International Journal of Maritime Policy
Vol. 4, Issue 13, Spring 2024, pp.61-89
DOI: https://doi.org/10.22034/irlsmp.2024.316542.1058
ISSN: 2717-4255

Cyber Warfare from the Perspective of the Law of Naval Armed Conflict

Behzad Seify[1]*, Rasul Hamidpourrazian[2]

Received: 02 September 2023 Accepted: 27 February 2024 Published: 26 Mach 2024

Abstract

Background and Theoretical Foundations: The traditional military technologies and methods at sea have undergone many changes since the approval of naval warfare documents and have developed in such a way that they will transform future naval wars, and these developments necessitate the transformation of rights. It leads to a naval war. Cyber war has been accepted as one of the methods of war along with other land, sea, air, and space methods, but the difference between this method and other methods is that each of the mentioned territories can be used as a base to carry out a cyber-attack. The emergence of cyber capabilities in the sea means that naval forces are always more connected which leads to greater vulnerability at sea. The purpose of this brief is specifically to examine the cyber-attack at sea from the perspective of the law of maritime armed conflicts. Therefore, the ability to apply international humanitarian law and the rules governing the law of maritime warfare in the case of a cyber-attack at sea will be interpreted and investigated.

Methodology: The research method of this article is descriptive and analytical, and the process of collecting library information is reference, by referring to sources through books, documents, periodicals, and the Internet, we obtain research data.

Findings and conclusion: The findings of the research indicate many ambiguities in applying the law of maritime conflict to maritime cyber warfare, but humanitarian law can be used with all modern tools, which has been supported by the International Committee of the Red Cross in recent decades.

Keywords: Cyber Warfare, Naval Conflict, Humanitarian Law, Internet.

[1].Assistant Professor of Law, Department of Law, Imam Khomeini Maritime Sciences University, Mazandaran, Iran, (corresponding author), Email: behzadseyfiii@yahoo.com
[2]. Lecturer of Islamic Jurisprudence and Law, Imam Ali University, Tehran, Iran

1. Introduction

In the international arena, alongside the observation of new actors and legal developments, there has been a notable increase in new weapons technologies (Saifi, 2019: 36). Simultaneously, the cyber issue has raised numerous concerns. Presently, disruptions in the cyber domain have far-reaching implications across all aspects of human life. Of particular significance is the high level of integration of military and civilian components in cyberspace (Lin, 2011: 141). Consequently, governments have consistently stressed their entitlement to exert control over cyber infrastructure situated within their territories (Heinegg, 2012: 10).

One of the uses of tools and methods in cyberspace is their application in armed conflicts. Internet attacks in the virtual space, referred to as "information war" or "cyber war," represent a form of warfare where parties utilize computers and computer networks, particularly the Internet, as means to employ war tools and conduct battles in the virtual realm. In such warfare, the intensity of attacks and resulting damages can surpass those seen in traditional conflicts. The utilization of means and methods of warfare in cyberspace is akin to weapons of mass destruction and, in certain instances, may even exceed the severity of nuclear weapons (Ziai Bigdli, 2014: 265). Presently, the utilization of cyber activities as tools of war has gained acceptance, exemplified by incidents like the deployment of the Stuxnet worm virus in an attack on Iran's nuclear reactor (Hitchens, 2011: 61). Consequently, in cyber warfare, the entire global Internet serves as a potential battlefield, with billions of electronic devices acting as potential combatants (Conti, Nelson, Raymond, 2013: 287). As cyberspace represents a layer that intersects all actors, it faces significant risks of widespread disruption, leading to its emergence as a distinct arena for conflicts hosting a unique form of armed confrontations (Dombrowski, Demchak, 2014: 76).

Cyber attacks are actions carried out by a government or individuals acting on behalf of the government to target the critical infrastructure of another government, such as the banking system, energy sector, public transportation, and other systems connected to computer networks. It is important to note that while private individuals may engage in such actions due to the unique nature of cyberspace, cyber attacks discussed here are those conducted by or with the support of governments, as only such attacks can trigger the international responsibility of the government (Ziaei & Khalilzadeh, 2012: 35). According to the Tallinn guidelines, a cyber attack is defined as an "attack on a computer network," involving operations that manipulate, disrupt, deny, degrade, or destroy information on computers and networks, or gain control over designated networked computers. In response to a cyber attack, the affected country may employ civilian countermeasures against the attacking government (Halmi, 2007: 393). It is evident that cyber warfare takes place in the electronic realm (Giles & Hagestad II, 2013: 419).

Currently, it can be asserted that approximately 140 countries are actively engaged in the development of cyber warfare programs (Lülf, 2013: 36). In the maritime domain, naval forces acknowledge the significance of cyberspace as a critical determinant. For instance, NATO, as a maritime alliance, recently announced the establishment of a cyber operations center (Thiele, 2018: 13). Conversely, the Russian Navy is enhancing its capabilities. In tandem with Russia, emerging powers such as China and Iran have bolstered their maritime involvement, not only through commercial endeavors but also by expanding the reach and presence of their naval forces across diverse maritime regions. For instance, in the South China Sea, China is constructing artificial islands, enlarging rocky outcrops, and installing air and naval facilities, as well as anti-access systems and barriers to deter potential intrusions and attacks (Thiele, 2018: 2).

In recent years, the US Navy has implemented numerous initiatives in response to cyber warfare threats at sea. These measures include the establishment of the cyber command within the 10th Fleet to safeguard and defend cyber networks against internet attacks, the Naval Intelligence Command tasked with developing information technology policies and guidance, and the Intelligence Forces Command responsible for organizing, training, and equipping cyber security task forces. Notably, Admiral Jonathan Grunt, Chief of Naval Operations, and Sean Stockley, US Undersecretary of the Navy for Research, Development and Acquisition, authorized the Cyber Force Operational Readiness Directive in August 2014. This directive aimed to enhance the cybersecurity of Navy systems, vessels, and coastal structures while identifying effective solutions to bolster defense capabilities (Norton, 2016: 24-25). Furthermore, findings from the 2012 IT Strategy Training Report of the US Navy indicate that the nation's cyber operations policies primarily emphasize defensive strategies (Adkisson, Davies, Evans, Lanchantin, Walters, 2012: IV).

In naval warfare, the development of precision weapons in both offensive and defensive sectors has long been a priority, aiming to reduce barriers to the use of force and minimize collateral damage. This has led to increased legitimacy of the tools of war (Halchin, 2002: 243-254). Similarly, in the realm of cyber operations, these conditions may also apply. The operational environment, whether on land, sea, or air, plays a significant role in determining the appropriate rules of the law of armed conflict. In the case of cyber attacks, the location of the hardware used to carry out the attacks has a substantial impact on determining the applicable rules (Henderson, Dulk, 2015: 483). For instance, if a cyber attack is initiated from a warship or a research eavesdropping vessel primarily equipped with computer and electronic systems but directed through a land-based network, a question arises regarding which laws govern such an attack. Would the law of sea warfare apply to this scenario, or would it involve the law of land warfare, or perhaps both?

It is evident that significant changes have occurred in traditional naval military technologies and methods, which have evolved far beyond those present at the time of the establishment of naval warfare doctrines. Moreover, modern military equipment and methods in naval operations have been developed in a manner that is poised to shape future naval conflicts. Consequently, it is foreseeable that these advancements will necessitate revisions to the laws governing naval warfare, with these regulations being influenced by the evolving technologies. The advent of cyber capabilities has resulted in increased interconnectedness among naval forces, thereby rendering them more susceptible to vulnerabilities while operating at sea. As new opportunities arise, so do corresponding vulnerabilities. This study focuses specifically on cyber attacks in maritime environments, exploring the existence of cyber warfare at sea and its potential interpretation within the frameworks of international humanitarian law and the rules governing naval warfare. The research methodology employed is descriptive analysis, with information gathered through library and documentary sources.

2. Cyber Attack From the Perspective of the International Law

According to NATO studies, cyberspace is considered a crucial geographical dimension that encompasses land, air, sea, and space. Cyber operations permeate all aspects of the world (Waxman, 2011: 147). Essentially, the location of cyber specialists, whether in a closed-door basement or on the deck of a ship, does not impact their role in cyber operations. Every time a sailor, civilian, or contractor accesses a Navy computer system and connects to Navy networks, they are entering the cyber battlefield at sea (Norton, 2016: 26). Within this domain, activities have emerged that challenge established parameters such as purpose (military versus civilian), consequences (copy versus original), guidance (direct versus indirect), and continuity (short-term versus long-term), presenting complexities for international law frameworks related to warfare and the use of force (Lin, 2011: 143).

Cyber attacks present significant challenges, particularly when carried out through informal means. Unlike traditional warfare, these attacks are based on electronic information in the form of binary code (zeroes and ones), which raises questions about the legitimacy of armed defense (Lin, 2011: 142). Recent incidents have underscored the growing expertise and technical capabilities in utilizing cyber operations as a new tool. Notable examples include the 2007 operation targeting Estonia's communications infrastructure and the deployment of Stuxnet, a computer worm designed to disrupt Iranian nuclear facilities. These events occurred during peacetime, prompting inquiries into whether such operations could be classified as armed attacks under the provisions of the United Nations Charter, potentially justifying legitimate defense under Article 51. In contrast, the 2008 conflict between Russia and Georgia exemplifies cyber activities during armed conflicts, falling under the purview of international humanitarian law. This conflict highlighted the susceptibility of governments to cyber attacks, as demonstrated by Georgia's limited military response to Russia's conventional operations. By disrupting command and control capabilities, Russia amplified the impact of traditional warfare tools (Lülf, 2013: 37).

Currently, there are no clear examples of cyber attacks during armed conflicts or instances where civilian populations have been severely impacted by computer network attacks in such scenarios. However, technical experts acknowledge the potential for catastrophic outcomes, such as collisions between aircraft, the release of radioactive materials from nuclear power plants, the dispersion of toxic chemicals from factories, or disruptions to critical infrastructure and services like electricity and water networks, which cannot be ruled out (Droege, 2012: 539). Therefore, cyber techniques could be utilized to cause tangible physical harm, such as inducing collisions between military aircraft. Additionally, there exist non-physical cyber attacks that may not result in casualties, damages, or injuries but can impede information flows, communication channels, and lead to data corruption. In general, the law of armed conflict does not explicitly address issues related to cyber attacks. Nevertheless, this does not imply that their use is unrestricted or that they operate in a legal void (Lülf, 2013: 37). It is evident that when cyber operations are intertwined with physical conflicts, they are categorized as armed conflicts, and humanitarian law fully applies to all cyber operations connected to warfare, irrespective of whether they are initiated by governmental bodies, non-governmental entities, or individual hackers (Schmitt & Vihu, 2016: 29).

The most appropriate definition of a cyber attack appears to be one based on the target, as it allows for the use of any means to carry out such an attack. In contrast, defining cyber attacks based on the end rather than the means presents three key advantages. Firstly, this approach offers clarity and distinguishes between technologically advanced conventional warfare, as exemplified by using a computer network in Nevada to control a drone for a physical attack in Pakistan, and a true cyber attack like cutting submarine network cables to disrupt information flow between continents. This perspective aligns with the United States Department of Defense's view of physical attacks as a strategic component of cyber offensive operations. Secondly, adopting a goal-oriented perspective is logical and necessary in the context of evolving warfare, where traditional military operations span air, land, sea, and space, with cyber space emerging as the fifth dimension. Military forces historically organize around territory rather than specific platforms, with each force tasked with controlling its respective domain. Thus, access to various tools and weapons—including planes, ships, missiles, artillery, and computer networks—is essential for territorial control. Similarly, a cyber command need not exclusively rely on computer networks but should possess the capability to defend cyberspace using any means necessary. Lastly, defining cyber attacks based on means poses significant risks that can be mitigated by focusing on the end goal. As cyber technology use inherently threatens stability, tool-centric cyber warfare may inadvertently restrict online freedom of expression and political dissent. The primary aim of a cyber attack is to disrupt the functioning of a computer network, which can be achieved through various methods such as worms, viruses, Trojan horses, and service-disrupting attacks. (Hathaway et al., 2012: 11-13).

Therefore, when the military employs cyber weapons to disrupt civilian infrastructures with dual military and civilian functions, it constitutes an armed attack (Kelsey, 2008: 1435). In these instances, the anticipated outcomes of death, injury, damage, or destruction serve as pivotal factors in defining the attack (Boothby, 2014: 61). The criteria governing cyber conflict within the framework of legitimate defense measures revolve around the legal principles of necessity and proportionality, which must be adhered to. The International Court of Justice recognized these criteria in the Nicaragua judgment and affirmed them in the context of oil platforms (Schmit, 2011: 593). By categorizing such incidents as armed attacks, the corresponding rights and responsibilities under international humanitarian law come into effect. This recognition underscores how emerging threats have expanded the military's role in safeguarding areas where the use of force is required to a lesser extent compared to traditional scenarios (Abdollahi, 2008: 268).

3. International Law Governing Naval Warfare

Naval **warfare**, led and commanded by submarines and warships, involves armed conflict carried out by naval ships. While traditionally defined as conflicts conducted from sea to land (Ziaei-Bigdali, 2014: 320), this definition no longer aligns with advancements in technology, weaponry, and legal frameworks governing naval armed conflicts. A contemporary understanding of naval warfare encompasses the use of tactics and military operations on, under, or above the sea, incorporating various methods and tools such as ships, submarines, naval mines, electronic warfare, and cyber warfare (Saifi, Sharifi-Tarazkohi, 2018: 71). The legal foundations of naval warfare were primarily established through international agreements during the late 19th and early 20th centuries, notably at the Hague Peace Conferences of 1899 and 1907. While older documents like the 1856 Paris Declaration on Smuggling of War remain relevant, subsequent efforts post-1907, including the 1909 London Declaration on War Smuggling and the 1936 London Protocol on Submarines, aimed to regulate rules and norms related to naval warfare. The 1949 Geneva Convention addressed humanitarian aspects of naval warfare but did not introduce new regulations. Principles of humanitarian law applicable in land warfare also extend to naval operations (Saifi, Majdafar, 2019: 41-42). In conflicts like the Arab-Israeli wars, the Vietnam War, India-Pakistan conflicts, and the Iran-Iraq war, issues surrounding the right to search and inspect neutral ships arose, highlighting tensions between this practice and international legal frameworks prohibiting the use of force in international relations.

When the negotiations for additional protocols to the Geneva Conventions were adopted in June 1977, Article 49, paragraph 3 of the First Protocol stipulated that the provisions of Part I (Articles 48-67) apply to any land, air, or sea warfare that may impact the civilian population, military personnel, or civilian targets on land (land war). These provisions also extend to attacks from the sea or air against land-based targets, while not overriding the rules of international law governing conflicts at sea and in the air. Warships and submarines are utilized for land-based attacks on ships or aircraft at sea during wartime (Saifi, Majdafar, 2019: 42). Regarding the potential application of the Additional Protocol rules to the civilian population or individuals during naval warfare, conflicting interpretations have arisen based on Article 49, paragraph 4 of the First Protocol. Paragraph 3 of Article 49 specifically excludes the application of Articles 67-48 in naval warfare, but other provisions of the First Protocol, particularly Articles 35-41, remain relevant. The initial section of the protocol addresses naval warfare's impact on the civilian population on land and can be invoked for attacks from the sea on land-based targets. The customary prohibition against targeting civilians or the population, as articulated in paragraph 2 of Article 51 of the First Protocol, applies when there is a potential for civilian casualties or harm (Saifi, Majdafar, 2019: 42).

4. Rules Governing Cyber Warfare At Sea

There are numerous uncertainties surrounding the application of naval warfare laws to naval cyber warfare, which has garnered increasing attention from the International Red Cross in recent years (Jeremy, 2013: 202). The challenge lies in balancing the enhanced capabilities of cyber warfare with the necessary adaptability to bolster the Navy's "cyber power," which has become an essential component for long-term naval operations. This integration of cyber capabilities has paved the way for the acceptance of tactics such as deception, camouflage, mobility, and the initiation of autonomous cyber operations independent of traditional naval assets. Presently, most naval forces possess the capability to effectively address systematic cyber threats and counteract the advantages that adversaries may have in terms of scale, proximity, and precision. The diverse technological framework supporting these operations plays a crucial role in safeguarding the Navy's cyber security (Dombrowski, Demchak, 2014: 89).

The challenges of cyber warfare at sea vary during cyber conflicts due to the interconnected nature of cyberspace platforms spanning multiple countries, enabling various governmental and non-governmental actors to infiltrate and operate within this domain (Dombrowski & Demchak, 2014: 82). Some scholars suggest that warfare in the open sea can be likened to conflicts in cyberspace. Several commentators have observed parallels in their regulatory frameworks, although they have not fully explored the implications of these similarities. Cyberspace, like the open seas, transcends national boundaries and serves as a crucial conduit for trade and communication (Rabkin & Rabkin, 2012: 205). However, this assertion may be challenged as the open sea is a natural phenomenon, whereas cyberspace is a human-created environment.

A merchant ship traveling at high speed may aim to capture an enemy merchant vessel. However, it cannot anticipate victory in a direct confrontation with an enemy warship, which typically possesses more potent weaponry. Enemy warships have the authority to treat a captured attacker as a criminal, while also having the ability to seize the attacker's assets in accordance with naval strategies. When considering potential cyber-attacks aimed at disabling distant targets, cyber-conflict initially appears analogous to traditional naval warfare, where there is no requirement to secure civilian cooperation in the target state. Conducting cyber attacks for seizure or disruption is not contingent on a specific geographical location. Nevertheless, governments engaging in cyber warfare are still bound by the general principles of humanitarian law and must implement precautionary measures to mitigate harm or damage to civilians.

During the 18th and 19th centuries, raiders would board and inspect commercial vessels, subsequently escorting the entire crew and cargo back to a home port before potentially scuttling the ship once the crew was safely relocated. Historically, there has been a shared interest among seafarers to collaborate in safeguarding against maritime perils. However, such limitations were less prevalent during the world wars of the 20th century, where the devastating impact of new technologies underscored the need for restrictive regulations post-war. Despite post-war efforts to establish rules, the United States and other Western nations insisted on retaining their rights to counter sea tactics (Rabkin & Rabkin, 2012: 206). In essence, armed conflicts and the principles of naval power offer valuable parallels for understanding cyber warfare (Rabkin & Rabkin, 2012: 210).

Underwater naval forces are typically less vulnerable to cyber attacks, allowing the electromagnetic spectrum to provide enduring benefits through "silent services." Cyber warfare strategies at sea represent a potent form of naval warfare, reducing concerns over delays in individual command and control, promoting independent tactical actions for cumulative impact. Conventional air and naval forces must be actively engaged to utilize such communication capabilities and are initially tasked with supporting blockades from a distance, thereby impeding enemy access to the area and targeting their operations. During defensive maneuvers, their responses will be bolstered by deep air and sea capabilities, enabling ships and aircraft to advance towards their objectives to execute missions through methods of deception and networking (Kline & Hughes, 2012: 39). In the interim, the provisions of international treaties can directly influence the conduct of information warfare operations. Consequently, while many contemporary international legal instruments may lack comprehensive regulations pertaining to information warfare operations, this gap may prompt the development of rules within the international legal framework. Should future circumstances demonstrate that unauthorized computer activities pose a significant threat to global peace and security, it is probable that members of the international community will endeavor to establish a stringent legal framework governing the tools and methodologies of cyber warfare (Delibasis, 2006: 18-19).

Considering the cyber activities of the past decade, there is uncertainty regarding the prospect of a new treaty or the development of new customary legal norms to govern them (Delibasis, 2006: 45). However, customary international humanitarian law is applicable to the conduct of belligerents and the utilization of all methods and tools of warfare without geographical limitations. The International Court of Justice, in its advisory opinion on the legality or threat of use of nuclear weapons, affirms that the principles and rules of humanitarian law are relevant in armed conflicts "in all forms of warfare and with all types of weapons" (Paragraph 86), including those that may emerge in the future (Other reports and documents, 2015: 1447).

4-1. Cyber Warfare at Sea and Humanitarian Law

Cyber attacks represent a novel and unfamiliar tool that cannot be directly equated with conventional weapons in all respects. However, when utilized in the context of armed conflicts, the legitimacy of their use is determined by international humanitarian law. The primary aim of these legal principles is to "regulate the competing interests of individuals arising from their interactions" (Bourbonnière, 2011: 161). Although cyber operations are not explicitly addressed in international humanitarian law regulations, the evolving nature of cyber technology and its potential to fundamentally alter the landscape of warfare have led to debates about the applicability of existing humanitarian laws to cyber warfare. Nevertheless, despite the absence of specific references to cyber operations, these activities are still bound by international humanitarian rules. As new technologies continuously emerge, international humanitarian rules have expanded to accommodate these advancements. Through overarching principles, humanitarian law governs all tools and methods of warfare, encompassing the use of various weapons (Droege, 2012: 540). Notably, Article 36 of the First Additional Protocol establishes a specific obligation for parties to adhere to the rules of international humanitarian law with regard to new technologies.

In the realm of technology, it is evident that cyber attacks can target critical infrastructure such as airport control centers, transportation systems, dams, and nuclear power plants, potentially resulting in significant humanitarian consequences by causing harm to civilians. Assessing the potential risks posed by such cyber attacks may initially be challenging, but delaying action until a comprehensive evaluation is completed could lead to catastrophic events (Kellenberger, 2011: 25). Numerous observers and international legal experts argue that humanitarian law serves as the most dependable branch of international law applicable to cyber warfare, as its principles constitute mandatory rules that must be upheld (US Department of Defense, 1999). It is important to note that many fundamental provisions of the Hague and Geneva Conventions, as well as the First Additional Protocol, have attained the status of customary international law, thereby imposing binding obligations even on states that are not party to these treaties.

In the realm of military cyber operations, a significant majority of these operations are typically cyber exploitation operations that do not clearly meet the threshold of an attack as defined in Article 49 of the First Additional Protocol. Even visible operations that may be perceived as attacks, such as those against Estonia and Iran, often lack clarity regarding their potential humanitarian consequences. Nonetheless, there appears to be a general consensus that the fundamental principles of humanitarian law are applicable to emerging threats of cyber warfare (Anil, 2011: 152). The International Committee of the Red Cross asserts that cyber warfare becomes a humanitarian rights issue under the following circumstances: 1) when warfare tools and methods are employed in cyberspace, and 2) when cyber operations conducted during an armed conflict result in harm to the enemy (Ziaei Bigdali, 2014: 266). It is emphasized by the International Committee of the Red Cross that international humanitarian law specifically applies to situations of armed conflict (Beard, 2014: 97). In essence, international humanitarian law is only invoked when cyber operations are conducted in the context of an armed conflict, thereby governing the rights and obligations in such scenarios (Ayalew, 2015: 215).

4-2. Convention on the Law of the Sea and Cyberspace

Governments have the ability to establish new norms pertaining to cyber warfare through alternative means. As one scholar has articulated, "From one perspective, norms concerning cyber warfare should be shaped through the development of customary norms and general principles, derived by analogy from well-established institutions such as the law of the seas, the law of naval warfare, and the law of air warfare, with input from experts, before serious consideration is given to a binding treaty" (Kelsey, 2008: 1450). Given the widespread acknowledgment that principles from existing non-cyber treaties can be extended to cyberspace, there exist a range of international agreements regulating governmental actions that can be broadly applied to online activities.

For instance, the 1963 Treaty on the Moon and Celestial Bodies was established with a focus on peaceful objectives. As a result, the launching of military cyber operations from the moon or other celestial bodies is explicitly prohibited (Schmitt & Vihu, 2016: 33). Another illustration of norm-setting in the realm of cyber warfare is evident in the International Civil Aviation Agreement. Firstly, all governments are bound by their commitment to prioritize the safety of national aircraft navigation under all circumstances and are prohibited from interfering with safety measures (The Chicago Convention, 1944: Art. 3(d), 28, 37). Secondly, states are forbidden from using any form of weaponry against civil aviation, which encompasses the utilization of cyber warfare tools and tactics (The Chicago Convention, 1944: Art. 3). Moreover, the 1982 United Nations Convention on the Law of the Sea stands as a significant international legal instrument that delineates applicable norms concerning cyber warfare activities at sea. Specifically, Articles 19, 109, and 113 of the Convention address cyber attack operations in maritime environments, providing guidelines to prevent cyber assaults targeting computer systems on ships (Hathaway et al., 2012: 61). By acknowledging the right of peaceful passage for all naval vessels through a State's territorial waters, the Convention mandates that such vessels refrain from engaging in activities that jeopardize the peace, order, and security of the coastal State (UNCLOS art. 19). The Convention outlines various forms of harmless jamming activities, each of which could form a crucial component of a cyber warfare operation.

Indeed, conducting cyber operations against a coastal state from naval vessels in the territorial sea of the coastal state constitutes a violation of the right of innocent passage, regardless of the fact that this treaty predates the emergence of sea-based cyber operations (Schmitt & Vihu, 2016: 33). Furthermore, the Convention mandates all nations to collaborate in suppressing unauthorized broadcasting of waves and signals from the high seas, while also ensuring the prosecution of individuals engaged in potential illegal broadcasting on the high seas through multiple procedural steps (UNCLOS 1982: Art. 109). Lastly, the Convention offers safeguarding for submarine cables (UNCLOS 1982: Art. 113). Article 113 of the Convention on the Law of the Sea necessitates states to enact domestic criminal legislation to penalize harm to submarine cables. These provisions establish legal mechanisms against cyber attacks that occur or originate from the high seas (Hathaway et al., 2012: 61).

4-3. Tallinn Directive: Applicable International Law on Cyber Warfare

The publication of the Tallinn Manual has been widely acclaimed in the realm of cyber warfare. Prepared with the objective of offering a comprehensive overview of the rules of international law relevant to cyber warfare (Chatterjee, 2015: 16), the Tallinn Manual on International Law Applicable to Cyber War 2013 aims to apply an extensive interpretation of the rules of international law, including the law governing the use of force and international humanitarian law, to cyber warfare. Commissioned by the NATO Cyber Defense Center, this manual was developed by a panel of experts and presents a valuable set of rules that offer reinterpretations reflecting diverse perspectives on complex issues associated with this emerging technology. The International Committee of the Red Cross participated in the consultation process with the expert group as an observer, although not all viewpoints were explicitly detailed in the manual (Droege, 2012: 541; Chatterjee, 2015: 16).

The Tallinn Manual is not a legally binding document, but it serves as a valuable resource for determining legal principles in the context of cyber warfare (Chatterjee, 2015: 16). While the Tallinn Manual does not require ratification as a treaty, it has emerged as a significant tool in shaping future agreements aimed at regulating cyber warfare (Sullins, 2013: 12). Furthermore, it has brought attention to novel legal issues in cyberspace and their impact on military operations, leading to the evolution and utilization of cyber capabilities. Key treaties relevant to armed conflict, such as the United Nations Charter on the use of force, the 1949 Geneva Conventions, and the 1977 Additional Protocols on international humanitarian law, play a central role in this domain. Given the broad applicability of cyber tools in conflict scenarios, the critical challenge lies in interpreting their norms within the context of cyber warfare. The Tallinn Manual, developed by an expert panel, has played a pivotal role in shaping this research focus. Despite its acknowledgment of the presumptive application of principles of the use of force and international humanitarian law, the Manual presents various scenarios where experts have not reached a consensus on the precise interpretation of cyber operations (Schmitt, Vihu, 2016: 34).

However, it appears that not all countries embrace the Tallinn guidelines universally. The limited representation of legal experts and national representatives involved in drafting the guidelines suggests that diverse viewpoints may not have been fully considered, unlike other established guidelines such as the San Remo Manual. The dissemination and citation of the Tallinn Manual may be crucial for its wider acceptance. Discrepancies persist among countries regarding the characterization of cyberspace, its territorial aspects, and temporal considerations, leading to divergent legal interpretations in many cases.

5. Technical and Legal Challenges of Cyber War At Sea

The escalating utilization of new technologies in modern armed conflicts has engendered numerous challenges. The advent of advanced weaponry, satellite technology, cyber warfare, and other innovations has posed a threat to the established framework of international humanitarian law (Mirachian, 2011: 41). The proliferation of cyber attacks and cyber warfare presents a host of complexities, including the need for a comprehensive comprehension of cyber threats and attacks, the delineation of defensive and offensive measures in real-time, the interception of hostile actions targeting espionage activities in cyberspace, investigative concerns, and the attribution of attacks while safeguarding confidentiality (Waxman, 2011: 145-146).

In the maritime domain, ships are increasingly utilizing systems that rely on digitization, integration, and automation. Virtually all primary systems of ships, aircraft, submarines, and unmanned vehicles are interconnected and frequently linked to the Internet via satellite. This encompasses mechanical and electronic systems, weaponry, navigation systems, as well as control systems that heavily rely on positioning, navigation, and timing mechanisms such as the global positioning system and gyroscopes for navigation and weapon accuracy determination. These systems exhibit significant technical vulnerabilities, thereby heightening the risk of unauthorized access or malicious attacks on ship systems and networks (Thiele, 2014: 4). The sheer volume of data and its rapid transmission speed poses a threat to maritime operations. Essentially, in the realm of cyberspace, nearly all facets of artificial intelligence will eventually evolve into cyber capabilities.

In the context of adapting the rules of the law of armed conflict to the emergence of cyberspace as a theater of war, there remains uncertainty regarding the readiness of the Navy to engage in a diverse range of activities within this dynamic environment. The maritime domain, which has historically received less attention in terms of the application and adherence to the laws of armed conflict in cyberspace operations, presents challenges that necessitate naval forces to address and comply with these regulations. This raises questions about the implications of the law of armed conflict on naval personnel engaged in cyberspace operations (Adkisson, Davies, Evans, Lanchantin, Walters, 2012: III). Two fundamental principles govern cyber operations. Firstly, the deliberate targeting of civilians resulting in death or injury through cyber attacks is strictly prohibited. Secondly, additional protocols govern cyber operations (Henderson, Dulk, 2015: 484).

In naval warfare, as opposed to land warfare, a key consideration is the historical principle that maritime conflicts adhere to distinct rules. Unlike the evolving norms in land warfare during the 18th century, civilian property at sea has never been immune from attack. Disrupting enemy trade has consistently been a primary objective in naval warfare, a principle that has persisted into the 20th century (Rabkin & Rabkin, 2011: 204). Similarly, cyber warfare raises analogous concerns about disruptions impacting third parties. The fundamental aim in the law of armed conflict is to restrict attacks on combatants based on the principle of distinction, a concept underscored by the International Committee of the Red Cross when proposing the potential application of the law of armed conflict to cyber conflicts (Rabkin & Rabkin, 2011: 6). Some argue that extending rights designed for one form of warfare to all types of warfare, as suggested by the International Committee of the Red Cross, is erroneous. This viewpoint has led to efforts in the last century to develop international conventions specifically addressing the laws of war. Historically, distinct regulations have been established for maritime operations. While the Hague Peace Conventions of 1899 and 1907 resulted in a convention on "Laws and Customs in Land War," they also produced a separate set of conventions governing naval warfare, reflecting the differing tactics employed in land and sea conflicts. Challenges arise in achieving objectives in certain locations with strategic or tactical significance, often complicated by the presence of civilians (Rabkin & Rabkin, 2011: 6). The four Geneva Conventions do not impose specific limitations on targeting. The first Additional Protocol, arising from a conference dominated by third world countries, faced challenges in universal acceptance. The United States did not ratify it, and several regional powers such as Turkey, Iran, India, and Indonesia followed suit. Key NATO countries like Great Britain, Canada, Germany, and Italy ratified the document with significant reservations (Rabkin & Rabkin, 2011: 207).

Almost all the limitations of the First Additional Protocol were included in the Statute of the International Criminal Court in 1998. However, again, the United States and a significant number of other countries (including Russia, China, India, Pakistan, Egypt, Indonesia) refused to ratify the ICC Statute. Hence the Court's actual authority is somewhat ambiguous, often showing no close adherence to the standards of the First Additional

Protocol. Although each of these developments has had a significant impact, the majority of maritime powers, including a number of official signatories, consider the content of the First Additional Protocol as a guide for permissible tactics at sea. . Naval powers have spared no effort to get the rest of the world to bargain over how they legitimately use their naval power in times of war. Instead, the San Remo Directive provides for responsibility to prevent direct harm to civilians at sea and to prevent blockade measures that lead to starvation or severe deprivation of civilians on land.

Otherwise, it does not prohibit the targeting of the enemy's commercial ships at sea. This specifically results in imposing restrictions on the enemy's commercial vessels to hinder extensive long-distance shipping and their access to and departure from enemy ports. Consequently, it authorizes the interception of neutral ships when their cargo could be utilized in armed conflicts. The San Remo Directive seeks to apply the constraints outlined in the First Additional Protocol and the principles of land warfare to naval operations. The San Remo Directive on interventions at sea focuses on scenarios where a targeted vessel can be intercepted by naval warships, redirected to a naval home port, and potentially engaged without causing loss of life or physical destruction. It facilitates interventions in international waters in a straightforward manner (Rabkin & Rabkin, 2011: 208). The Tallinn Manual briefly touches upon the attribution of a cyber attack and its interpretation. In the short term, experts involved in drafting the Tallinn Manual only concurred that "there is no established law determining the permissibility of a cyber attack originating from an enemy vessel or one flying a neutral flag." Regrettably, there is no explanation provided as to why a cyber attack from an enemy aircraft (ship) should be treated differently from the launch of anti-aircraft missiles. Perhaps this issue will be elucidated in future editions of the manual (Henderson & Dulk, 2015: 485).

Cyber warfare at sea typically differs from other methods, with the primary objective being to disrupt and harass the enemy rather than capture and occupy their territory. One such tactic involves targeting the enemy's commercial ships to impede their trade, which necessitates adherence to the rules of naval warfare when dealing with surrendered crews on warships or commercial vessels (Rabkin & Rabkin, 2011: 6). In the 20th century, advancements in radio communications enabled merchant ships under attack to swiftly seek assistance from allied warships, complicating the boarding process and ensuring the safety of crew members before any potential sinking. However, submarines and aircraft emerged as formidable weapons during this period, lacking the capability to conduct rescue operations or inspect the ships they targeted, resulting in deadly surprise attacks during World War I by the belligerent parties (Rabkin & Rabkin, 2011: 7).

It is evident that the seizure of merchant vessels is a prevalent aspect of naval warfare, driven in part by economic motives. This practice allows governments to extend their maritime influence without the expense of maintaining a large fleet, offering diplomatic and strategic advantages. Launching commercial attacks becomes crucial for inflicting harm on another government without resorting to outright warfare (Rabkin & Rabkin, 2011: 8). This scenario presents striking parallels with cyber warfare, where a diverse array of civilian facilities fall victim to cyberattacks. During the world wars, there was a stance advocating that merchant ships remain vulnerable to attack. In the initial stages of both conflicts, British and French authorities were apprehensive about significant American responses and reactions to their policies, particularly in areas where American interests were directly impacted. Throughout the first year of World War I, caution prevailed regarding imposing stricter restrictions on neutral trade with Germany. The protests of smaller neutral powers like the Netherlands and Sweden, whose maritime activities were severely curtailed by Allied blockades in both world wars, largely went unheeded by the major powers. Towards the end of the conflict, the Allies opted to implement a system permitting neutral shipping access to the Atlantic Ocean, subject to inspection by Allied officials at loading ports or through boarding at sea, including inspections even in neutral harbors. Despite objections from neutral nations, this system was enforced in accordance with Allied dominance at sea. The extensive control exerted by the Allies drew criticism and undoubtedly constrained business opportunities. Nevertheless, the restrictions imposed on neutral vessels by the Allies did not elicit the same outrage as submarine attacks, as they did not pose a direct threat to the lives of crew members or passengers, thereby justifying the limitations on engagement. In the 21st century, cyber warfare should be conducted in a manner that safeguards civilian lives and avoids escalating to levels of severe casualties rapidly.

The current challenge lies in questioning the specific rules that have developed regarding the application of land warfare regulations, which have not universally acknowledged the general exemption of "civilian objects," encompassing nearly all aspects of commercial traffic that may become targets of military actions. The approach derived from naval warfare practices in the 20th century suggests that even a neutral state can implement defensive measures and strategic restrictions on itself if their implementation poses a threat to civilian lives. However, there are compelling arguments in favor of prioritizing humanitarian considerations, without necessitating the blanket application of "humanity" to policies concerning the exemption of civilians in all wartime contexts (Rabkin & Rabkin, 2011: 219-220).

Hence, based on the differentiation between land and sea warfare as distinct categories, it is imperative to classify cyber warfare within the latter framework. Indeed, cyber warfare initially shares more similarities with naval warfare tactics. In cyber conflicts at sea, there is a tendency to introduce minimal risks to civilians, resulting in substantial economic repercussions without directly endangering the lives of inhabitants. Analogous to historical naval raiders, cyber attackers typically refrain from engaging in direct communication with the civilian populace of the targeted nation. Consequently, cyber assailants are not bound by the regulations of that nation, thereby lacking immunity for engaging in hostilities against civilian populations (Rabkin & Rabkin, 2011: 7).

It is premature to conduct a comprehensive evaluation of the Navy's progress in cyber warfare at this stage. Nevertheless, considering the emerging perspectives within the Navy and the dynamic evolution of global cyberspace trends, it is evident that future military conflicts will be influenced by the cyber threats present in the maritime domain. The Navy is actively working towards establishing an organizational and operational framework to effectively address the impending cyber challenges. As emphasized by Admiral Jonathan Greennert, the Commander of Naval Operations, the operational virtual space, characterized by its capacity to manipulate a broad electromagnetic spectrum, attain information superiority, exercise temporal control, and impact our operations where necessary, will play a significant role (Dombrowski & Demchak, 2014: 82).

Various methodologies have been employed to regulate the use of military forces in both maritime and terrestrial environments under distinct sets of rules. However, it is plausible to consider cyberspace as a unique domain for armed conflicts, prompting a reevaluation of whether cyber attacks should be governed by the same conventional regulations that apply to ground warfare. Although cyber warfare bears resemblances to naval operations or engagements on the high seas, it does not imply an absence of legal frameworks governing cyber operations. Consequently, akin to the normalization of the use of force at sea, there is an expectation for cyber operations to become routine and adhere to the laws of armed conflict.

6. Blockade in the Manner of Cyber Warfare

International law seeks to constrain the impact of warfare to combatant armed forces while simultaneously safeguarding nations' legitimate ability to apply economic pressure on adversaries. The concept of blockade embodies this delicate balance, as it is both acknowledged and governed within the framework of the laws of war, concurrently enabling the imposition of economic constraints on civilian populations of hostile entities. Blockade rights have evolved within the maritime domain, empowering blockading forces to impede access to enemy ports through the utilization of visitation rights and, if required, the application of force (Midson, 2014: 84).

In accordance with international law, a blockade must be effective while also allowing access to neutral maritime territory. The effectiveness requirement does not preclude access to a state's territory; this issue is particularly relevant in the context of cyberspace, where decisions must be made regarding territorial boundaries within the cyber realm. Similarly, concerns arise regarding the prohibition of interference with neutral territory's cyber traffic, necessitating belligerent parties to determine the extent of cyber space within a neutral country's territory. One approach to this dilemma is to deny access to cyber infrastructure deemed effective for cyber blockade purposes or any physical cyber infrastructure located in another state's territory. However, this approach presents challenges, such as the difficulty in assigning mobile infrastructures to specific territories and discrepancies in determining the importance of certain infrastructure for providing internet services based on logical rather than physical location. Applying the principles of blockade rights to cyberspace is more intricate than initially perceived, with the potential for these rights to be redefined as new blockade methods emerge. The Minister of Defense of Estonia equates a cyber blockade to a naval blockade of ports that restricts a country's global access, underscoring the significance of adapting traditional concepts to the information age (Midson, 2014: 86; Gasemi, Chaharbakhsh, 2011: 127). Undoubtedly, cyber warfare can serve as a valuable complement to naval blockades, and it appears that it can be examined within the context of common law in this specific domain. Cyber techniques align with traditional blockade strategies, encompassing actions such as causing damage to port infrastructure through cyber methods, disrupting port services via attacks on software or service platforms, and interfering with positioning system services both within and outside a port (Toth, 2011: 10-11). These effects, which may include reduced port utilization, potential harm to ports or vessels due to maritime incidents, and cargo loss due to delays or errors in transportation, are directed towards a particular government or vessel under the jurisdiction of the flag state, thus warranting regulation based on geographically rooted rules. It is evident that during a blockade, virtual traffic in cyberspace should be taken into account alongside physical traffic if it proves to be effective, particularly given the significance of electronic commerce transactions. The physical infrastructure of the Internet enables governments to exert control over cyber communications through either physical means (such as damaging cables or servers) or cyber means. When these actions are conducted as part of a physical blockade, it appears that a common approach applies blockade rights to all activities. However, in cases where there is no physical blockade and the blockade is solely in cyberspace, enforcing blockade rights becomes challenging (Midson, 2014: 85).

A cyber blockade occurs when a series of cyber attacks significantly disrupt a government's network connectivity in cyberspace, leading to the impairment of that government's cyber operations (Lin, 2010: 64). Cyber blockades can be more effective than economic aggression as they often require minimal or no physical force (Jenkins V, 2005: 135). However, the absence of physical force does not negate the necessity for creating an impact; whether physical force is employed or not, cyber blockades are generally subject to the same regulations as traditional blockades. This determination is primarily based on an evaluation of whether force was utilized in the cyber blockade activities. Unlike traditional naval blockades, the concept of "use of force" is not easily applicable to cyber blockades unless it is interpreted as an economic embargo, which would place it beyond the scope of a blockade. If a cyber blockade is not deemed a use of force, then blockade rights would not be applicable, and the principle of non-interference in sovereign territory would be invoked. It may be argued that in instances where a government faces material consequences, regardless of whether physical harm is inflicted, such as disruption to cyberspace, it could be considered a use of force. However, historical reluctance to classify economic sanctions as coercive actions suggests that such measures are unlikely to be categorized as uses of force. Nevertheless, the extent of economic damage caused by cyber attacks could lead to different conclusions. With the increasing reliance on the Internet and the need for secure access within national boundaries, governments are likely to address the regulations governing cyber blockades more comprehensively. Blockade rights may indeed be applicable to cyber attacks (Midson, 2014: 85-86). Some argue that restricting access to communication networks can be likened to blocking access to sea or airspace (Valo, 2014: 63).

7. Conclusion

Cyber warfare has been acknowledged as a distinct method of warfare, alongside traditional land, sea, air, and space methods. One key distinction between cyber warfare and these conventional forms of warfare is that each of the aforementioned domains can serve as a launchpad for conducting cyber attacks.

In the maritime domain, the utilization of a ship equipped with radar and satellite systems primarily focused on information gathering and identification, or the installation of various cyber warfare systems, enables the launching of cyber attacks. These attacks can target critical infrastructure such as ports, docks, lighthouses, offshore oil platforms, missile systems, and other assets associated with a nation's naval vessels.

The potential disruption and destruction caused by these attacks underscore the need to adhere to fundamental principles of humanitarian rights, despite the absence of specific regulations governing cyber warfare at sea.

In conclusion, despite the absence of specific provisions in the Hague Naval War Conventions, the additional protocols of 1977, and other relevant documents addressing new technologies and military methods in naval warfare, these advancements have significantly influenced the development of naval warfare law. This evolution necessitates a thorough reexamination of the legal framework governing naval conflicts. The principles outlined in the Hague Naval War Conventions and humanitarian law can be applied to modern military technologies and methods due to their customary nature. Key rules in humanitarian law, human rights, international criminal law, and other legal frameworks safeguard the essential interests of the global community. Consequently, international law regulating naval armed conflicts recognizes the legitimate use of both traditional and modern naval warfare tools, including unmanned naval and cyber devices, as weapons in warfare. It mandates adherence to humanitarian norms, neutrality rights, and maritime laws. Moreover, restrictions grounded in humanitarian considerations and principles of necessity, proportionality, and distinction can also be imposed on these technologies and methods.

References

- Abdullahi, Mohsen, (1388), Human Rights Terrorism and Humanitarian Rights, Shahr Danesh Institute, Tehran.

- Anil, Suleyman, (8th-10th September 2011), “How to integrate cyber defence into existing defence capabilities”, International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.

- Ayalew, Yohannes Eneyew, (2015), “Cyber Warfare: A New Hullaballoo under International Humanitarian Law”, Beijing Law Review, 6, 209-223, Published Online December 2015 in SciRes. http://www.scirp.org/journal/blr, http://dx.doi.org/10.4236/blr.2015.64021

- Adkisson, James, Davies, Tokunbo, Evans, Brian, Lanchantin, Rick, Walters, Patty, (2012), “Law of Armed Conflict: Implications for Navy Cyber

Strategy', Information Networking Institute, Masters of Information Technology Strategy Practicum.

- Beard, Jack M., (2014), "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law", vanderbilt journal of transnational law [vol. 47:67.
- Bourbonnière, Michel, (8th-10th September 2011), "Law, technology and the conduct of hostilities in space", International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.
- Boothby, William H., "Where Do Cyber Hostilities Fit in the International Law Maze?" New Technologies and the Law of Armed Conflict, Ed: Nasu, Hitoshi, McLaughlin, Robert, (2014), The ANU College of Law Australian National University Canberra, ACT Australia, Springer.
- Chatterjee, Bela Bonita, (2015), "International Law and Cyber Warfare An agenda for future research", Lancaster University Law School/Security Lancaster.
- Conti, Gregory, Nelson, John, Raymond, David, (2013),"Towards a Cyber Common Operating Picture", 5th International Conference on Cyber Conflict, Podins, J. Stinissen, M. Maybaum (Eds.).
- Chatterjee, Bela Bonita, (2015), "International Law and Cyber Warfare An agenda for future research", Lancaster University Law School/Security Lancaster.
- Droege, Cordula, (Summer 2012), "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", International Review of the Red Cross, Volume 94 Number 886.
- Delibasis, Dimitrios, (February 2006), "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century Peace Conflict and Development" Interdisciplinary Journal, Issue 8.available from http://www.peacestudiesjournal.org.uk
- Dombrowski, Peter, Demchak, Chris C., (Spring 2014), "Cyber War, Cybered Conflict and THE Maritime Domain_Dombrowski-Demchak", Naval War College Reivew, Vol. 67, No. 2.
- Ghasemi, Ali, Chaharbakhsh, Viktorbarin, (Summer 2011), "Cyber Attacks and International Law", Judiciary Legal Journal, No. 78.

- Giles, Keir, Hagestad II, William Divided, (2013), Common Language: “Cyber Definitions in Chinese,Russian and English”, 5th International Conference on Cyber Conflict, Podins, J. Stinissen, M. Maybaum (Eds.).

- Herb, Lin, (8th-10th September 2011), “Operational reality of cyber warfare”, International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.

- Herb, Lin, (2010), “Offensive cyber operations and the use of force”, J Natl Secur Law Policy 4: 63-86.

- Helmi, Nusratullah, (2017), Development and development of international law: international responsibility of the government and political support, Tehran: Mizan, first edition.

- Heinegg, Wolff Heintschel von, (2012), “Legal Implications of Territorial Sovereignty in Cyberspace”, 4th International Conference on Cyber Conflict.

- Halchin, L. Elaine, (2002), “Electronic Government in the Age of Terrorism,” Government InformationQuarterly 19, no. 3.

- Hathaway, Oona A., Crootof, Rebecca, Levitz, Philip, Nix, Haley, Nowlan, Aileen, Perdue, William, Spiegel, Julia, (2012), “THE LAW OF CYBER-ATTACK”, Forthcoming in the California Law Review.

- Henderson, Ian, Dulk, Jordan den, Lewis, Angeline, (2015), “Emerging Technology and Perfidy in Armed Conflict”, 91 INT’L L. STUD. 468.

- Hitchens, Theresa, ((8th-10th September 2011)), “New technologies: science fiction or real world?”, International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.

- Lülf, Charlotte, (2013), MODERN TECHNOLOGIES AND TARGETING UNDER INTERNATIONAL HUMANITARIAN LAW, master thesis LL.M. in Public International Law. http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf

- Jeremy, Rabkin, Ariel, Rabkin, (2013),“Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea”, Chicago Journal of International Law, Volume 14 Number 1. Available at: http://chicagounbound.uchicago.edu/cjil/vol14/iss1/7

- Jenkins V, Antolin, (2005), “Defining the parameters of cyberwar operations: looking for law in all the wrong places?” Naval Law Rev 51.

- Kellenberger, Jakob, (8th-10th September 2011), “Keynote addres”, International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.
- Kline, Jeffrey E., Hughes, Jr., Wayne P., (Autumn 2012), “BETWEEN PEACE AND THE AIR-SEA BATTLE A War at Sea Strategy”, Naval War College Review, Vol. 65, No. 4.
- Kelsey, Jeffrey T.G., (2008), “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare”, Michigan Law Review [Vol. 106:1427.
- Mirachian, Laura, (8th-10th September 2011), “Statement”, International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.
- Midson, David, (2014), “Geography, Territory and Sovereignty in Cyber Warfare”, New Technologies and the Law of Armed Conflict, Editors: Nasu, Hitoshi, McLaughlin, Robert, the ANU College of Law Australian National University Canberra, ACT Australia, Springer.
- Nancy Norton, (SPRING 2016), “The U.S. Navy’s Evolving Cyber/Cybersecurity Story”, THE CYBER DEFENSE REVIEW.
- Other reports and documents, (2015), “International humanitarian law and the challenges of contemporary armed conflicts”, International Review of the Red Cross, Volume 97 Number 900 Winter.
- Schmitt, Michael N., Vihu, Liis, (2016),“The Nature of International Law Cyber Norms International Cyber Norms Legal”, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications.
- SCHMITT, MICHAEL N., (2011), CYBER OPERATIONS AND THE JUS AD BELLUM REVISITED, VILLANOVA LAW REVIEW [Vol. 56.
- Seifi, Behzad, (Autumn 2019), Legitimacy of using unmanned military underwater vehicles from the point of view of international law of the seas, Defense Policy Magazine, 28th year, number 111.
- Seifi, Behzad, Sharifi-Tarazkohi, Hossein, (Winter 2018), "Necessity of training in the law of armed conflicts (sea) in the armed forces with an emphasis on the personnel of the strategic navy of the Islamic Republic of Iran Army", Scientific Quarterly of Maritime Science Education, No. 19.

- Seifi, Behzad, Majdafar, Sohrab, (Spring 2019), "Examining the methods and technologies of naval warfare from the perspective of international humanitarian law", Scientific Quarterly of Maritime Sciences and Technology, No. 93.
- Sullins, John P., (2013), "An Ethical Analysis of the Case for Robotic Weapons Arms Control", 5th International Conference on Cyber Conflict.
- Rabkin, Jeremy A., Rabkin, Ariel, (2012), "An emerging threats ESSAY To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict, Koret-Taube Task Force on National Security and Law", Hoover Institution, www.emergingthreatsessays.com p 6.
- Thiele, Ralph D., (2018), Game Changer – Cyber Security in the Naval Domain, ISPSW Strategy Series: Focus on Defense and International Security, Januar.
- Toth, Michael H., (2011), Maritime trade warfare in the 21st century. Naval War College, Rhode Island.
- Valo, Janne, (2014), Cyber Attacks and the Use of Force in International Law, Master's Thesis University of Helsinki Faculty of Law International Law, Supervisor: LL.D. Jarna Petman.
- Waxman, Matthew, (8th-10th September 2011), "Cyber warfare: is there a need for new law", International Humanitarian Law and New Weapon Technologies, Editor Wolff Heintschel von Heinegg and Gian Luca Beruto, Sanremo.
- Ziyai-Bigdali, Mohammad Reza, (2014), International Humanitarian Law, third edition, Gaj Danesh Publications, Tehran.
- Ziyai, Sidyaser, Khalilzadeh, Mona, (Spring and Summer 2012), "The International Responsibility of the Government Due to Cyber Attacks", Scientific Journal of Promotion of Legal Research, No. 23.

Documents

- Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research at Harvard University, Bern, 15 May 2009.
- US Department of Defense, An Assessment of International Legal Issues in Information Operations (2nd edn, Washington, DC: US Department of Defense Office of the General Counsel, 1999).

- The Chicago Convention “Chicago International Air Services Transit Agreement, U. K. T. S. 8 1953 Cmd.
- 1982 United Nations Convention on the Law of the Sea, 1982, UN Doc. A/CONF. 62/122 and Corr. 1833 U.N.T.S 3; hereinafter: LOSC.
- Tallinn Manual on the International Law Applicable to Cyber Warfare 2013
- San Remo Manual on international Law Aplicable to Armed Conflicts at sea, June 1994.