interfere with the rights of neutral states. The minority of the group of experts applied this paradigm strictly to the cyber context, and came to the conclusion that it would be conceptually impossible to establish a cyber blockade along the lines set out in the San Remo Manual. The majority concluded that a cyber blockade is a meaningful notion, in the context of naval warfare, because it can be effectively launched only from a belligerent territory without breaking the neutrality of adjacent states (SCHMITT, 2017b, p. 505).

The international group of experts discussed a great deal about the effectiveness of a classic naval blockade and its application to cyber blockades. A minority of experts considered that sufficient effectiveness was unattainable, because the communications to be blocked could be obtained by other means, such as radio and telephone. However, most experts pointed out that the transportation of materials by air that cannot be transported by sea due to a naval blockade does not render the naval blockade ineffective, and vice versa (SCHMITT, 2017b, p. 506).

A naval cyber blockade can be completed by means other than cyber, such as: combining cyber operations (denying access to an internet router by modifying routing tables), with an electronic warfare action (employing interferers to affect the enemy's radio transmissions) and with kinetic means as well (knocking out the internet service and destroying the enemy's internet centers by means of an air strike or naval bombardment). However, care must be taken that such actions do not affect neutral states (SCHMITT, 2017b, p. 506).

In short, some experts completely rejected the idea ofadapting the cyber naval blockade to the existing rules for the traditional naval blockade in the San Remo Manual. Other experts accepted this adaptation conceptually, but understood the practical difficulty of adapting the concepts, or even had different approaches to applicability in the cyber context. Some others believed that the concept of a cyber naval blockade is legitimate, is in line with the DICA, is adaptable to the traditional concept of a naval blockade and is feasible from a practical and technical point of view. Given that the experts were unable to reach a minimum consensus on the possibility of establishing a naval cyberblockade, articles 128 to 130 are limited to addressing how cyber operations can be used in support of the classic naval blockade.

Conducting cyber operations in support of a naval blockade can be an excellent tool in the hands of a commander in order tomaintain the

effectiveness of the blockade. Cyber operations aimed at remotely accessing a ship's propulsion and navigation system is a good example of the type of operation that could be used in support of a naval blockade. It should be noted that any use of cyber means or methods in the context of a naval war to reinforce a blockade will be subject to the rules for the conduct of naval warfare. The distinction between civilian and military objectives and the principle of proportionality must be observed. If cyber operations in support of the naval blockade cause damage to the civilian population, to neutral ships or are disproportionate to the military advantage achieved, this blockade will be illegal. Cyber actions in support of the blockade cannot affect neutral countries' access to their cyber structures or cyber communications.

Regarding the application of the concept of "naval exclusion zones", already established in the naval doctrine of most states, since the edition of the San Remo Manual, such zones are not areas of free fire or unrestricted warfare. Rather, they are areas that are specifically demarcated, in a theater of maritime operations, which remain bound by international law applied to naval warfare. Neutral ships and other means that enjoy protection under international law preserve their protection when crossing such zones, even if they ignore the instructions of the belligerent party that established the zone (SCHMITT, 2017b, p. 508).

With regard to the establishment of a cyber "naval exclusion zone", according to the experts, two contexts were analyzed: the use of cyber means and methods to reinforce the establishment of a "naval exclusion zone" and the actual establishment of a "cyber naval exclusion zone". The first approach can be implemented, as was seen with regard to the naval blockade. As for the second approach, the experts emphasized the difficulty of delimiting a "zone" in cyberspace. In addition, complying with the San Remo Manual's recommendations for establishing a "naval exclusion zone" can be technically challenging, since in many cases cyber communications can be based on cyber infrastructure over which the operator has no control. Thus, establishing a "cyber exclusion zone" at sea, from the point of view of international law, is quite difficult. Cyber detection actions can be employed to benefit the control activities of an Exclusion Zone, as well as operations that provide a cyber visit to ships suspected of flouting the rules of the zone (SCHMITT, 2017b, p. 508).

## CONCLUSION

The Information Age has come to completely change the art of war. In addition to the devastating kinetic weapons known to mankind for a long time, a new dimension of combat has emerged, whose technological paraphernalia, despite acting in a sneaky and sub-reptitious way, has an extremely lethal potential, capable of causing anything from simple data jams to large-scale destruction and death. State sovereignty, once an unshakeable element of evidence of state power, enters the 21st century under serious threat from this new dimension of war. Cyberspace, which until then had been the stage for anarchy, meets international law and slowly obtains the outlines of legality that are useful for maintaining international peace and security.

As far as naval warfare is concerned, there is still a considerable way to go,but the regulation of cyber operations carried out on board ships, under the focus of International Humanitarian Law, can already be considered an extremely important step for the context of war at sea.

Care and diligence must be taken with the cyber defense of the Blue Amazon. Brazil needs to be attentive to the work, albeit slow, of standardizing cyberspace, so that its strategic interests are not affected.

It is believed that, in the not too distant future, the warriors will present themselves in segregated compartments, secret bases, to engage in a different kind of combat, which, in contrast to the peculiar silence and clandestinity, will prove frighteningly threatening.

# INTERNATIONAL LAW AND THE CYBER DEFENSE OF SOVEREIGNTY IN THE BLUE AMAZON: AN APPROACH IN THE LIGHT OF THE TALLINN 2.0 MANUAL

**ABSTRACT**

In 2013, the first Tallinn Manual on International Law Applicable to Cyber Operations was published and that manual referred only to cyber operations in times of war. The second manual, published in 2017, also considered cyber operations carried out in peacetime. Bearing in mind the importance of the regulation of cyberspace for naval warfare, this article proposes to analyze the rules suggested by the emerging International Law Applied to Cybernetic Operations, for activities that are carried out in the context of naval operations. Thus, the research employs the literature review method, based on primary and secondary sources, such as the report of the UN Governmental Experts Group (UNGGE), the Tallinn 2.0 Manual and scientific articles on the subject. It is noteworthy that Tallinn Manual 2.0 promoted the meeting of the emerging International Law Applicable to Cybernetic Operations with the consolidated Law of "Naval War". This meeting generates legal perceptions that must be carefully evaluated.
Keysword: International Cyber Law; Cyberwarfare; Naval Operations.

**REFERÊNCIAS**

ACCIOLY, Hildebrando; SILVA, Geraldo Eulálio do Nascimento. Manual de Direito Internacional público. 12. ed. São Paulo: Saraiva, 1996.

BHATTI, Jahshan; HUMPHREYS, Todd. Hostile control of ships via false GPS signals: Demonstration and detection. Journal of the Institute of Navigation, [S.L], v. 64, n. 1, p. 51-66, 2017.

BRASIL. Decreto no 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília – DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 11 set. 2021.

BRASIL. Decreto nº 75.963, de 11 de julho de 1975. Promulga o Tratado da Antártida. Brasília – DF: Presidência da República, 1975.

BROZOSKI, Fernanda Pacheco de Campos. A Disputa Global por Recursos Energéticos Oceânicos e sua Repercussão na Geopolítica Mundial da Energia. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 25, n. 1, p. 63-88. jan./abr. 2019. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/796. Acesso em: 28 set. 2021.

CHOY, Yeong. Prescriptive Jurisdiction in the Law of the Sea: Cases of Contentions and Evolution. Journal of Territorial and Maritime Studies, [S.l.: s.n.], 2019. Disponível em: https://www.journalofterritorialandmaritimestudies.net/post/2019/12/13/prescriptive-jurisdiction-in-the-law-of-the-sea-cases-of-contentions-and-evolution. Acesso em: 23 set. 2022.

CORN, Gary; TAYLOR, Robert. Sovereignty in the age of cyber. In: Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. American Journal of International Law, EUA, v. 111, p. 207-212, 22 Aug. 2017. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70. Acesso em: 10 jul. 2021.

FAHEY, Sean. Combating “ciber fatigue” in the maritime domain.

Humanitarian Law & Police, [S.l.: s. n.], 7 Dec. 2017 Disponível em: https://blogs.icrc.org/law-and-policy/2017/12/07/combating_cyber- fatigue-in-the-maritime-domain/. Acesso em: 22 set. 2021.

FERREIRA, Pinto. Teoria Geraldo Estado. 2. ed. ampliada e atualizada. São Paulo: José Konkino Editor, 1958.

GHAPPOUR, Ahmed. Tallinn, Hacking, and Customary International Law. Boston University School of Law, [S.l.], v. 111, n. 224, 24 Aug. 2017. Disponível em: https://ssrn.com/abstract=3024380. Acesso em: 22 set. 2021.

HABER, Eldar. The Cyber Civil War. 44 Hofstra Law Review, [S.L.: s.n.], v. 41, 7 Dec. 2015. Disponível em: https://ssrn.com/abstract=2699644. Acesso em:17 ago. 2021.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Convenção XIII: Direitos e deveres das Potências neutras na guerra naval. Haia, 18 Oct. 1907. Disponível em: Disponível em: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/240. Acesso em: 12 de set. 2021.

JOHNSON, David Reynold; POST, David G. Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review, [S.l.: s.n.], v. 48, p. 1-1367, 1 Feb. 1996. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535. Acesso em: 17 out. 2021.

MANUAL San Remo de Direito Internacional Aplicável a Conflitos Armados no Mar. Direito Internacional sobre a conduta de hostilidades, Comitê Internacional da Cruz Vermelha - CICV, Suíça, 1996.

MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. Melbourne Journal of International Law, [S.l.], v. 14, n. 155, p. 1-496, 2013. Disponível em: https://ssrn.com/abstract=2557517. Acesso em: 15 jun. 2021.

MCLAUGHLIN, Stephen. et al. The cybersecurity landscape in industrial control systems. Proceedings of the IEEExplore, [S.l.], v. 104, n. 5, p. 1039-1057, 2016.

MELLO, Celso D. de Albuquerque. Curso de direito internacional público.

v. II. Rio de Janeiro: Renovar, 1992.

MONTEIRO, Renato Leite. The Balance between Freedom and Security in the Age of Surveillance: a Brief Analysis of the Recent Intelligent Electronic Surveillance Scandals. SSRN, 2014. Disponível em: https://ssrn. com/ abstract=2468060. Acesso em: 15 ago. 2021.

OLIVEIRA, Liziane Paixão Silva. A soberania frente à globalização. Revista do Programa de Mestrado em Direito do UniCEUB, Brasília, v. 2, n. 1, p. 202-225, jan./jun, 2005.

ONUF, Nicholas Greenwood. Sovereignty: outline of a conceptual history. Alternatives: Global, Local, Political, [S.l.], v. 16, n. 4, p. 425-446, 1991.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. Convenção das Nações Unidas sobre o Direito do Mar. Convenção de Montego- Bay, 28 jul. 1994. Disponível em: https://www2.camara.leg.br/legin/fed/ decret/1990/ decreto-99165-12-marco-1990-328535-publicacaooriginal-1- pe.html. Acesso em: 12 set. 2021.

PENA, Rodolfo Alves. Era da informação. [S.l.]: Mundo Educação, 2013. Disponível em: https://mundoeducacao. bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 13 ago. 2021.

RABOIN, Bradley. Corresponding Evolution: International Law and the Emergence of Cyber Warfare. National Association of Administrative Law Judiciary, [S.l.], v. 31, n. 2, 2011. Disponível em: https://digitalcommons. pepperdine.edu/naalj/vol31/iss2/5. Acesso em: 17 ago. 2021.

REIS, Marcos; SANTOS, Tamiris P. Análise das Ameaças Transnacionais Contemporâneas no Entorno Atlântico Brasileiro: A Terceirização da Segurança e a Revisão Dos Estudos de Política de Defesa. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 211-229, jan./ jun. 2014. Disponível em: https://revista.egn.mar.mil.br/index.php/ revistadaegn/article/view/195. Acesso em: 20 jul. 2021.

RIBEIRO, António Silva. A Expansão dos Direitos Soberanos nos Oceanos. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 19, n. 2,

p. 269 - 276, jul./dez. 2013. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/198. Acesso em: 17 mar. 2021.

RICHARD, Clarke; KNAKE, Robert. Cyber war: the next threat to national security and what to do about it. New York: Ecco, 2010, 320 p. [Reprint edition].

ROCHA, Marcio; FONSECA, Daniel Farias da. A Questão Cibernética e o Pensamento Realista. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 25, n. 2, p. 517-543 maio/ago. 2019. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/849. Acesso em: 21 jul. 2021.

SALDAN, Eliane. Os desafios jurídicos da guerra no espaço cibernético. 2012. 118 fl. Dissertação (Mestrado em Direito Constitucional) – Instituto Brasiliense de Direito Público, Brasília, 2012.

SCHMITT, Michael. Grey Zones in the International Law of Cyberspace. Yale Journal of International Law, [S.l.], v. 42, p. 1-21, 2017a. Disponível em: https://www.yjil.yale.edu/grey-zones-in-the-international-law-of-cyberspace/. Acesso em: 13 jul. 2021.

SCHMITT, Michael. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017b.

SHACKELFORD, Scott. Estonia Two-and-A-Half Years Later: a progress report on Combating Cyber Attacks. Journal of Internet Law, Forthcoming, [S.l.], 2009. Disponível em: https://ssrn.com/abstract=1499849. Acesso em: 17 out. 2021.

STOCKBURGER, Peter Z. Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum. American University International Law Review, [S.l.], v. 31, n. 4, 2016. Disponível em: https://digitalcommons.wcl.american.edu/auilr/vol31/iss4/2/. Acesso em: 22 ago. 2021.

VIDIGAL, Armando Amorim Ferreira; BOAVISTA, Marcílio. Amazônia Azul: o mar que nos pertence. Rio de Janeiro: Record, 2006.

WATTS, Sean; RICHARD, Theodore T. Baseline territorial sovereignty and

cyberspace, 2018. Lewis & Clark Law Review, [S.l.: s.n]. Disponível em: https://ssrn.com/abstract=3142272. Acesso em: 13 jul. 2021.

*** Received on December 0, 2021, and approved for publication on September 15, 2022.**