

The Protection of Undersea Internet Cables during Armed Conflicts: An International Humanitarian Law Perspective

Ihsanullah Butro

ihsan.butro@usindh.edu.pk

Visiting Faculty member, Department of Law, University of Sindh, Jamshoro, Pakistan.

Naseer Nisar

naseernisarmon5222@gmail.com

Law Student, Department of Law, University of Sindh, Jamshoro, Pakistan.

Nirmal Arif

nirmalarifjamali@gmail.com

Law Student, Department of Law, University of Sindh, Jamshoro, Pakistan.

Sania Khair Muhammad

saniakhairmuhammad101@gmail.com

Law Student, Department of Law, University of Sindh, Jamshoro, Pakistan.

Corresponding Author: Ihsanullah Butro ihsan.butro@usindh.edu.pk

Received: 31-01-2026

Revised: 14-02-2026

Accepted: 28-02-2026

Published: 15-03-2026

ABSTRACT

The global digital communication system depends on undersea Internet cables for its strength. Most international Internet is carried through these cables, which are essential to the operation of banking, trade, healthcare, education, government and diplomatic communications. As digital connectivity grows or becomes more relied upon these cables have become critical infrastructure for national and international security. However, submarine cable networks have been shown to be vulnerable to rising geopolitical tensions, armed conflicts, sabotage and new cyber threats, especially in strategically important maritime regions such as the Strait of Hormuz. This study analyses the protection of undersea Internet cables during armed conflicts from the perspective of International Humanitarian Law (IHL). The study is doctrinal legal research, which will analyze relevant international legal instruments, such as the United Nations Convention on the Law of the Sea (UNCLOS), the Geneva Conventions, Additional Protocol I, customary international law and the law of state responsibility. The study assesses the legal status of submarine cables and analyses the application of key IHL principles, such as distinction, proportionality, military necessity and precaution. The findings indicate that undersea Internet cables are typically protected as civilian objects, but legal uncertainty arises when they serve both civilian and military purposes. The study also highlights major deficiencies in current international legal arrangements with respect to accountability, protection standards and responses to contemporary threats to digital infrastructure. It finds that strong international legal protections, improved guidance and greater international cooperation are needed to protect the security, resilience and continued operation of the global submarine cable networks in armed conflict.

Keywords: Undersea Internet Cables, International Humanitarian Law, Armed Conflict, Strait of Hormuz, Civilian Objects, State Responsibility.

INTRODUCTION

The Internet has become beneficial to people's daily lives. The internet is used in business, banks, government, healthcare and education throughout the world to communicate. Most International Internet Data is transported in the fibers optics cables in the Seabed and such cables have been used in the Communication services. In simple terms, these cables are called the backbone of the Internet world that connects various continents. Therefore, undersea internet cables are now in the realm of national security as well as national economic growth and connectivity amongst countries (Burnett, Beckman &

Davenport, 2014). Particularly in today's digital world, submarine cables are even more vital to countries as they depend on them. This kind of cable is employed in a number of areas like international banking uses, for cloud computing services, in military information systems and in diplomatic communications. When one such cable is cut, millions of people's lives in various countries are paralyzed and it disturbed and huge economic losses occur (Burnett, 2021). Thus, now, the submarine cable can be considered as strategic infrastructure and should be duly protected both legally and physically.

Even though they have many significance, numerous dangers exist for undersea Internet cables. In particular, anchors of ships, natural stock and technical problems turned out to be the most important damaging elements of cables. But new threats or issues have arisen due to the geopolitical tensions and the form of warfare in modern times. In today's armed conflicts important civilian infrastructure can be directly impacted or indirectly influenced. Digital communication networks are the backbone of today's society and submarine cables attacks could raise humanitarian, economic and security issues (Bennett, 2019).

The Strait of Hormuz is an internationally important digital communications route, well known to many as one of the world's most important energy transport routes. Important submarine cables such as AAE 1, FALCON, Gulf Bridge International (GBI) have this territory as their submarine making point. These are the cable systems that provide the Internet connection for most of the Middle East, Asia, Europe and Africa. There are many countries that can be involved in such an escalation or in the event that a war breaks out in the Strait of Hormuz, a narrow sea bridge, many of the cable systems are in groups. This Strait of Hormuz is the type of chokepoint that could be assumed to be a large communication hub with the influence of many in the world, for this reason it is one of the most important chokepoints. (TeleGeography, 2024; Zenodo, 2025). The main legal frameworks for maintenance of submarine cables are the United Nations Convention on the Law of the Sea (UNCLOS), which allows for laying and maintenance of submarine cables in different maritime areas (United Nations, 1982). At the same time, International Humanitarian Law aims to protect civilians and civilian objects during armed conflict are to be found in the Geneva Conventions and the Additional Protocols. The Main IHL principles such as distinction, proportionality, and precaution require an object or party to a conflict to avoid unnecessary harm to civilian infrastructure (ICRC, 2025). However, the implementation of these principles with regard to submarine Internet cables is still in the process of development.

In times of war, this is especially important these days as the utilization of digital communications is growing and concerns about the security of the cables have surfaced. Breakdown of such cables could not only put states at conflict at risk, but could also impact neutral states and civilian populations internationally. Therefore it is relevant to look at the extent of the protection of undersea cables under IHL to understand how existing provisions of IHL might be sufficient to meet the challenges to the critical nature of the global digital infrastructure. Equally significant is the increasing regional concentration of communications infrastructure along a limited number of submarine cable routes. International cable systems frequently pass through strategic chokepoints that, during periods of war or political instability, may become vulnerable to interference or disruption. Damage to a major cable route could have repercussions that cross state lines and could impact international trade, the financial markets, emergency communications and access to information. This inter-dependency, the need to improve the legal regimes and international cooperation for submarine cable infrastructure resilience and protection in the event of armed conflict has gained increasing attention (Klein, 2020; ITU 2024). Moreover, the security of the undersea (submarine) Internet cables is well connected with the general concept of Critical Infrastructure Protection. In recent years, governments from around the world and international organizations have been more conscious than ever about the need for digital connectivity as a means to guarantee economic stability and the citizens welfare. Digital networks have become part of today's society and the disruption of submarine cables could be similar to a war against the other civil critical infrastructures. Existing international legal systems can thus be interpreted and enhanced to meet the new challenges facing the global communications system, as well as to offer a way to solve these security issues (Tsagourias 2020; NATO CCDCOE 2017).

In this paper, undersea Internet cables will be discussed with regards to International Humanitarian Law (IHL) during an armed conflict. It examines the law relating to submarine cables and their legal protections; examines the relevance of the principles of IHL to attacks on submarine cable facilities; looks at the connection between IHL and the law of the sea and evaluates if the existing international law rules adequately cover submarine cable facilities as a very important component of global connectivity.

Research Questions

1. What are legal principles of the underwater Internet cables under International law especially involving UN Convention on the Laws of the Seas (UNCLOS)?
2. How do the principles of International Humanitarian Law (IHL), including distinction, proportionality, and precaution, apply to the protection of undersea Internet cables during armed conflicts?
3. What dangers and weaknesses do undersea Internet cables face during armed conflicts, particularly in important maritime areas such as the Strait of Hormuz?
4. Are the current international legal rules enough to protect undersea Internet cables during armed conflicts, or is there a need for stronger legal protection and greater international cooperation?

LITERATURE REVIEW

Submarine communication cables are just as important and critical to modern-day society and are subject matter of a number of international groups, security studies and law. Past studies on submarine cables mainly focused upon questions of maritime law and freedom of navigation and the UN Convention on the Law of the Seas (UNCLOS) state rights. However, these studies and interpretations have undergone an evolution of the following understanding: International humanitarian law (IHL), security threats, cyber operations during armed conflict. (Zhang & Li (2025).

A key issue in research is to observe whether enough protection is provided under international law for submarine cables but, Zhang & Li (2025) argue that the overall law presently fails to consider cables that are deliberately severed. UNCLOS has provisions on the protection of cables as does the Convention for the Protection of Submarine Telegraph Cables (1884), but these are dated now and do not address some of the current security threats, including hybrid warfare and non-state actors, as enumerated in the UN study. They also argue that the protection of submarine cable infrastructure has not been emphasized to a certain degree as well due to the lack of clearly defined jurisdictions and weak enforcement mechanisms (Zhang & Li, 2025).

The other major area of research is that of submarine cables during times of war. The scholars, McLaughlin, Paige and Guilfoyle (2022), state that the law regarding submarines and the use of cables is not clear. In times of war they claim 'cables' do not have a clearly-worded status in legal acts. This uncertainty is even more serious for both civilian and government communications via the cables. The authors emphasize that these laws must be more clearly formulated and clearly specify when it is acceptable to target submarine cables in armed conflicts. More recent ones have been the fields of crucial strategic issues concerning 'submarine cables as critical-components of infrastructure'. There are numerous reasons for this, one of the most obvious being that far from merely commercial property, now submarine cables are elements of national and international security (2026: Jaffal). As more and more communications go over digital cable networks, submarine cable disruptions can have repercussions similar to attacks on other critical resources. Jaffal also noted that international law is trying to find a balance between security of countries, freedom of communication and a necessity to secure civilian infrastructure.

A number of investigations have been carried out to consider the trade in protection of Submarine cables and to have some idea of what is meant by the right of self defence in international law. How to consider any attack on submarine cables to be an "armed attack" as per Article 51 of the United Nations Charter? It says not all cable severing incidents would be deemed to be armed attacks, but severing large tracts of cable, or at choke points could be a state's right to self defence. One of these is the value of the vulnerability of submarine cables which in some cases could also be termed a national resource, and which if cut, could create security issues. Especially underground cables are becoming identified as an important part of today's security specter. The United Nations Institute for Disarmament Research (UNIDIR) released a research on the behavior of states towards subsea communication cables, given the rising worries. Submarine cables are now a concern of national security, as geopolitical rivalries, technological sensitivities and the growing strategic competition has pushed submarine cables to the fore. The report also includes the information that the international guidance that States receive on activities related to submarine cables, is not clear.

Another aspect of the new observations made in the treaties of international advices is about the understanding of 'intentional sabotage of cables'. Schaller (2025) argues that sabotage of cables of submarine communications might even be legitimate in the exercise of force and as armed attack, as defined in the UN Charter. That interpretation would dovetail nicely with an interpretation of international law which has taken a new turn among scholars that attacks against critical infrastructure can be as effective as for example other types of military attacks. However, the experts are still speculating on what exactly the exact range of the law will be. The literature that have been identified are those in challenges such as jurisdiction and enforcement. Lott (2025) argues that, the classical jurisprudential approach may not at all times be adequate as the marine space and the involvement of a number of them is fraught with challenges, states. The author recommends more spreading of responsibility internationally, as well as protecting accountability.

Overall, existing literature reviews it is clear that general concern of the existing literature has increased and concern about the vulnerability of the submarine communication cables and existing legal weakness has arisen. Views are highly agreed upon that submarine cables are vital infrastructure that should be protected during armed conflicts; however, opinions are scarce regarding the definition of submarine cable from an international law perspective, how to apply the principles of self defence in practice as well as on existing international law. Moreover, there has been research focused on the concept of distinction, proportionality and precaution in IHL as can be seen in the application of the undersea Internet cables that are strategically important in the chokepoints in the sea, such as the Strait of Hormuz. Given the lack of literature it is necessary to research further on the protection of submarine Internet cables in the context of an armed conflict from the perspective of IHL.

Research Gap

Previous studies have examined submarine cables from a legal, security and critical infrastructure protection and global connectivity perspective. However, IHL noted that, there have been a couple of numbers studies in the 'right of protection' of the undersea Internet cables region. The studies partly mention the principle of distinction and principle of proportionality, but neither of them has a detailed analysis in relation to submarine cables in armed conflicts and there is no reference to military necessity and precautionary principle in the existing studies. In addition, research on such issues is very scarce in critical seas, such as the Strait of Hormuz. Therefore this study is intended to fill this gap and analyse the rights to safeguard the subsurface Internet cables under the IHL and explore the question of whether it is sufficient or not to say in times of armed conflict, the existing international legal system is enough to safeguard undersea cables. However, not much research has been conducted on protecting the undersea Internet cables, in particular from the background of IHL. A great deal of research on this subject has focused on maritime law, rights and responsibilities of States or infrastructure security with little research being undertaken on the impact of basic IHL principles such as those of distinction, proportionality and military necessity and precaution on the submarine cable system in times of armed conflict.

Moreover, no research has been conducted to date to analyse whether these undersea Internet cables can be considered as civilian objects or dual use critical international infrastructure under IHL in today's conflict context where Communications networks & infrastructure will be used for public, civilian and military purposes. There is no emphasis, even in the literature dealing with the study of strategic chokepoints in the sea, including the state of Hormuz. The area is of a high strategic value for energy supplies and digital connectivity and the studies have been dedicated to the legal aspects of potential damage to submarine cables during armed conflicts. The security of the Strait of Hormuz and the sufficiency of current laws have received many queries on civilian protection, regional security, and whether existing legal protections are sufficient.

So therefore the studies examine that since the "gap" was found in the currently above study. This study tried to fill this gap by analyzing such incidents on armed conflict occurring on undersea Internet cables with detailed analysis from IHL perspective. It examines how the IHL principles could be applicable in the case of submarine cable facilities, explores the current legal safeguards and considers new threats that emerge in the more strategically critical straits, specifically such as the Strait of Hormuz.

RESEARCH METHODOLOGY

The study uses a Doctrinal Legal Research method as the problem to be studied in this research. It is related to the legal aspect of the protection of undersea Internet cables during the armed conflict. Doctrinal Legal Research is useful for understanding rules, principles and treaties and academic view related to legal questions. This study is not intended to be about collecting data, the study also to analyze the legal context and what its significance involves the Submarine Cables infrastructure and IHL.

The study mainly uses secondary sources. The sources include: the Articles on Responsibility of States for Internationally Wrongful Acts 2001, Geneva Conventions 1949, Additional Protocol (I) 1977, Customary IHL, UN Charter (1945) and UN Convention on Law of Sea (UNCLOS) (1982). Special interest is the legal rules related to critical infrastructure, maritime communications in armed situations and citizens objects. The study also analyses documents and publications coming from international organizations – such as the International Committee of the Red Cross (ICRC), the International Cable Protection Committee (ICPC), the International Telecommunication Union (ITU), the United Nations Institute for Disarmament Research (UNIDIR) and other relevant United Nations bodies. These resources offer valuable insights into the significance, fragility and auctorial security of the submarine cable systems in today's security environment.

The study also reviews academic books, peer-reviewed journal articles and books as well. Certain attention is given to the controversy about the protection of submarine Internet cables, both during times of peace and war, whether as civilian objects, as dual use facilities or strategic assets. It is actually applied in the research form doctrinal study method, analytical study method. Analytically, this study will examine implementation of these principles of IHL (distinction, proportionality, military necessity and precaution), but will examine in the context of a hypothetical armed conflict between ITU and undersea Internet cables. It also reviews the existing international legal schemes and instruments that are relevant for the protection of submarine cable facilities and the degree to which these provide protection to the areas where cabinets are not legally protected. It's also targeting the consequences of the activity of the legal cases that have been raised by the possible attacks on the submarine cables passing from the key sea lanes, the main sea lane where several great international submarine cable systems pass is the Strait of Hormuz.

This study examines various international legal instruments, academic works, institutional reports and policy documents to existing legal gaps and problems of the protection of undersea Internet cables during armed conflicts. The study will then try to suggest ways to further improve legal protections and promote cooperation and interdependency among the international community to secure the future security and stability of global digital communications networks in the framework of International Humanitarian Law.

DISCUSSION

1. Legal Status and Protection of Undersea Internet Cables Under International Law:

Undersea Cables are one of the most crucial components of today's global infrastructure. Whereas satellites (usually associated with international communications) have relatively low numbers of communications, submarines are used mainly for international communications. These cables are used for cloud communications, emergency response as well as financial transactions and military and diplomatic operations. Thus, the ramifications of a failure of the submarine cable networks could reach beyond the actual outage and impact millions of people simultaneously from a variety of countries (UNIDIR, 2023). Their role in global critical infrastructure with increasing importance of digital communications is making them a key element of undersea infrastructure. While it is important, it is not fully fledged; International Law has not created a complete legal system specifically for the protection of the submarine Internet cables during times of armed conflict. It gives protection, however, through various different international definitions of protection, such as the United Nations Convention on the Law of the Sea (UNCLOS), International Humanitarian Law (IHL), customary international law and the general principles of state responsibility but, when applied to current conflicts, there are some critical legal issues.

The United Nations Convention on the Law of the Sea (UNCLOS), 1982 is the main international law concerning submarine cables. Highlights the importance of submarine cable systems, and state's rights to lay them and maintain them in the sea areas. All states are free to lay submarine cables on the high seas under Article 112 of UNCLOS. Articles 113 to 115 impose obligations for the protection and repair of submarine cable systems. These provisions require states to enact domestic laws prohibiting intentional or negligent damages to submarine cables and to provide for the prosecution of persons responsible for such damage (UNCLOS, 1982). UNCLOS provides great protection, which, however, is ineffective during armed conflicts. This Convention largely aimed at ensuring the maintenance of peace in maritime matters, not for military purposes. Therefore, UNCLOS fails to explicitly deal with a number of issues that may arise during the disturbance of a submarine cable system by acts of violence. The Convention, for example, contains nothing much about the lawfulness of an intentional strike on a submarine cable, the lawfulness of a submarine cable used by civilians for telecommunication as well as for military cables and the responsibility of a State for damage to submarine cables during times of war. However, due to this gap, many scholars contend that UNCLOS is insufficient on its own to provide adequate protection for submarine Internet cables for modern conflicts (McLaughlin, Paige & Guilfoyle, 2022).

This location of submarine cables also makes the process to make them legally safe. The territorial seas, continental shelves and areas beyond the national jurisdiction are crossed by numerous large cable systems. For different cable systems, however, there may be different parts of the law that will come into effect. Not helpful with jurisdiction since if impact occurs there could be several different jurisdictions interested in the infrastructure network impacted. Therefore, submarine cable networks are international in nature and it is necessary to seek international cooperation in terms of protection and maintenance (Lott, 2025).

In addition, UNCLOS there exist more traditional legal instruments that also contain some clues regarding the protection of communication facilities during armed conflict. The Hague Regulations, 1907, is one of the few subjects specifically evinced in the few international treaties which mention submarine cables directly. According to Article 54 of the Hague Regulations, submarine cables connecting occupied territory to neutral territory shall not be seized or destroyed except when it is absolutely necessary. It was in an era prior to the Internet and it basically indicates that when it was developed an understanding was formed that communication infrastructure should be offered special protection at least in wartime. It is also understood that multiple communication networks may be impaired at the same time. (Hague Regulations, 1907). The protection of civilian objects also had positive impacts under IHL. Legal principles set out in the Geneva Conventions (1949) and the

Additional Protocol (1977) also tried to protect civilians and civilians in times of armed conflict. The instruments don't mention submarine Internet cables, but the rules are quite relevant as most cable systems already exist for civilians. Normally, attacks against civilians are prohibited under the International Humanitarian Law, except if they transform into a lawful military object. Hence, the undersea Internet cables are not to be attacked unless their use meets the legal criteria for being considered military objectives (Additional Protocol I, 1977).

One of the most important debates on the modern day academics of the law is: What are submarine Internet cables? Based on the observations of many of the scholars, submarine cables as their primary function for civilian communications and information delivery, business, education and provision of health care services should be predicated as civilian objects. Thus, any attacks on submarine communications cables in general can be seen as a violation of the International Humanitarian Law unless such use can be used to effectively contribute to the military operations (Pedrozo, 2025). The important with regard to the maritime chokes, including the Strait of Hormuz, therefore emphasizes on the maritime-strategic significance of the submarine cables on the one hand only. The Strait of Hormuz is also well known for its role in transporting energy but also provides energy service for international digital communications. There are several main Cable systems which pass through this area. Many of the cable systems are based on relatively small geographical areas; if one is severed a huge number of messages from many countries are severed simultaneously. Thus, the Strait of Hormuz can showcase the importance of the submarine cable network in this region's and world security. On the one hand, recent advances in strategic importance of submarine cables raise the question of the sufficiency of international law to adequately protect digital infrastructure as it stands, in the context of the current uses of submarine technology during armed conflict and on the other hand they suggest changes to international law. While there are important frameworks in the laws of the sea, the Hague regulations, Geneva conventions and customary International Humanitarian Law, yet there are also some remarkable gaps in the laws. Many of these laws and policies were formulated prior to the advent of the modern Internet and thus neglect to solve many of the issues arising from today's electronic systems. But the extent of the associated legal problems isn't clear: the reach of dual use communication systems, cyber-assisted attacks against tangible assets and the question of responsibility, when it comes to the security of networks spread all across the world. Thus, although international law recognizes the importance of submarine cable systems and provides some level of protection under different legal regimes, the current regime is patchy and incomplete. As states and societies become more dependent on digital connectivity, the need for a more holistic legal approach to address the peculiar vulnerabilities of undersea Internet cables in the context of armed conflicts becomes evident. The following sections will discuss the application of some of the principles of International Humanitarian Law on submarine cable infrastructure and if these principles provide enough protection to modern threats or not.

2. Application of International Humanitarian Law Principles to Undersea Internet Cables

The protection of undersea Internet cables during armed conflicts mainly depends on the application of the basic principles of International Humanitarian Law (IHL). There are no specific terms relating to submarine Internet cables in the Geneva Conventions and Additional Protocols but there are general rules governing warfare that are borne out of some legal context and provide valuable legal aid for protecting the submarine Internet cables. As more and more modern societies are based on digital communication systems, the importance of these principles in the installation of submarine cable became evident as a theme in the legal studies. The concept of the principle of distinction is a general principle of IHL. It encourages the parties to armed conflicts to always make the distinction between civilian objects and military objects. Article 48 confining military operations to military objectives. In fact, while most of the undersea Internet cables are used to carry civilian data, financial transactions, health-care information, education etc., they are not normally military targets and only those undersea cables that serve a military purpose, in accordance with 52(2). (Additional Protocol I, 1977). But it is more complex to apply the principle of distinction for submarine cables which serve civilian and military communications. In today's communication systems, common infrastructure can be utilized - a single cable can be utilized for civilian networks, government communications and military

information. Those circumstances when the classification of a submarine cable is legally ambiguous and whether it is or isn't a military target is challenging. Under Article 52 (2) of Additional Protocol I, an object qualifies as a military objective only if it makes an effective contribution to military action and its destruction offers a definite military advantage. And the mere presence of military communications in a cable system does not in itself justify an attack. Prior to any legal strike, it is essential to carefully examine in detail the actual importance of the military target (Dinstein, 2022). Proportionality assessments are at the moment more important than ever due to the increased integration of digital use in everyday services. Apart from that, today's economies depend on the uninterrupted connectivity in the digital domain, therefore, any cable cut could affect civilian citizens of the country where the war is played, as well as in other neutral countries. Thus, an attack against one of these systems was, according to the scholars, weighed when determining proportionality and the international impact to analyze the compliance of an action with the principle. This sentiment is representative of the increased understanding of the uniqueness of digital infrastructures compared to many more conventional military targets – at the international level (ITU, 2024).

Another principle is that of Military necessity. Where international law would for example deem such actions unlawful, it is necessary to achieve a legitimate military goal, then those actions are lawful. Unfortunately this is a rule of war that cannot be taken advantage of by military commanders as much as they like. If several military communications, however, are present the attacking party would have to carefully consider if there are other modes of communications (submarine cable) other than harmful. So if you're going to affect military communications, a lesser impact on civilian communications is possible if you're going to affect that military communications facility. But in all cases military necessity shall never be separated from humanitarian concerns and consequently, considerations for the protection of life of non-combatants (NATO CCDCOE, 2017). The rise of cyber operations and hybrid warfare has brought a new found complexity to the use of International Humanitarian Law with regard to submarine cable systems. There is a new type of warfare which has just started to include attacks on diffusion of information and on critical infrastructures. Some States are, in fact, trying to do some damage but without even going so far as to close down undersea cables, trying to put some damage to digital communication networks. But this does not need to be the physically aggressive nature of an armed force to have equal consequences: impeding civilian communications and services seriously can be as bad as armed aggression. As such, legal scholars argue that the scope of the application of International Humanitarian Law needs to be greatly expanded to consider protection of the threats posed by non physical and physical sources to critical digital infrastructure (UN Open Ended Working Group on ICT Security, 2021). However, another important aspect is that of a neutral state's protection. Since submarine cable systems often connect several countries, attacks on such infrastructure may affect states that are not involved in the conflict. In fact, according to the traditional rules, it is a question of International Humanitarian Law; this is the question of limiting the war to the duration of the hostilities and of maintenance of the interests of the neutral states. Thus, if an attack on submarine cable systems was to be disrupted, it might pull itself into a legal mess, should it not have large effects on neutral states, and on civilians. In the region where a cable system is used by a region or internationally is of special importance. (International Law Association, 2024)

Among these is the strategic importance of submarine cable systems as they get threatened with new technologies which are challenging the traditional laws. However, the rules of distinction, proportionality, military necessity and precaution also apply and in a more complicated way in the digital age. Most existing legislation was drafted prior to the global Internet and so not necessarily drafted with clarity to deal with modern communication networks. Despite this, there is still a lot we don't know about how lawful and how directly protected the subsea Internet cables are in times of armed conflict. Actually, there are no changes to the points of interest of IHL. The point of the law is to reduce the impact of the use of force, provide for the protection of civilians and to prevent unnecessary suffering. A high degree of protection is needed for Submarine Internet cables, which are vital to many international communications, economic activity and civilian life during armed conflicts and there are good reasons for providing that protection in law and humanism. In a world that becomes increasingly

interdependent, this kind of increased legal predictability would help to strengthen the stability of international relations and safeguard civilians better.

3. State Responsibility, Strategic Vulnerabilities in the Strait of Hormuz, and the Need for Stronger Legal Protection

As countries more and more rely on digital communication networks, submarine Internet cables have become strategically valuable assets from simple commercial infrastructure. No matter whether it is the government, financial institutions, military organizations or civilians, all rely on the continuous digital connectivity. Therefore, targeted attacks against submarine cable infrastructure have to be able to have impacts well beyond the immediate conflict zone. These attacks could cause disruption in banking systems, financial markets, emergency response services, cloud computing services, transport networks and government communications. These issues come into focus when considering the global importance of these systems and the question of whether the current legal regime is enough, of state responsibility, and of international security. The Articles on Responsibility of States for Internationally Wrongful Act, 2001 is one of the important legal documents relevant to such scenarios being applicable in such cases. An 'internationally wrongful act' is an act which is in violation of an 'international obligation' and for which the conduct is attributable to the state under Article 2. Under International Humanitarian Law, law of the sea or any other international obligations, States can become liable for international responsibility if they intentionally damage submarine Internet cables. Where this is the case, the violating state may be required to cease the wrongful act, make assurances that it will not be repeated and provide adequate compensation for the harm done (International Law Commission, 2001). The United Nations Charter is also crucial in the assessment of attacks to the submarine cable infrastructure. Under article 2(4) the use or threat of force is forbidden against the territorial integrity or the political independence of states. In the past, debates over the use of force were based on conventional military strike issues. But today's scholars increasingly have noted that an attack on critical infrastructure can have the same results as a traditional military attack. However, if the intentional disruption of submarine cables "results in significant economic disruption, in some degree of paralysis of governmental functions or in long lasting consequences of national security" the following questions could arise: are such actions a "prohibited use of force" under Article 2(4) of the Charter (Roscini, 2014)

A related issue concerns Article 51 of the United Nations Charter, which recognizes the inherent right of self defence in response to an armed attack. The question of whether there is an armed attack on a submarine communications cable is not without controversy. Some scholars argue that, only attacks of a certain magnitude on a certain country that have consequences of a national dimension would be deemed to reach the thresholds for a self defence response. Others argue that there are other disruptions of communication architecture that would not be considered armed attacks. It is part of the larger debate on the evolving nature of international law with regard to the new challenges to critical infrastructure posed by the digital age (Tsagourias & Buchan, 2021). Submarine cables strategic significance is particularly evident in the Strait of Hormuz. The strait is regarded as one of the world's strategic maritime chokepoints, playing a crucial role in global energy transportation. However, the strait also plays a vital role in global digital communications, as numerous submarine cable routes connecting the Middle East to Asia, Europe, and Africa pass through or across the region. The cable systems enable international internet traffic, financial transactions, government communications and commercial activities to the benefit of many countries (International energy agency, 2024). There is a very big strategic vulnerability given that they are all concentrated in a very thin layer of the oceans where the submarine cables are located. Military fighting, naval maneuvers sabotage or heightened regional tensions could pose a potential threat for damaging the cable infrastructure, and thus throwing a large geographical area of communications out of order. Most of the cables in the Strait of Hormuz are submarine cables which, as opposed to local infrastructures, simultaneously provide service to several countries. Thus, the disruption of these systems could impact countries not directly affected by conflict, posing challenges to neutrality and defense of civilians, as well as to regional security (TeleGeography; ITU, 2024). Geopolitical tensions over military deployments, maritime incidents and security issues have plagued the Strait of Hormuz for the past few years. Such an environment might allow not only

attacks on submarine cable systems to be feasible, but accident damage caused by military activity to be as well. International Humanitarian Law calls for the parties to a conflict to take into consideration the foreseen civilian impact of military operations. Hence, any actions that may impact the submarine cable facilities in the Strait of Hormuz should be analyzed under the concept of distinction, proportionality, military necessity, and precaution (Middle East Council on Global Affairs, 2025).

This demonstrates the weaknesses of existing international legal frameworks as the submarine cables are vulnerable in important maritime chokepoints. While UNCLOS contains procedures for laying and maintaining submarine cables, it also was originally developed for “peacetime use” and contains only a small amount of information for armed conflict. Likewise, international humanitarian law does not specifically refer to the particular qualities of digital infrastructure that is universally connected, but instead affords general protection to “civilian objects.” This leaves matters unclear with regards to the legality of such submarine cables, particularly where they are used for both the civil and military interests.

The analysis in this study will show that in the modern international legal framework undersea Internet cables have a particular status. They are at the same time civilian infrastructure, economic assets, communication network and strategic resources. As they constitute an increasingly significant aspect of the security equation, a legal framework should be in place to cope with not only with conventional uses of armed force, but also with the new issues relating to cyber operations, hybrid warfare and geopolitical competition. The protection is provided under the existing legal principles; however, there are still many legal gaps. Thus, it is important to reinforce international legal framework, clarify the use of International Humanitarian Law, and advance international cooperation to maintain security and protection of the global digital communication networks.

FINDINGS

Undersea cabling Internet is significantly important for the overall functioning of a digital infrastructure. They are a major part of international communication, financial transfers, governmental functions and the economy. Indeed much has been written about the contribution of the Internet to the right of freedom of expression and their protection in case of armed conflict but nothing specifically to the protection of submarine Internet cables in times of or during armed conflict.

The study also reveals that the existing legal regime of submarine cables comes from or composed of the United Nations Convention on the Law of the Sea (UNCLOS), International Humanitarian Law (IHL) and general principles of international law (GPIL). While there are some legal measures for safeguarding in these legal frameworks, it does not mean they are in place and protecting digital infrastructures against the current threats.

The study further finds that undersea cables are as civilian property under IHL and therefore are not legitimate objects of attack. However, there is legal uncertainty when cable systems are used for both civilian and military purposes. Modern communication networks are dual-use, making it hard to know when a submarine cable may be a legitimate military target.

Another finding is that the significance of the principles of distinction, proportionality, military necessity and precaution remains valid for submarine cable during armed conflicts. But in practice it is very hard to apply because it can have consequences which affect millions of civilians in a number of countries, due to the damage suffered by one cable system. In addition, the research shows that the existing legal framework lacks guidance when it comes to questions of attacks on submarine cables, of identification of the responsible actor and accountability for damage caused by this responsible actor in an armed conflict. There are no clear legal rules to cover liability and legal implications of an intentional attack on submarine cables.

The study finds another issue is at the Strait of Hormuz, another critical and cornerstone maritime chokepoint area that has a number of critical structures for submarine cables. If any of the above areas were disturbed it would be a fact with regard to regional and international consequences. Finally, the research acknowledges that there is still a major legal gap in questions of the digital infrastructure of the world, which needs to be protected. The existing set of laws is not well-equipped for dealing with the growing significance of the submarine Internet backbone cables in this contemporary digital age. Hence, it is necessary to have transparency in the law and to enhance cooperation between countries.

RECOMMENDATIONS

Clear rules and explicit explanation should be given about the legal status of the submarine cables and its infrastructure, and how the infrastructure can be protected. States need to cooperate with their foreign counterparts as to monitoring, maintaining and protecting submarine cable systems. As soon as there is better cooperation the information sharing, risk assessment and emergency response would increase and improve.

International organizations should give direction on how the principles of IHL apply to submarine cables, and especially with respect to their use, for civilian and military operations. States should build stronger regulations for the protection of submarine cable facilities in their domestic laws and ensure accountability for the perpetrators of intentional damage along with the companies persons responsible for such damage. It should improve the international communications network available by establishing a new route of cables; setting up a back-up system and enhancing cable security. Submarine cables are likely to be more vulnerable in maritime chokepoints like the Strait of Hormuz, which could be of special interest.

International and regional efforts need to be reinforced for safeguarding critical infrastructure in the region or areas. Providing more detailed provisions and definitions on the attribution of attacks, and State responsibility and liability in connection with armed attacks on submarine cable facilities, should be included during armed conflict. Future legal and policy talks need to show that submarine Internet cables are vital global infrastructure and therefore the security of such cables are important in international security, international stability and civilians. Finally, even more challenges could be encouraged at the academic level that would seek the solution related to Cyber Operations issues, International Humanitarian Law (IHL) protection of Digital infrastructure, etc.

CONCLUSION

Undersea Internet cables are among the most important components of modern global infrastructure. They carry the majority of international Internet traffic and support essential services such as banking, trade, healthcare, education, government operations, and international communications. As societies become increasingly dependent on digital connectivity, the security and protection of these cables have become matters of international importance. This study examined the legal protection of undersea Internet cables during armed conflicts through the framework of International Humanitarian Law (IHL) and related rules of international law.

The study finds that although international legal instruments such as UNCLOS, the Geneva Conventions, and Additional Protocol I provide a degree of protection, there is no specific international legal framework dedicated solely to the protection of undersea Internet cables during armed conflicts. As a result, the existing legal regime remains fragmented and does not fully address the challenges created by modern digital infrastructure and evolving security threats.

The research further concludes that undersea Internet cables are generally regarded as civilian objects and are therefore protected from attack under International Humanitarian Law. However, legal uncertainty arises when cable systems perform both civilian and military functions. The dual use nature of modern communication networks makes it difficult to determine when a submarine cable may legally

become a military objective. This uncertainty creates challenges for the practical application of the principles of distinction, proportionality, military necessity, and precaution during armed conflicts. The study also highlights the strategic importance of the Strait of Hormuz as a major digital communication corridor. The concentration of several important submarine cable systems within this narrow maritime route creates a significant vulnerability. Any military confrontation, sabotage, or disruption in the region could affect communications, economic activities, and essential services across multiple countries, including states not directly involved in a conflict.

In conclusion, the growing reliance of the world on digital communication networks requires stronger legal protection for undersea Internet cables. Existing international legal rules provide an important foundation, but they are not fully equipped to deal with contemporary threats such as hybrid warfare, cyber operations, and attacks on critical digital infrastructure. Therefore, clearer legal standards, stronger mechanisms for state responsibility and accountability, and greater international cooperation are necessary to ensure the protection of submarine cable systems. Strengthening these protections will help preserve global connectivity, support economic stability, protect civilian populations, and contribute to international

REFERENCES

- Douglas R Burnett, Robert C Beckman and Tara M Davenport (eds), Submarine Cables: The Handbook of Law and Policy (Brill Nijhoff 2014). <https://share.google/pPlpcYoSTL21Jgqyg>
- Douglas R Burnett, Submarine Cable Security and International Law (2021). <https://share.google/C6CdIgNsK9vQNrbfN>
- A Bennett, Submarine Cables and Infrastructure Vulnerabilities: Threats and International Law (2019). <https://share.google/3F94TItzXUAbQ0N7A>
- TeleGeography, Global Submarine Cable Map (2024). <https://www.submarinecablemap.com/>
- The Undersea Cable Network of the Strait of Hormuz as a Critical Infrastructure Corridor (2025). <https://share.google/KMVJs0gyMMrtGWB6z>
- United Nations Convention on the Law of the Sea (UNCLOS) (United Nations 1982). <https://share.google/6v7Mqv2rAmO2uqto2>
- International Committee of the Red Cross, International Humanitarian Law and Connectivity Disruptions During Armed Conflict (2025). <https://blogs.icrc.org/law-and-policy/2025/07/03/international-humanitarian-law-and-connectivity-disruptions-during-armed-conflict/>
- Natalie Klein, Maritime Security and the Law of the Sea (Oxford University Press 2011). <https://share.google/b6ggnv7LVOT3vGSE7>
- Nicolas Tsagourias, 'Autonomous Weapons Systems and Command Responsibility' (2020). <https://share.google/QK8yzaI32RsLAdjll>
- NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017). <https://share.google/HIjh9ISE6j2TDotSC>
- Zhang D and Li H, 'Research on the International Legal Regulation of Willful or Culpably Negligent Damage to Submarine Cables' (2025) Marine Development. <https://share.google/MwENTf16eoEqurBDT>

- R McLaughlin, TP Paige and D Guilfoyle, 'Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization' (2022) 27(3) Journal of Conflict and Security Law. <https://share.google/dnmyjNCQZ3vm45OVs>
- Safeguarding Global Connectivity: International Law and Cyber Operations Against Submarine Data Cables. <https://www.tandfonline.com/doi/abs/10.1080/00908320.2026.2661346>
- Lonér T, Submarine Cables and Armed Attacks (2024). <https://lup.lub.lu.se/student-papers/record/9180266/file/9182917.pdf>
- UNIDIR, Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour (2023). <https://share.google/6nPkU8hD5EV6oeOHi>
- C Schaller, 'Sabotage of Submarine Cables and Pipelines as a Use of Force' (2025). <https://share.google/sQk7sadEuacoxayUN>
- A Lott, 'Conventional Jurisdictional Approaches to Protecting Submarine Cables and Pipelines' (2025). <https://share.google/78vPcrBUz0NjlqKMA>
- United Nations Convention on the Law of the Sea (UNCLOS) 1982. <https://share.google/mPwH6YtepEgiLjY7O>
- Additional Protocol I, 1977. <https://share.google/LclyRy3w0K6qjmmWf>
- Geneva Conventions, 1949. <https://share.google/Yk5nEx82udhUOASs0>
- Customary International Humanitarian Law. <https://share.google/QCxBahQI5ggrIvSK2>
- United Nations Charter, 1945. <https://share.google/VhoKR9cXtHmvi6Z0p>
- Hague Regulations, 1907. <https://share.google/ZBx6EJLIPKEbWW3mg>
- International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts (2001). https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf
- United Nations Charter 1945. <https://www.un.org/en/about-us/un-charter>
- United Nations Convention on the Law of the Sea (UNCLOS) 1982, arts 112, 113, 114 and 115.
- Hague Regulations 1907, art 54. <https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907/regulations-art-54>
- RA Pedrozo, Safeguarding Submarine Cables and Pipelines in Times of Armed Conflict (2025). <https://share.google/sMTENeA6miDSB1OB>
- Additional Protocol I 1977, art 48. <https://share.google/GtUEuSJdcM5jnW7uj>
- Additional Protocol I 1977, art 52(2). <https://share.google/cXhUFPJBqqcgFkqAe>
- Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (4th edn, Cambridge University Press 2022). <https://share.google/peR4o0pJragCnQcgA>
- International Telecommunication Union (ITU), International Advisory Body for Submarine Cable Resilience (2024). <https://share.google/UsDj4gLDP3frRoxc2>

United Nations Open Ended Working Group on Security of and in the Use of ICTs, United Nations Open Ended Working Group on Security of and in the Use of ICTs (2021). <https://share.google/9yH43sFvv2w2ZCdNd>

International Law Association (ILA), Committee on Submarine Cables and Pipelines under International Law Report (2024). <https://share.google/0AFqsJecfw7A5RjP5>

International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts (2001) art 2.

Charter of the United Nations 1945, art 2(4). <https://share.google/6B3nmrZynFi50pvWR>

Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford University Press 2014). <https://share.google/pz7JnFaol2b82vkIQ>

Charter of the United Nations 1945, art 51. <https://legal.un.org/repertory/art51.shtml>

N Tsagourias and R Buchan, Research Handbook on International Law and Cyberspace (Edward Elgar Publishing 2021). <https://share.google/hcCU1D7TzgnHhQ722>

International Energy Agency, The Strategic Importance of the Strait of Hormuz (2024). <https://share.google/2KfLpWuyheyNBws24>

Middle East Council on Global Affairs, Navigating Rocky Waters: GCC Strategies for Maritime Security (2025). <https://share.google/EvxQ5gC26GhQoLAsh>