*International Journal of Maritime Policy*
*Vol. 2, Issue 6, Spring 2022, pp.57-81*
*http://dx.doi.org/10.22034/irlsmp.2022.293324.1033*
*ISSN: 2717-4255*

# Naval Electronic Warfare from the International Humanitarian Law Perspective

Behzad Seify[1], Mansoor Lashani[2]

Received: 3 July 2021 Accepted: 9 March 2021 Published: 26 April 2022

**Abstract**

The naval conflict has undergone many changes due to environmental factors and various tools, as well as the increasing growth and development of marine technologies, aligned with the inclusion of new tools and methods in naval conflict and electronic warfare at sea. The procedure taken by countries indicates the acceptance of electronic warfare as one of the methods and tools of agreed warfare. However, from the perspective of international humanitarian law, the use of electronic warfare tools and methods is challenging, and international treaty law lacks a legal rule regarding this method of warfare. Indeed, the only guideline that has sought to regulate electronic warfare is the Air and Missile Warfare Directive, which imposes no legal requirements on governments. So the question we are going to answer in this brief is that, can humanitarian law be applied to electronic warfare? The purpose of this study is to explain and investigate the various dimensions of naval electronic warfare from the perspective of international humanitarian law, and proving that international humanitarian law can be applied to the methods and tools of electronic warfare at sea. The research method selected for the present paper is an analytical-explanatory method and the data collection method used is the library research method

***Keywords***: Humanitarian Law, Naval Electronic Warfare, Information Warfare, Manual;

---

[1]Assistant Professor Assistance Professor Public International Law University of Marine Science, Imam Khomeini (RA), behzadseyfiii@yahoo.com.

[2] PhD Student in International Relations, Lecturer at Imam Khomeini University of Marine Science.

## Introduction

The naval warfare has undergone many changes due to environmental factors and various tools, as well as the increasing growth and development of marine technologies, as a result, the use of new tools and methods in naval warfare are increasing. From the traditional point of view, naval warfare is an armed conflict that is led and commanded by submarines and warships and conducted by naval vessels (Ziaeibigdeli, 1994, p.11). However, this traditional definition of naval warfare, which originates from the previous rules and it is conventional, this definition is inconsistent with the use of new technologies and new tools and methods of warfare, as well as legal developments in the field of naval armed conflict, and calls for a more up to date definition. Hence, it seems that in a more general and complete definition, naval warfare means the use of tactics and the conduct of military operations on, below, or above the surface of the sea. In this definition, a combination of the two terms tactics and military operations, to some extent, various methods and tools of naval warfare, including the use of ships, submarines, naval mines, electronic warfare, etc., have been mentioned (Seify & Sharifi Traz Qvhi, 2020, p.71).

Electronics is one of the technologies that seems to have changed the naval war a lot. With the arrival of radio equipment and satellite links to the seas, navigation changed and with the use of these devices, sailors can sail more confidently not only in coastal but also in offshore areas of the seas or during unfavorable weather conditions. However, the mentioned technology exposes ships to the dangers of some methods of naval and electronic warfare. Electronic warfare at sea is defined as "a set of actions that cause the use of magnetic electronic spectrum against enemy ships and disrupts electronic systems, in such a way as to disrupt the operation of the ship's defensive and offensive systems. In return, the enemy also wouldn't be able to use their electronic systems too." (Adami, 2016:17).

"The air and missile warfare directive define electronic warfare as any military action, involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy" (Hitchnes, 2011: 61; HPCR Manual, Section A, Rule 1, Para (P)).

Electronic warfare at sea is both active and passive. A) Active electronic warfare is the propagation or re-propagation of electromagnetic waves to disrupt or damage the use and operation of the enemy's electronic devices or to mislead the enemy in interpreting the information received from its electronic devices. These proceedings include disruption, chaff, and flare used to interfere with the operation of radars, military communications, and heat ray weapons. This includes electronic countermeasures, which include anti-electromagnetic measures (jamming, chaff, and flare), as well as anti-reflection devices and directed energy weapons. B) Passive electronic warfare is the search and analysis of electromagnetic emissions to detect the existence of a source and the properties associated with the use of the electromagnetic spectrum. Moreover, electronic warfare provides ships with a tool that can counter infrared-guided missiles, which these countermeasures include, flares3, disruptors4, traps5 and infrared chaffs6 (Adami, 2016:18). Disrupting the navigation and telecommunication systems of warships, as well as tracking them and diverting or destroying their missile systems and torpedoes are what electronic warfare is concerned with.

Nowadays, more than twenty members of the international community, including the most prominent ones; The Unites States, Russia, China, Australia, and several EU members have worked hard to do so. For example, various elements of information warfare, including attacks on computer networks, as well as defense of computer networks, were widely used in the 1998 Kosovo war. In 2001 during Operation Enduring Freedom (OEF) in Afghanistan; in 2002, the tension between the People's Republic

[3] The most basic action against an infrared-guided missile is to fire a high-temperature flare shot from an aircraft or ship to confuse the missile locked on the target. This flare breaks the target lock of the missile and misleads it toward itself.

[4] Disruptors produce Infrared (IR) signals that attack conduction signals. These disruptors produce infrared signals similar to those generated by the IR energy of the target passing through the aperture. When the jammer signals and the target energy signal reach the missile IR sensor, they cause the tracker to generate incorrect commands.

[5] Traps can deviate missiles from a variety of protected platforms. Traps can be maneuvered both steadily and ambulatory in ways that increase the deviation of tracker weapons.

[6] If a substance with very high infrared characteristics enters the space from an aircraft or ship rocket launcher against infrared-controlled weapons, it provides the same defense capability as Chaff against radar-controlled weapons. Infrared Chaff, like radio frequency (RF) Chaff, used both to break the target lock of the missile and to increase the ambient temperature to make the tracking process more difficult.

of China and Taiwan information warfare was implemented. In 2003 in Operation Enduring Freedom in Iraq; in 2001 during the international peacekeeping operation "Belisi" led by Australian Defense Forces; finally, it was exploited in the conflict between the occupying regimes of Jerusalem and Palestine (Delibasis, 2006, p.4). Indeed, in recent conflicts, electronics have evolved as a "tool of war" and modern armies are developing information technology as a "method of warfare" (Schmitt, Dinniss, Wingfield, 2004, p.1). Recent developments also suggest the use of advanced information warfare systems, often referred to as network-centric warfare. This leads to careful military actions and the avoidance of unintended damage of electronic warfare (Jonsson,2008, pp.10-11). Moreover, nowadays several countries have conducted or conducting research programs on electromagnetic bombs. There are also limited reports of their use on the battlefield (Commentary on the HPCR Manual, 2010, p.36).

In this regard, the guidelines for air and missile warfare states that electronic warfare includes all actions taken against the enemy during an international armed conflict, whether by the armed forces or even by civilian forces such as intelligence agencies (Commentary on the HPCR Manual, 2010, p.36). Therefore, electronic warfare at sea and its tools are one of the agreed methods and tools of warfare. Thus, the use of electronic warfare in naval conflict is very important. Most naval tools and methods are like a double-edged sword. However, despite tremendous progress, international law seems incapable of meeting the challenges and the needs of the international community and it is falling far behind. Thus, from the perspective of international humanitarian law, the use of information warfare tools and methods such as electronics, the internet, and computers are challenging. So the question here is that, can humanitarian law be applied to electronic warfare? The purpose of this study is to explain and study the various dimensions of electronic naval warfare from the perspective of international humanitarian law.

The research method of the present article is analytical-explanatory. And the method of data collection is the library method of data collection, with

reference to sources through books, documents, periodicals, through web browsing and phishing we obtain the research data.

**1. Rules Governing Naval Electronic Warfare**

Although electronic warfare is now widely used as a method of warfare, it is not yet explicitly regulated or even discussed in contract law (Commentary on the HPCR Manual, 2010, p.36). It seems that the only guidelines that have tried to regulate electronic warfare are the air and missile warfare guidelines. This guideline was published in 2009 by the Harvard University of Humanitarian Policy and Armed Conflict under the Handbook of Applicable International Law of air and missile warfare. The authors agreed on 175 rules that, according to the assessment made by jurists, it reflect existing treaties and specific customary international law applicable to air and missile warfare. Also, the interpretation of the applicable international law book on air and missile warfare, by repeating each rule, clarifies the prominent legal interpretations and shows different perspectives (HPCRManual,2009,p. iii). Although the purpose of the booklet is to convey the international law governing air and missile warfare, this guideline attempts to discuss electronic warfare as a method of warfare used by aircraft. The addressed instruction seeks to regulate the use of this method of warfare and to apply the fundamental rules of the law of armed conflicts to them in accordance with air warfare. For example, the guideline states that a government aircraft – which does not qualify as a military aircraft – passively collects information or even conducts electronic warfare, a war that merely disrupts enemy communications, which is not considered as an attack, but the same actions from the government aircraft present it as a military target (Commentary on the HPCR Manual, 2010, p.113). The important point here is that this directive does not impose any obligation on governments.

Documents that are related to the law of naval warfare were largely in the form of international documents in the second half of the nineteenth and early twentieth century; they have consisted of no rules about electronic warfare at sea. After World War II, except for part of the Geneva Convention, which culminated in 1949 with the Second Convention for the protection of the wounded, the sick, and shipwrecked, unfortunately up to

date no international conference has been able to draft rules to protect civilians and civilian targets against hostile activities at sea (Kalshoven, 2011, p.27), including electronic warfare at sea. At the time being, the fundamental rules for conducting armed conflict are set out in the 1949 Geneva Conventions and the same as the first protocol of 1977, in addition to ground warfare, applies to naval warfare (attacks on coastal targets). Some of the most important provisions of the first additional protocol do not apply to naval warfare, insofar as they affect the land-based civilian population or are aimed at ground targets. The result is that most naval rules are still customary international rules (Maresca & Maslen, 2000, pp.11-13).

Perhaps the most important document governing naval warfare and electronic naval warfare after World War I is the first additional protocol of 1977, which in addition to ground warfare, it is used to some extent in naval warfare (attacks on coastal targets). Under paragraph 3 of article 49 of the first protocol, the regulations of part one (Articles 48-67) shall be applied to "any land, air or naval war that may affect the civilian population, military personnel or civilian targets on land. These rules apply to all attacks from sea or air against objectives on land" (Kalshoven, Delissen, Tanja, 1991, p.27). It seems due to the custom nature of the rules of the First Additional Protocol; the additional protocol is applicable if electronic warfare at sea affects the civilian population, military personnel, or civilian targets on land.

Concerning the applicability of the rules of the Additional Protocol to the civilian population or civilians during naval or electronic warfare, this article as well as paragraph 4 of article 49 of the First Protocol have been cited in support of conflicting and contradictory positions. Paragraph 3 of Article 49 of the First Protocol merely excludes the application of Articles 48-67 of the Protocol in naval warfare. Other provisions of the First Protocol, in particular Articles 35-41, shall be applicable. The first part of the protocol deals with naval warfare, which may affect the land-based civilian population and, additionally, applies to offshore attacks against land-based objectives (Heinegg, 1387, p.553).

Paragraph 4 of Article 57 stipulates that the adversaries shall take all reasonable precautions in carrying out their military operations at sea to avoid killing civilians and harming civilian targets. Therefore, paragraph 3 of Article 49, Article 48 to 67 of the Protocol shall apply in the following cases: A: Naval operations; Although they do not take place on land and only take place in maritime areas, they may detect civilian populations or civilian targets on land. B: Marine bombardment against ground targets. On the other hand, Paragraph 4 of Article 49 provides that the provisions of section four shall be added to other rules of international law applicable to the protection of civilians and civilian targets at sea against the effects of hostilities, and it is, therefore, clear that the regularities of Section four, it applies not only to operations from the sea against the land but the collision of ships with each other (Zamani, 1996, p.15). This section of the First Additional Protocol is applicable without regard to the method of naval warfare affecting the civilian population, military personnel, or civilian targets on land.

Unfortunately, the San-Remo Directive, which was created by a group of jurists and naval experts from different countries under the supervision of the International Organization for Human Rights "San Remo" and in collaboration with the International Committee of the Red Cross in 1994, created the San Remo Directive, which is a contemporary revision of international law applicable to armed conflict at sea (Seify, Sharifi Traz Qvhi, Rohani, Nasiri Larimi, 2018, p.65) and lacks a rule on electronic warfare at sea, based on international law. Although, it contains regulations on the use of torpedoes and naval missiles.

### 1.1 Legal review of cyber-attacks in the framework of international law

Article 2 (4) of the Charter of the United Nations prohibits the "threat or use of force" in international relations. The question that exists here is when can a government resort to legitimate defense in response to an electronic action or so-called electronic warfare? Naturally, to understand what kind of an operation means, "Armed attack", one must consider the situation and the relevant information. In naval electronic warfare, the use of naval missiles and torpedoes against relevant targets can certainly be

considered as an armed attack. However, in some situations, this matter is difficult to be recognized. Attacks on "vital national resources", such as oil platforms and other offshore facilities, docks, and ports by using electronic systems, may well cross the threshold (of attack) if it caused minor or up to no direct damage to those facilities. In this sense, "there are many similar factors used to assess whether this is a 'use of force' operation, which may be used to achieve and prove a conclusion and it will be useful to reach an estimate whether it is a specific operation which perceived by the victim as an armed attack"( Schmitt, Dinniss, Wingfield, 2004, p.4). What is certain here is that the information and electronic warfare used as an operation to prepare the battlefield for a conventional attack. However, the lack of a precise practical standard is evident.

The interpretation of air and missile warfare guidelines seek to dispel this ambiguity by stating that the use of electromagnetic, guided, or anti-radiation weapons to attack personnel, facilities, or equipment to destroy, neutralize, or demolish enemy combat capabilities either by preventing or reducing the enemy's use of the electromagnetic spectrum constitutes as an electronic attack (Commentary on the HPCR Manual, 2010, p.36).

Another question that can be raised here is whether, with the mere occurrence of an information war, especially an electronic war, can it be considered as an armed conflict, so that the application of international humanitarian law would be initiated? A useful framework has been put in place, which according to that the International Committee of the Red Cross, in its interpretation of the 1949 Geneva Convention, stated that in armed conflicts "dispute between the two countries lead to the involvement of members of the armed forces and ..., it does not matter how long the conflict lasts, or how many are killed". The International Committee of the Red Cross continues to have the same approach in the interpretation of the Additional Protocol: "Humanitarian law … covers any dispute between the two countries concerning the use of their arm forces. Neither the duration nor the severity of the war plays a rule." However, the mere use of the armed forces is not decisive; if it was the case, a government could simply avoid using humanitarian law by using civilian forces to carry out violent attacks against the enemy. Contrary, they should refer to the use of force by

referring to the armed forces, which in turn indicates the casualty of (or intention to cause) physical harm or damage to military and civilian targets. Therefore, humanitarian law applies to the extent that attacks resulting from information and electronic warfare are based on government actions and create the mentioned effects. The only exception to this rule is operations with minimal results, which can be destructive or harmful (Schmitt, Dinniss, Wingfield, 2004, p.4). This claim is not based on small attacks or cross-border incidents, which the Court ruled in Nicaragua incidents.

Following Article 49 of the Additional Protocol, "attack" means using an act of violence against the enemy for attack or defense. Emphasis on violence, is interpreted as physical force and in a limited way, since in many methods and tools of electronic warfare we do not have violent attacks like other methods, comprehending this type of attack and its compliance with Article 49 of the First Additional Protocol is somewhat difficult, but there is universal agreement that the use of biological and chemical weapons that do not appear to be associated with violence is considered as an attack. In contrast, in broad interpretation, "violence" must have violent consequences, in particular, it should cause injury or death of a person and damage or destruction of physical property. Certainly, severe physical or mental suffering, especially in the sense of injury is also included. According to this interpretation, only electronic warfare weapons that directly endanger the civilian population and violate human rights are prohibited (Schmitt, Dinniss, Wingfield, 2004, p.5). Naturally, the use of electronic devices to disable and disrupt naval navigation systems following the principles of humanitarian law would be legitimate. Therefore, according to the type of weapon used in information and electronic warfare, there is no specific prohibition for electronic naval warfare. Thus, their legitimacy as a weapon must be interpreted in the light of the principles of the distinction of unnecessary suffering (superfluous injury), which is one of the "fundamental principles" of humanitarian law, recognized by the International Court of Justice in various opinion as customary international law.

## 1.2 Rights of neutrality in electronic warfare at sea

Undoubtedly, electronic warfare at sea, like naval warfare, is based on the issue of neutrality. Therefore, in electronic warfare, the neutral government must exercise the necessary control over its aircraft, military, and merchant ships, so that the equipment under their control does not lead to a breach of the neutrality of the parties. This commitment implies that the neutral government has fundamental oversight and constant control over all of its available devices, including radars and other electronic equipment, so as not to lead to a violation of neutrality rights (Commentary on the HPCR Manual, 2010, p.314). Thus, taking hostile actions in support of the enemy, such as; intercepting and attacking aircraft; Attacking persons or targets on land or at sea; Engaging in electronic warfare, or providing targeting information to enemy forces which can be used as a tool of attack; is a violation of neutrality (Commentary on the HPCR Manual, 2010, p.161).
The areas of electronic naval warfare operations in the Maritime Law Convention and San Remo Directive have changed and affected each other. This unpleasant compromise is a constant response to excessive maritime claims, so governments must take the necessary steps to safeguard the achievements of both the Convention on the Law of the sea and the San Remo Directive. The San Remo Directive and the Convention on the Law of the sea on operational areas appear to have sufficient provisions (Jeffrey, 2012, p.108).
Naval electronic warfare usually takes place in the communicating location of neutral ships. The territory of executing armed conflict at sea, the area in which naval electronic warfare operations can be carried out, which includes:

- Land of the parties of the conflict which is accessible to the hostile navy;
- Inland waters, waters of Algerian archipelago and territorial sea of the parties of the conflict,
- The free seas include the exclusive economic zone, and
- Airspaces above the before mentioned areas.

Areas outside the battlefield can also be divided into two groups: First, the territorial waters of neutral countries, the principle mentioned in Article 2 of the Thirteenth Hague Convention, 1907, is that any hostile act in neutral

waters, including electronic warfare at sea, is prohibited. However, the execution of this rule is conditional on the behavior of the neutral country itself, because the adversaries only respect neutrality, so they would remain neutral themselves. Second, the treaty areas, as well as some maritime areas subject to international treaties, are far from the conflict and their neutrality system is predetermined: The Suez and Panama Canals, the Strait of Magellan, and the Aland Archipelago (Ziaeibigdeli, 1994, p.99-100).

### 1.3 Setting objectives in naval electronic warfare

The method of determining military and civilian objectives in naval electronic warfare is somewhat different from other methods of targeting. In electronic warfare, any object that is hit by waves emitted from the radar and reflects part of it is called a target. Targets vary depending on the radar mission. For example, in military radar, warplanes, and in a non-military radar, ships are considered as targets. Target designation in electronic warfare has several fundamental steps, which the first one is target detection. This step is the process of plotting targets automatically on the radar screen. In other words, if the target ship is within range of the radar system, then the radar sends signals toward it and finally obtains the information received from the ship, providing the final information to the computer processing system. The second step is target tracking. Radar approximately calculates new information about the position of a target and information about its previous position, how it changed direction or did not change its course. The next step is to identify vessels that are in a dangerous situation which in this step after calculating the path, speed, and direction of the moving vessel, the possibility of any danger and collision in the path of the friendly ship is determined (Nasri, Frasat, 2012, p.5). A warship that uses this system to determine and recognize a target can easily determine on its radar screen whether the target is a military or commercial ship. Because the peculiarities, shape, and appearance of warships and other military ships are fundamentally different from merchant ships. But the view toward this issue must be realistic because in most cases the development and acquisition of new technologies for peaceful purposes to serve humanity have always been in the first place, but there were also existed the possibility of its abuse. In naval electronic warfare, all lawful

targets are considered military targets and are not different from other methods of naval warfare. However, the issue that exists is that the target will not be considered a lawful military target if there is any doubt or it does not have any direct or indirect role in military operations.

In general, military targets are combatants and targets who, by their nature, location, purpose, or application, have an effective contribution to the combat readiness (operations) and combat support of the enemy or their total or partial destruction, capture or neutralization, is an explicit military advantage for the attacker (Paragraph 2 of Article 52 of the first protocol, 1977). Military targets include the armed forces; ships and military aircraft; buildings and supporting units of military services; and business objectives that have an effective share in military action. The United States has have had a broad interpretation of military objectives, but also puts other indirective objectives in war, such as economic objectives that are not directly related to military operations, as military objectives (Schmitt, Dinniss, Wingfield, 2004, p.4). As a classic example, the oil industry is a major source of export revenue for a country, and to some extent, it can reduce the enemy's ability to finance itself by crippling the industry. According to this view, electronic attack on the network and computer systems of the enemy offshore oil platforms has the necessary legitimacy, while will be a controversial issue.

Electronic warfare can be legitimately used against combatants, for example, it can prevent the movement of the ships carrying troops by tampering with and changing signals and disrupting navigation systems, causing them to stop or be destroyed. Finally, many of the potential targets of information and electronic warfare have dual applications in the military and civilian sectors. Typical examples include different frequency bands, satellites, and navigation aids at sea, depth finders, and navigators. As long as they are amongst the military targets, and the planned operations are carried out following the principles of proportionality and possible precautionary measures in attack, they are considered as the lawful targets of information and electronic warfare.

## 2. Applying the fundamental principles of humanitarian law in naval electronic warfare

Electronic warfare technologies also have different legal challenges. During the Persian Gulf War, the use of electrical systems in air combat operations not only disrupted Iraq's bilateral use of it and reduced Iraq's military capability, but also led to long-term and widespread deprivation of civilians. In addition, NATO forces bombed radio and television stations on the ground during air operations in Kosovo, fully destroyed Serbs intelligence systems capacity, and again raised questions about the legitimacy of such targeting (Waxman, 2011, p.144). However, what is important is that the flexibility of humanitarian law has historically been well established in adapting to changes in methods and tools of warfare (Schmitt, Dinniss, Wingfield, 2004, p.2). The use of electronic warfare can lead to civilian casualties. The Air and Missile Warfare Directive considers electronic warfare as a method and tool of warfare. The directive states that engaging in electronic warfare or computer networks is attacking military targets, combatants, or civilians who are directly involved in the war, may cause death or injury to civilians or damage or destruction of civilian property (HPCR Manual, Section F, Rule 1, Para (iii).

### 2.1 The principle of limitation and prohibition of unnecessary suffering

In war, the sides involved in the use of tools, weapons, equipment, and methods of battle are limited. Other limitations on naval warfare equipment and practices are inferred from the First Additional Protocol to the Geneva Conventions, which is also emphasized in the San Remo Guideline. The choice of weapons and methods of warfare is not unlimited, there are a series of prohibitions on the use of weapons and missiles, and weapons and method of warfare that cause enormous damage or unnecessary suffering or those that cause severe, long-term, and widespread harm to the environment are forbidden to be used. According to Article 35 of the First Protocol to the Geneva Conventions stated in the second paragraph that "the use of weapons, projectiles, materials and methods of warfare that cause unnecessary injury or superfluous suffering is prohibited" (Seify &

Majdfar, 2020, p.44). Therefore, the tools and methods of electronic warfare at sea are prohibited if they lead to unnecessary suffering.

## 2.2 The principle of Distinction

One of the fundamental tenets of "humanitarian law" which is directly applicable to cyber and electronic warfare, is the principle of Distinction between the military and civilians, which imposes an urgent need on cyber warfare (Delibasis, 2006, p.4). According to the principle of Distinction, the use of a weapon with a rudimentary or unreliable guidance system that cannot be used with confidence against a specific military target is prohibited (Article 48 of The First Additional Protocol). It is clear that electronic devices are not by themselves unreasonable, because they can be used more to disrupt the electronic and missile systems of hostile units, so to disrupt their functions. For example, by jamming, all electronic systems can be disrupted and the possibility of using communication equipment as well as warship missile systems can be disrupted and disabled.

It is important to apply the principle of Distinction to electronic warfare, as depending on the exact nature of network-based and electronic network attacks, they may directly cause death, injury or destruction, or malfunction of electronic systems adversely affecting enemy military capacity or operations (Commentary on the HPCR Manual, 2010, p.122).

Humanitarian law has provided extensive and specific support for many targets that, without this support, would have been considered as potential targets for information and electronic warfare attacks. Article 35 of the Additional Protocol, prohibits the use of methods or means of warfare that are intended to cause severe, widespread, or long-term damage to the natural environment or likely to have such effects. Therefore, any electronic attack that causes extensive damage to the environment is prohibited. For example, a magnetic disturbance caused by an attack on ships carrying chemical and radioactive materials in various sea areas that cause damage or harm to the environment will be prohibited.

## 2.3 The principle of proportionality

Generally, even if in information and electronic warfare the operational objectives of a military target are lawful, if that attack is disproportionate, it's prohibited (Article 58 of the First Additional Protocol). Although, sometimes due to overcrowding and interference with civilian activities it may cause damage to civilian equipment, if the damage is minimal compared to the expected military superiority of the attack, it is accepted international humanitarian law and will comply with the principle of proportionality. For example, the United States and its allies have successfully used existing electronic warfare systems, such as radio signals, to detonate hand-made explosive bombs (Schmitt, 2008, p.50).

Unintentional and accidental damage usually arises due to three factors which include lack of awareness or understanding of what is being attacked; the inability to determine the exact amount of force to be used against a target, or the inability to ensure that the weapon strikes the intended target. Although all three instances apply to the electronic case, the first one is the most difficult to be observed (Schmitt, Dinniss, Wingfield, 2004, p.9). Suppose a warship gunner locks its missile on a warship based on radar calculation while the opposing side is deceiving the gunner so that the coordinates on the radar screen belong to a merchant ship, which gets damaged by a fired missile, so such an action seems unintentional. Actually, in such circumstances, the warship must take the necessary precautions to prevent such an incident. Air and missile warfare in air operations or missile combat prohibits the use of incorrect military codes and incorrect electronic, optical, or audio devices that lead to enemy deception (HPCR Manual, Section Q, *Rule 116, Para* (C)). Basically, in electronic warfare, the use of incorrect military codes and incorrect electronic, optical or audio devices to deceive the enemy can be considered as a special case of illegal information" (Commentary on the HPCR Manual, 2010, p.256).

On the other hand, in electronic warfare, a warship may create a condition for itself on the enemy's radar and computer screen to present itself as a hospital or civilian ship and pretends to have a protected status; any use of such a method is prohibited and seems to be a deception. For example, suppose a warship uses electronic pulses to deceive the enemy in such a way that it puts several merchant ships in a network web so that the radar

of the hostile side detects all those ships as enemy warships. In other words, the geographical coordinates sent on the radar screen of the warship recognize the hostile side of the merchant ships as a military target, and based on this assumption; the hostile side decides to attack. Certainly, this action will be considered as deception and will be a violation of humanitarian law.

It will be forbidden to use electronic warfare to create the idea of ceasefire or abusing ceasefire to get closer and engage with the enemy. Doing so would be tantamount to displaying a traitorous white flag, which is prohibited. Thus, electronic warfare requires the pursuit of rights in warfare and the principles of humanity and chivalry, and no combat techniques or tools that may rely on the concept of deception should be used (Delibasis, 2006, pp.13-14).

It seems that only deceptions which are considered fraudulent and lead to human rights violations should be banned, and war tricks in electronic warfare are acceptable. An example of legal warfare tricks involves the incorrect return of signals to enemy radar by a hostile party, giving the impression of a large aircraft approaching, results in enemy confusion. During World War II, this method was used by dropping aluminum strips (windows) and is still used nowadays as an electronic warfare method (Commentary on the HPCR Manual, 2010, p.256).

The use of camouflage, which includes the reduction of electronic, acoustic, or infrared signals (effects) of a military aircraft, to make it "invisible" or "obscure" to sensors other than the human eye is also considered as deception (Commentary on the HPCR Manual, 2010, p.257).

### 2.4 Principle of taking precautionary measures

In addition to limiting the attack on military targets and the appropriateness of the attack, Article 57 of the First Additional Protocol and customary humanitarian law requires adversaries to take precautionary measures during an attack. In this regard, the European Union "has to some extent tried to use very precise methods to comply with the rules of this type of operations. For example, in addition to electronic warfare, it has tried to use a set of secondary measures such as interaction, target identification either

visually or with other systems, and a need for a positive response from an anonymous unit, including electro-optical, thermal imaging, and then launch an electronic warfare operation." The idea that "electronic warfare or even use of force, against a boat full of immigrants is allowed, requires at least precautions and warnings. Anyway, an assessment of the legality of the operation and whether it can be in full compliance with humanitarian law, as well as its compliance with the international human rights system, can only be demonstrated in one operation or operation workshop" (*Papastavridis, 2016, p.66*). Compliance with these requirements is essential in electronic warfare, especially when there is an intention to destroy the target. It is important to note that electronic warfare requires a great deal of expertise, and electronic expertise is essential during the process of targeting and assessing unintended and accidental damage. Therefore, cyber-attacks must be properly performed by trained military officers who can make a reliable estimate in the mainstream. Generally, electronic warfare provides opportunities to minimize unintended and accidental damage. For example, if oil extraction is to be cut off from an oil platform on the continental shelf, it may simply be disrupted by sending magnetic waves into the computer system instead of using a bomb or missile to destroy it. Similarly, electronic warfare significantly allows a target to be demolished to a lesser extent.

Naval electronic warfare since it takes place in the naval territory is more efficient and less costly warfare than other forms of warfare, but it is likely to affect the civilian population as well. This possibility is due to the widespread use of merchant shipping at sea and the use of various types of civilian vessels, which increase the likelihood of damage to civilian targets and as the result of naval electronic warfare, merchant ships and other civilian targets may get damaged, in which these incidents would violate the customary principle codified in Article 57 of the First Additional Protocol. In most cases, however, naval electronic warfare increases the reliability and through the information received, increases accuracy in decision-making and attack processes, thus ensuring to some extent the observance of the rules of international humanitarian law. It can be argued that countries, by providing technical and financial facilities in carrying out

processes and with the help of electronic tools, take possible precautionary measures and bring them into compliance with humanitarian law.

### 2.5 The principle of exigency

In electronic warfare, by using electronic methods such as jamming and parasite, it is possible to disrupt the electronic systems of a warship and disable its defensive and offensive systems, it seems that this action is in line with the principle of necessity, because according to the principle of necessity in war, only the amount of force is needed to prepare the ground for overcoming the enemy, with this approach, it will be easily possible to capture a warship or merchant ship. Another important point is that with electronic tools it will be easier to distinguish military targets from civilians. Therefore, the method of using this tool is very effective in observing or violating humanitarian rights. Thus, according to the principles of military necessity, "potential electronic warfare techniques can only target military objectives and related national and vital infrastructure." Targets that are not military-related are attacked during an electronic operation only if they give a military advantage or superiority (Delibasis, 2006, p.13).

## 3. Naval electronic warfare and the rules governing the use of torpedoes and missiles

Among the naval warfare tools that are very similar are missiles and torpedoes, both of which are highly in the effect of electronic warfare, as their accurate launch triggering of them are completely dependent on electronic equipment, which disruption of electronic systems will lead to unfortunate disasters. Torpedoes and missiles seem to be among the most accurate guided weapons. An accurately guided weapon means a weapon that can be aimed at a target using an external guide or guidance system of its own. They use a browser to detect electromagnetic fields. These weapons by reflecting energy from a target or a reference point and through processing guidance send commands to a control system that directs the weapon toward the target. However, other systems may be used to increase the accuracy of the weapon (Commentary on the HPCR Manual, 2010,

p.257). The law of contractual armed conflict does not contain specific provisions regarding these instruments, and only the San Remo Directive addressed them for the first time. Air and missile warfare guidelines also contain rules on the use of missiles. The follow-ups are an attempt to briefly review them.

### 3.1 Rules governing the use of sea torpedoes

Torpedoes, like other naval warfare instruments, must be used following the rules of humanitarian law. Torpedoes that have lost their effect must be neutralized (Article 1 of the Convention on the Rights and Duties of Neutral Powers in Naval War). When using torpedoes, procedures must be under the principles of naval warfare to ensure that only military targets and no other ships or targets get damaged. In other words, the type of torpedoes should be used that have excellent ability and guidance capabilities, even in shallow waters, which can be guided toward the main targets and ignore other targets. This article is derived from paragraph 3 of Article 1 of the eighth Hague Convention and is now generally accepted as a part of customary law. It is also emphasized in Article 79 of the San Remo Directive. Generally, torpedoes currently used by the Navy meet the requirements of the first sentence. The rules of the second sentence are applied according to the accuracy of the new torpedoes against ships are used above or below the surface of the sea. But guided torpedoes, in the first stage, seek their targets independently of the final stage of their movement; so they can blow up targets other than what they have intended to destroy in the first place. The purpose of the second sentence is to remind the Naval Commander of its duty to ensure that it attacks only military targets (Heinegg, 1387, p.603).

### 3.2 Rules governing the use of naval missiles

Unlike other methods of naval warfare, the rules governing the use of naval missiles, and particularly anti-ship missiles, are not the subject of any specific treaty and the International Court of Justice has not had a say in the use of such missiles (Mundis, 2008, p.232). However, the air and missile warfare Directive define a missile as a self-propelled unmanned weapon launched from aircraft, warships, or land-based launchers (HPCR Manual,

Section A**,** *Rule 1, Para (Z*). The directive mandates that missiles comply with the basic principles of humanitarian law (differentiation and prevention of unnecessary suffering) (HPCR Manual, Section, *Rule 5, Para* (A).

The general principles of naval warfare apply to the use of missiles at sea, including cruise missiles. The inclusion of a specific material on missiles means that modern naval warfare should be considered. So specific rules for the use of cruise missiles or other types of them have not yet emerged in naval law (Heinegg, 1387, p.604). Therefore, the fundamentality of principles governing naval missiles, which are a type of usable weapons system, should only be following the principles of targeting. Several issues raised with long-range weapons, such as missiles capable of long-range use, raise many concerns about target differentiation (Mundis, 2008, p.232).

Traditional law does not have a specific rule about them; therefore, when the adversaries use cruise missiles or other missiles, they are committed to ensuring that the missiles are aimed only at military targets. This is also emphasized in paragraph 78 of the San Remo Directive. Generally, the technical condition of new missiles enables the adversaries to comply with the basic principles of the law of naval armed conflict, in particular the principle of differentiation. Nevertheless, there are still issues regarding diagnosis and targeting (Heinegg, 1387, p.604).

"According to the principle of differentiation between military and civilian targets, naval missiles can be divided into two categories: those that fly horizontally on the surface of the radar, and those that fly off the surface of the radar and hit the target. Radar-guided missiles can select and hit the right target; Off-radar missiles, on the other hand, are usually guided by a heat source and operate automatically and independently. Such missiles are not accurate enough, and malfunction or insufficient performance of their guidance system means that they do not properly detect the target and cannot differentiate between military and civilian targets at sea. This was proven by the Stark warship incident on May 17, 1987, when two Iraqi Exocet missiles hit it. The procedure of blind and non-discriminatory attack of neutral shipping was condemned by Security Council Resolution 552,

528, and 598 in the imposed war, because "Iraq, unlike Iran, made little effort to identify targets before attacking them" (Zamani, 1996, p.30). In the International Committee of the Red Cross interpretive theory, long-range missiles that cannot be accurately targeted are considered as "blind weapons"; according to part 20 of paragraph (b) of Article 8 of the Status of the International Criminal Court, the use of weapons, ammunition, materials, and methods of warfare that are excessively harmful or cause unnecessary suffering or are inherently contrary to the international law of armed conflict, are considered as war crimes (Seify & Majdfar, 1399, p.50).

Additionally, when using naval missiles, one of the issues that arise is how the commitment to take precautionary measures and continuous vigilance applies to naval missile strikes. It is not easy to comment on this subject that the First Additional Protocol applies only to ground, ground-to-ground, sea-to-land, and air-to-ground attacks. Thus, in the case of a naval missile strike, the old debate is that whether surface-to-surface missiles can distinguish between lawful targets and protected targets according to new technologies. Article 57 of the First Additional Protocol and Article 46 of the San Remo Directive should be considered here (Slensvik, 2013. P.21). It is clear that, if the use of missiles and launchers is subject to large-scale targeting, the adversaries are committed to taking precautious proceedings to ensure that anything other than military targets is safe. If it is not possible to observe these procedures, the legitimacy of the use of missiles can not be questioned. Modern missiles are equipped with very strong intelligent resolution and destruction capability and usually do not lose their targets. Therefore, in light of the fundamental principles of naval armed conflict, it is not necessary to equip them with self-destructive tools or similar facilities (Heinegg, 1387, p.604). However, precautions must be taken when using such systems. In other words, in certain circumstances, some requirements appear that the attacker is required to take appropriate precautions as far as possible, that is, if the intended target takes defensive actions against it, and uses a tool such as chaff (a metal chip to mislead) or deceptive (enemy radar misleading device) that identify civilian targets or other non-combatant ships as targets (neutral merchant ships), in order not

to endanger or destroy them (Mundis, 2008. P.232), it should stop the attack.

## 4. Conclusion

Electronic warfare at sea is one of the new methods of naval warfare, and the author believes that electronic warfare can achieve the goals of international humanitarian law better than other methods. Electronic warfare at sea has not received much attention in the legal documents of armed conflict, especially the law of naval warfare, and there is no particular document specified to this type of naval warfare. In this regard, and due to the lack of subject matter rights, non-government agents have tried to regulate these new methods in the form of instructions such as air and missile warfare. However, regardless of what has been mentioned, it seems that in future naval wars or naval operations, this method of warfare will play a very important role. The practice of governments also indicates the importance of this method of naval warfare. But, this method of warfare must also be adapted to the requirements of the general principles of humanitarian law. Surely, it should not be forgotten that the use of electronic deception systems can easily lead to severe human rights violations. Certainly, if this method fails to respect the distinction between the military and civilians, or if it violates any of the fundamental principles of humanitarian law, it will be forbidden and the perpetrators will be held accountable. Therefore, it is necessary for the international community and countries to pay special attention to the method of electronic warfare at sea and to formulate legal rules about this method as soon as possible.

Finally, to gradually develop the law of armed conflict, especially the law of electronic warfare and issues related to this subject, the following suggestions are recommended:

- It is essential that when checking the weapons, this action be done with the cooperation of experts in various fields, such as lawyers, military experts, and operators so that the review is more transparent.
- Holding national or international conferences or seminars on maritime electronic warfare law.

- Compilation of dissertations and thesis on the topics of naval warfare law and electronic warfare at sea.
- Considering the mentioned issues by the naval organizations of the country, including the navy of the arm and the Revolutionary Guards of the Islamic Republic of Iran.

**References**


Adami, D.L. (2016). Electronic warfare, Translators: Baybordi, F.; Mousavinsab, S.; Karimpour, E.; & Mohammadzadeh, F. Imam Khomeini University of Marine Sciences Publications, Nowshahr. (in Persian)

Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare, (March 2010), Program on Humanitarian Policy and Conflict Research at Harvard University, Version 2.1.

Delibasis, D. (February 2006). State use of force in cyberspace for self-defense: a new challenge for a new century peace conflict and development, An Interdisciplinary Journal, Issue8, available from http://www.peacestudiesjournal.org.uk

Hitchens, Theresa, (Sanremo, 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.

Heinegg, W.H.V. (2008). Laws of armed conflict at sea, humanitarian law in armed conflict, translated by Sid Ghasem Zamani & Nader Saed, edited by Dieter Falak, Shahre Daneh Publications, Tehran. (in Persian)

Jonsson, N.B. (Spring 2008). Legal issues on self-defense and maritime zones in naval operations, Master Thesis, Faculty of Law University of Lund.

Jeffrey, D.P., (March 2012). An analysis of the legality of maritime blockade in the context of twenty-first century humanitarian law, A thesis Degree of Master of Laws, Queen's University Kingston, Ontario, Canada .

Kalshoven, F. (2011). Constraints on the waging of war: an introduction to international humanitarian law, Cambridge Universiry Press, International Committee of the Red Cross.

Kalshoven, F.; Delissen, S.J.M.; & Tanja,G.J. (1991). Humanitarian law of armed conflict challenges ahead, Martinus Nijhoff Pulishers Dordercht, Bosston, London.

Mundis, D.A. (May 2008). The law of naval exclusion zones, a thesis submitted for the degree of doctor of philosophy, University of London the London School of Economics and Political Science Law Department, England.

Maresca, L., & Maslen, S. (2000). The banning of anti-personnel landmines, Cambridge University Press.

Nasri, F.; & Frost, M. (2008). Electronic navigation, Imam Khomeini University of Marine Sciences Publications, Nowshahr. (in Persian)

Papastridis, E. (2016). Eunavfor operation sophia and the international law of the sea, MarSafeLaw Journal, 2.

Seify, B.; & Sharifi Traz Qvhi, H. (2020). The necessity of training the naval armed conflict law in the strategic Navy of the Islamic Republic of Iran Army, Journal of Marine Science Education, 19, 64-85. (in Persian)

Seify, B., & Majdfar, S. (Spring 2020). A examine of the methods and technology of naval warfare from the perspective of international humanitarian law, Scientific Journal of Marine Science and Technology, 93, 39-55. (in Persian)

Seify, B.; Sharifi Traz Qvhi, H.; Rohani, K.; & Nasiri Larimi, R. (Winter 2018). The Challenges of the Law Governing the Use of Mining in Naval Wars in the Light of New Technologies and Techniques, Journal of Private and Criminal Law Research, 43, 49-88. (in Persian)

Schmitt, M.N. (SPRING 2008). The principle of distinction and weapon systems on the contemporary battlefield, THE QUARTERLY JOURNAL.

Schmitt, M.N.; Dinniss, H.A.H; & Wingfield, T.C. (June 25-27, 2004). Computer and war: the lwgal battles pace, Program on Humanitarian Policy and Conflict Research at Harvard University, Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge,.

Waxman, M. (Sanremo, 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.

Zamani, S.Gh. (Winter 1996). The law of the sea war and new developments, Journal of Defense Policy, 17, 1-32. (in Persian)

Ziaeebigdeli, M.R. (1994). War law, Allameh Tabatabai University Press, Tehran. (in Persian)

Manual on International Law Applicable to Air and Missile Warfare (HPCRManual), 15 May 2009, Program on Humanitarian Policy and Conflict Research at Harvard University, Bern.

The Geneva Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, (1949).

The Geneva Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, (1977).

The San Remo Manual on International Law Applicable to Armed Conflicts at Sea, (12 June 1994).