TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation
http://www.transnav.eu
Volume 19
Number 3
September 2025
DOI: 10.12716/1001.19.03.26

GPS Jamming and Spoofing – Countermeasures for Safety and Security

M. Okochi[1] & M. Haberfeld[2]
[1] *Tokyo University of Marine Science and Technology, Tokyo, Japan*
[2] *City University of New York, John Jay College of Criminal Justice, New York, USA*

ABSTRACT: This paper aims to clarify the legal status of Global Positioning System (GPS) jamming and spoofing, which have a dichotomous nature of countermeasures and cyber-attacks. GPS is an indispensable tool to enable ships, aircraft, and weapons to navigate to a predetermined destination. The jamming and spoofing of these signals apparently hinder safe navigation through Sea Lines of Communication (SLOCs). At the same time, jamming has been positively employed to prevent the triggering of explosives and to conceal communications between terrorists during critical operations. In light of these positive uses of jamming, international legal structures have not been established to prohibit jamming and spoofing. In order to find essential factors to help legalise or criminalise jamming, this research analyses cases of GPS jamming. Both Ben Gurion International Airport in Israel and the Black Sea have often been disrupted by intentional interference with GPS, such as jamming and spoofing.

1 INTRODUCTION

This paper aims to identify potential effective regulatory instruments for preventing spoofing—one form of cyber-attack—by clarifying the current legal structures for the regulations on Global Positioning System (GPS) spoofing. Then the current safety and security measures for prevention of GPS spoofing will be examined through case studies.

GPS, the US form of Global Navigation Satellite System (GNSS), is a constellation of satellites providing signals from space that transmit positioning, navigational and timing (PNT) data to GPS receivers on the Earth [1]. These receivers are then able to determine their location from this data. Four global constellations: the US's GPS Navigation System with Time and Ranging Global Positioning Satellite (GPS NAVSTAR), the EU's Galileo, Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) and China's Beidou are providing global coverage services. Also the following regional satellite-based augmentation systems (SBAS) are in operation: Japan's Quasi-Zenith Satellite System (QZSS), India's GAGAN, the US's Galaxy 15 and the UK's Inmarsat 3-F2 and 4-F3 [2]. What would be indispensable to drawing up clear blueprints for the use of GNSS, or even future cyber warfare, should be an accurate understanding of not only the major GPS players but also states embarking on space activities, such as Iran.

Among these GPS services, errors in signals that inform vessels and aircraft of their locations and navigation routes have the potential to cause accidents. GPS spoofing is an act of deliberate conduct that sends false signals that may cause navigational hazards and danger. For example, ultra-large crude carriers (ULCC) that carry up to 500,000 tons of crude oil, navigate safely by GPS through narrow straits. Drill ships that extricate oil and gas from the ultra-deep seabed use

Dynamic Positioning System (DPS) depending on GPS signals to hold their positions. Naval fleets and unmanned aerial vehicles (UAV) know their and their targets' exact positions. On the other hand, authorities can use jamming to hinder precision-guided missiles, UAVs and the triggering of remote-controlled improvised explosive devices (RC-IEDs) [3].

Different parties' various activities, such as shipping, controlling air traffic, and engaging in military operations, can be done safely with the signals that notify these parties of their locations. Thus, GPS has become an indispensable infrastructure for individuals, private companies and sovereign states, along with their military and police forces [4].

While these activities require the accuracy and continuity of GPS signals, 'jamming', i.e., intentional radio frequency interference prevents receivers from locking onto satellite signals, rendering the system ineffective or degraded. Also, 'spoofing' involves broadcasting counterfeit satellite signals to deceive GNSS receivers, causing them to compute incorrect position, navigation, and timing (PNT) data [5]. Since spoofing is a newly emerging technological issue, in general, 'jamming' is often described as the impediment of satellite signals, such as broadcasting and communications jamming, electronic interference and any other form of cyber-attacks. Also, 'meaconing' is the transmission of original but delayed signals to confuse a GPS receiver. Lastly, spoofing is the stealthiest activity to make users misunderstand their location without their noticing. In a broad sense, jamming is an umbrella term that broadly means interference and covers spoofing, meaconing and non-intentional interference.

The actual situation of GPS spoofing, including Automatic Identification System (AIS) spoofing, is a threat to be eliminated; they can disrupt maritime traffic. Especially ports and chokepoints on international corridors are considered potential targets and high risk infrastructure [6]. If receivers catch and follow signals from multiple satellite constellations, the risk of spoofing might be reduced. However this robustness depends on the performance of receivers.

Therefore, considering the key role of GPS in safe navigation and prevention of spoofing, international technical standards in the design and construction of vessels are developed under the auspices of the International Maritime Organization (IMO), which is the international organisation in charge of the safe operation of ships [7]. Following these standards, many vessels are equipped with one or two standardised DPSs. DPS is an integrated control system that implements GPS signals to automatically hold the vessel's position via multiple thruster pods [8]. When a vessel is operating in the ocean, GPS signals from satellites to her DPS are critical for safe navigation.

In comparison to these concrete technical standards for safe navigation, no branch of international law, such as the Law of War, Maritime Law, Law of the Sea and Space Law, had either prepared for or solved this problem single-handedly. In addition to these legal instruments, the regulations of specialised international organisations and sovereign states overlap and are fragmented with respect to their issue-oriented approaches. In terms of the distribution of radio wavebands, the International Telecommunications Union (ITU) is an authoritative agency that has provided a common service since its founding in 1865. Regarding maritime safety, the IMO and its specialised committees are in charge of international legislation and technical standards in detail, as mentioned above. As an example of this fragmented nature, each state determines their rules of engagement during military operations and combat as circumstances require.

Thus, legal structures for the security of GPS signals - especially for the prevention of GPS spoofing - are not sufficiently discussed or established, even though spoofing can have serious consequences [9]. GPS is indispensable infrastructure that enables states to safely conduct operations such as counter-terrorism and counter-insurgency (COIN), military operations or offshore energy exploitation. In this regard, troubles with NATO's fleet in the Black Sea, the landing of the US drone in Iran and GPS spoofing in the areas surrounding Ben Gurion International Airport in Israel are one step ahead of the current regulatory frameworks. Consequently, it is essential to examine these cases from a legal standpoint to establish safety and security measures against GPS spoofing.

2 CASES AND MATERIALS OF GPS SPOOFING

GPS spoofing is progressing rapidly in all fields of GPS use and serious disturbances have arisen as a result. This disruption and interference has not been determined to be illegal since the legal instruments and concrete regulations that prohibit it do not exist yet. In addition to the legal characteristics, the activity is not defined as wrongdoing since it is also useful for protecting national security by preventing drone attacks on vital infrastructure such as military facilities, nuclear power plants and airports, as occasionally mentioned in cases of jamming carried out by certain governments.

In consequence, some cases should be given as examples which demonstrate the harmfulness of GPS spoofing to national security.

2.1 *The Black Sea Case*

The Black Sea is of critical concern to the international community as a shipping route and a seabed rich in energy resources. It is located between the Mediterranean Sea, connected by the Dardanelles-Bosphorus straits, and the Azov Sea, connected by the Kerch strait in the east of the Crimean Peninsula. It is 422,000 km^2 in area, and consists of high seas except for the territorial waters of the six coastal states; of Russia, Ukraine, Romania, Bulgaria, Turkey and Georgia. The principle of freedom of navigation is applied to the high seas area of the Black Sea.

Long before recent technological incidents relating to GPS, the Black Sea has historically been the focus of two types of dispute [11]. One is the freedom of navigation within this strategic half-closed sea, which essentially depends on the rights of passage through the Dardanelles-Bosphorus straits. The straits are under the governance of Turkey, in accordance with the Montreux Convention Regarding the Regime of the

Straits of 1936 (the Montreux Convention). The other is maritime delimitation between coastal states, which may determine the possession of seabed natural resources, namely oil and gas in the Black Sea.

Figure 1. The Black Sea and Ukraine. Source: US Department of Defense [10]

These two issues concerning freedom of navigation and sovereign rights to natural resources within the seabed are fundamental to the six coastal states of the Black Sea. Consequently, Ukraine has some disputes with the other coastal states with regards to the delimitation of the Black Sea.

Each of the six Black Sea states has its own interests in the solution to these two issues. In addition to that, not only these coastal states, but also other interested states, including EU members and the US, deploy their fleets to establish freedom of navigation even in peacetime. As a prime example, the Black Sea is one focus of the US Freedom of Navigation (FON) Program [12]. The Black Sea incident of 12 February 1988 occurred when two U.S. naval vessels entered the Soviet territorial sea in the Black Sea during the FON Program. This case illustrates the importance of the Black Sea as a strategic point in the region [13].

In addition to the issue of the freedom of navigation, Romania filed an application in 2004 with the International Court of Justice against Ukraine with respect to a maritime boundary in the Black Sea between the two states [14]. The case concerned the delimitation of the continental shelf and exclusive economic zones (EEZ) between them. As a further example, an arbitral case between Ukraine and Russia concerning coastal state rights in the Black Sea, Sea of Azov, and Kerch Strait has been pending before the Permanent Court of Arbitration since 2016 [15].

Thus, the Black Sea is a locus of interests and conflicts between states. Freedom of navigation is a critical issue which relates to the safety of life and stability of global order.

2.1.1 *Freedom of Navigation in the Black Sea*

First, an important feature of the Black Sea is that it is a half-closed sea. Its exit to the High Seas, namely the Mediterranean Sea, is limited to the Dardanelles-Bosphorus straits. The Black Sea or to be more specific, the Dardanelles-Bosphorus straits are essential to enabling the five coastal states except Turkey to exit to the High Seas.

As well as the issue about seabed natural resources and maritime delimitation, the Black Sea has the core value of transit corridor to the Mediterranean Sea for the coastal states with no ports or sufficient winter ports other than ports in the Black Sea. Thus, Dardanelles-Bosphorus Straits are characterised as the international straits, which are used as international routes between high seas according to geographical conditions provided by Article 37 of the UN Convention on the Law of the Sea (UNCLOS) of 1982.

At the same time, the straits are Turkey's territorial sea, where its sovereignty extends. As a result, the straits are controlled by the Montreux Convention in order to balance the interests between Turkey's sovereignty and other states' freedom of navigation. For instance, the convention provides Turkey the rights to control over the straits by prohibiting the passage of belligerent states' fleets in times of wars on the one hand, on the other hand, Article 19 of the Montreux Convention allows military vessels to return to their home ports.

As a prime example, the Russian fleet may return to their port, e.g., the Sevastopol Naval Base in Crimea although Turkey announced that belligerents' fleets may not pass the straits during the Ukraine war in 2022.

Thus, the Black Sea has been drawing attention under the Montreux Convention, especially since the invasion of the Crimean Peninsula of Ukraine by Russia in 2014 and a GPS spoofing case against the NATO fleet mooring at Odessa in Ukraine occurred in 2021.

According to the AIS and GPS plotter, the two naval warships HMS Defender (IMO 4907878) and HNLMS Evertsen (MMSI 244942000), were identified leaving and navigating from Odessa to Sevastopol, the port of the Russian Black Sea fleet in Crimea, on 18 June [16]. However, satellite imagery confirmed the two warships had stayed in Odessa. This case shows vessels and their crews rely upon GPS signals to identify their and other ships' locations, and moreover, false signals can be wrongly interpreted and given as correct by the vessel's GPS plotter.

This case illustrates that GPS spoofing may have a harmful influence upon international relations between unfriendly states who are not necessarily outright belligerents. Thus, the more ships that depend on GPS signal for navigation, the more GPS becomes the locus of offence and defence. As a result, manifold measures to keep ships navigating safely and accurately are being taken by various actors.

As another example, Russia placed radio-jamming equipment on a gas rig in the Black Sea after seizing it in 2015, thus blocking Ukraine from using telecommunications in the area. According to the Defense Intelligence of the Ministry of Defense of Ukraine, Ukraine retook the field from Russia on 11 September 2023. Now this field can not only extract natural resources but also act as a forward deployment base [17].

In preparing a response to the emerging threat of jamming and spoofing, US authorities have devoted themselves to countering GPS jamming. The Maritime Administration of the US Department of Transportation has reported AIS manipulation and jamming in the Black Sea since February 2022 [18]. These cases are available as part of the GPS Problem

Report Status, coordinated by the Navigation Center of the US Coast Guard [19].

Also, the US and its allies developed a concept called SLOC. SLOC recognises that one of the principal missions of the military is protecting SLOC and merchant vessels navigating sea lanes. GPS disruption is a threat that must be removed from these lanes.

Besides measures taken by the sovereign states such as the US, an international organisation, IMO adopted Resolution A.1106 (29) on 2 December 2015, which provides a Revised Guidelines for the Onboard Operational Use of Shipborne AIS [21]. The resolution warns that information provided by AIS may not be giving a complete or correct picture of shipping traffic in their vicinity.

Thus, the disputes concerning rights of coastal states potentially impede free and safe navigation in the Black Sea. These obstacles to safe navigation, especially GPS jamming and maritime disputes, need to be removed in order to achieve free and safe navigation. While the settlement of disputes and implementing countermeasures to GPS jamming in the Black Sea are imperative, the Black Sea is undergoing interruption of maritime traffic after the Russian invasion of Ukraine.

Therefore, safety and freedom of navigation guaranteed by GPS during wartime will be discussed in the next section.

2.1.2 *The Grain Export Initiative through the Black Sea*

Since the Russian invasion, the export of grains and iron ore, Ukraine's main export goods, could not be transported to and loaded at ports along the Black Sea. For example, seaborne exports from three main ports on the coast of the Black Sea, namely Odessa, Pivdennyi and Ismail, could not be used any longer. Commercial disruption—'*guerre de course*'—around Black Sea ports was implemented by Russia as a long-distance blockade.

Yet according to the traditional Law of War, Law of Neutrality and International Customary Law, which regulate freedom of navigation, protection of commercial cargo vessels, and safety of communications under the circumstances of wartime, are blockade must be effectuated with a naval fleet and set closely around the enemy state's ports. These two requirements are called 'effectiveness' and 'proximity' respectively [22].

In light of these requirements recognised by theories and state practise of the Law of War, Russia does not have the right to set a long-distance blockade in order to block commercial cargo vessels or the naval fleets that escort these vessels.

At the same time, freedom of navigation in the Black Sea is indispensable to continuing the export of goods such as iron ore, wheat, and sunflower oil from Ukraine and the import of essential materials into the country by stabilising international cargo transportation in the region. Without ports that provide Ukraine exits to the Black Sea, it becomes a land-locked state, which will have limited supply routes. From that strategic viewpoint, Russia has been imposing blockades around the Black Sea and the shipping routes going through international and Ukrainian territorial waters in order to disrupt Ukraine's seaborne trade.

Consequently, the states supporting Ukraine commonly consider that establishing a new supply chain and strengthening logistical capacity in and around Ukraine while roads and railways to ports and sea routes are blocked by the Russian military and navy is to be the stimulus for Ukraine's full recovery from severe war damage.

The EU Council penned a document on May 31 that demanded Russia stop attacking Ukrainian transport infrastructure and lift the blockade of the Black Sea ports, especially Odessa, to allow the export of grains. The EU Commission announced on May 12, 2022, the establishment of the 'Solidarity Lanes' that enable essential humanitarian aid and materials to be imported into Ukraine.

Within the framework of the Solidarity Lane, key players in and around Ukraine's logistics are Romania, Poland and Hungary. Romania is repairing the railway from the port city of Galati to the Moldovan border at Giurgiu. It will connect the port of Reni in the south of Odessa with other Danube ports. This railway line will allow the transport of goods to and from Ukraine via Moldova and the port of Galati. As a result of efforts to support Ukraine's export capabilities, 35,000 tonnes of Ukrainian iron ore at the Black Sea port of Constanta were loaded by a Romanian company in April. Also 80,000 tonnes of grains have been sent to Constanta since the start of the invasion.

In addition to the regional cooperation, the UN brokered an agreement between Ukraine, Russia and Turkey on resuming grain exports from Ukraine through Black Sea ports. The four parties finally reached an agreement - the Black Sea Grain Initiative - on July 22, 2022, not to attack vessels and infrastructure engaged in this transportation. The agreement means the lifting of the Russian de facto blockade in the Black Sea. At the same time, this agreement needs effective implementation through inspection at designated ports.

The agreement guarantees the maximum safety to vessels which transport grains from Ukraine in accordance with this agreement. Indeed, the Initiative allows for commercial food exports from the Ukrainian ports of Odessa, Chornomorsk and Yuzhny in the Black Sea after inspection by the monitoring team of the Joint Coordination Centre, Istanbul, at checkpoints set up at the ports on the Dardanelles-Bosphorus straits. The Centre consists of representatives of Ukraine, Russia and Turkey to check whether cargoes and crews are permitted to sail under the Initiative.

Russia objected to this scheme on October 29, 2022, alleging that the Russian fleet had been attacked at Sevastopol port, but later retracted their objection on November 2. Russia, however, also asserted they required the ability to export fertiliser to developing countries in order to stabilise agriculture. The agreement was extended on November 17, 2022, for an additional 120 days, as no party had announced its intention to end or amend the agreement. Finally, Russia decided to leave the Agreement on 17 July 2023.

Thus, the intentness of the EU's regional efforts and Grain Export Initiative illustrate how free and safe

navigation is critically essential for the maintenance of maritime transport even during an armed conflict. The halting or continuing of maritime transport via the Black Sea may influence regional stability and the outcome of the conflict.

While the issue of GPS jamming is not directly involved in the Grain Export Initiative, it is often used as a weapon for non-kinetic or cyber-based attacks to disrupt seaborne trade. Conflict concerning control of the Black Sea is inseparable from the issue of GPS signal accuracy as a precondition for free and safe navigation.

2.2 *Interferences in Israel*

Israel is, due to its location, one of several states that are influenced by GPS jamming. As a result, the country's cybersecurity policy is progressively and practically implemented by its authorities [23]. Cases and materials in Israel are worthy to be examined as a prime example.

2.2.1 *GPS Spoofing Cases and Countermeasures in Israel*

A disruption of GPS signals at Ben Gurion International Airport in Tel Aviv, Israel, was detected in 2019. The International Federation of Airline Pilots' Associations (IFALPA) issued a Notice to Airmen (NOTAM), which warned crews landing at the airport that the Association had received many reports from pilots of loss of GPS signals or erroneous positioning of several miles in the vicinity of the airport. The airport again experienced disruptions to their GPS signals in February 2022.

According to Kan News, a division of the Israeli Public Broadcasting Corporation, the Israel Defence Forces - specifically the Spectrum Warfare Center - identified that the GPS jamming signals emanated from Khmeimim Air Base, built by Russia in 2015 on the western coast of Syria. These signals caused GPS disruptions to nearby aircraft but were concluded to not be intentional. Russia asserted that she was attacked by drones in 2018 and used jamming as a defensive measure to protect their soldiers around the air base.

Israel's cybersecurity strategy has been in development since 2002, when the National Information Security Authority (NISA) was established. NISA focused on protecting vital computer systems in some critical fields of the period. Having gained experience in building robustness in cybersecurity, the government, via Resolution 2444, authorised the establishment of the National Cyber Security Authority (NCSA) in 2015 [24].

This continuation in the cyber security strategy of Israel can be outlined with two characteristics. The first is a theoretical and conceptual framework which is built to be flexibly applied. This framework consists of three layers. The efforts within the broadest layer target and improve the cyber-readiness capabilities of the civil and private sectors by setting standards for critical infrastructure. Then, more concrete measures within the second layer establish the sharing of information, the development of technologies, and the enhancement of education and training, all based on a supply and demand system between the government and private sector. Lastly, law enforcement and military organisations prepare for and respond to incidents through successfully battle-testing cyber defences against persistent cyber-attacks and intentional interferences.

The second is international cooperation. Israel has concluded cyber defence cooperation agreements with friendly states and organisations, and is actively participating in multilateral platforms. The country works to share its experience and lessons, and seeks to harness its advantages in cyber to promote global cyber resilience and cooperation based on shared values and trust.

However, as Israel itself indicates, the risk of cyber-attacks is intensifying. Offensive cyber tools are becoming stealthier and more sophisticated. They are available to a diverse range of actors as they become more accessible by growing smaller and more affordable. The technological landscape is becoming more interconnected and embedded in all areas of national security and people's lives.

The harsh environment of national and international cybersecurity requires clearly targeted threats, such as GPS spoofing, be examined and countered on a case-by-case basis.

Although difficult, the intent and result of spoofing can be used to determine the legitimacy and legality of individual instances of the activity. Therefore, the differentiation between every single incidence of spoofing should be examined according to their intent and result [25].

2.2.2 *Interferences to Leviathan Gas Field*

A recent example is the Israeli gas field 'Leviathan', discovered in 2010, 125 km west from Haifa, near the disputed border with Lebanon. It contains 33 Tcf of natural gas resources in place (22 Tcf recoverable). The offshore natural gas field was opened in 2019. Operations at the Leviathan gas field are ongoing. Another gas field, 'Tamar', discovered in 2009 and brought online in 2013, is 23 km (14 miles) off the coast of Ashkelon, a city in northern Israel.

Oil and gas rigs are primarily vulnerable to waves, winds and technical troubles even though states and contractors adhere to authoritative international technical standards. Furthermore, offshore support vessels carrying personnel and heavy modules between rigs and coast depend on GPS due to their proximity to condensate pipelines transporting extracted high-pressure gas to onshore facilities. While safe navigation and resource exploitation are secured by the accuracy and continuity of GPS, they can be hindered by the loss of GPS signals. According to accident reports distributed by the International Maritime Contractors Association (IMCA), collisions between a vessel and facility occur when the vessel comes alongside the rig or performs maintenance on a wellhead and the vessel experiences an unexpected movement due to a dysfunction in its DPS [26].

In addition to the primary vulnerabilities of oil and gas exploitation, if oil and gas fields are situated within areas disputed by adjacent or opposite coastal states, each state vehemently criticises the exploration and

exploitation of resources, as well as the entire operation of the other state [27].

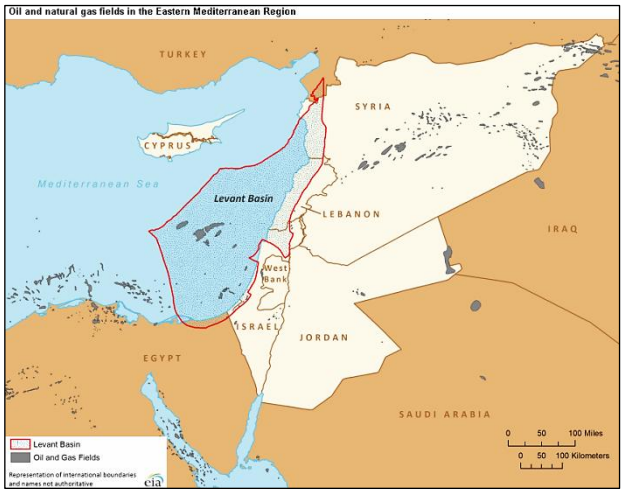

Figure 2. Oil and Gas Fields in the Eastern Mediterranean Region. Source: US Energy Information Administration [28]

Indeed, contests over the ownership of Leviathan have been aggravating the border delimitation dispute between Israel and Lebanon, which has been unresolved for several decades [29]. Lebanon is under the control of the Hezbollah political party, which plans to import gas from Iran and does not have diplomatic relations with Israel.

In fact, the region has the potential to become a pipeline hub of energy security in the Middle East, if an arrangement for the delivery of natural gas from Israel to Egypt, Jordan and Syria can be planned and agreed upon with the construction of new pipelines. However, the current situation in the region has aggravated the instability of the relationships between the states interested in energy security that requires the involvement of Israel.

Since such regional challenges and geopolitical risks have not been solved, the most major concern and focus for Israel is Hezbollah's Precision Guided Missile Project, which can bring significant threats to Israel's infrastructure via attack with GPS-guided missiles [30].

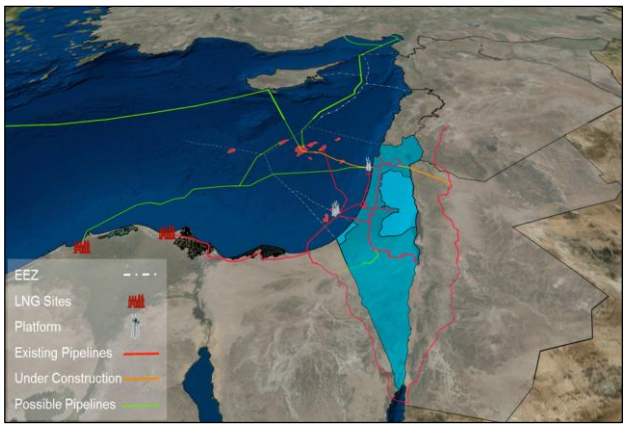

Figure 3. Leviathan and its export routes. Source: NewMed Energy [31]

The Precision Project depends on GPS guidance kits. The project consists of cruise missiles and UAV, among others. The Israeli Defense Forces believe the attacks are guided by GPS and each UAV is capable of delivering some 5 kilograms of explosives and each missile can carry 300 kilograms. Such weapons could be directed against targets both out at sea and along Israel's coastline. Indeed, the Karish gas platform, along with the Leviathan gas reservoir, has already experienced attacks by UAVs [32]. Indeed, the missile attack on Saudi Arabia's Abqaiq oil facility in September 2018 proved the capabilities of this GPS-guided weaponry.

The Israeli Navy and IDF assume that explosive-carrying UAVs or submarines guided by GPS could be directed against the country's offshore energy infrastructure, such as Tamar and Leviathan. In this case, GPS jamming will be a key countermeasure.

Meanwhile, Israel's Iron Dome defence system uses Tamir rockets to intercept Hezbollah missiles. The rockets are guided by onboard GPS receivers and electro-optical sensors, which enable the rockets to adjust their course to track down missiles.

The phenomenon of both sides depending on GPS is symbolic of how the technology is critical on the modern battlefield. GPS systems are simultaneously employed to attack and defend against other states. Indeed, immediately preceding their attack on the Iranian embassy in Syria in April 2024, Israel prepared for Iranian counterattacks by jamming GPS signals within Israeli territory, although civil life was affected. Jamming is a measure with two sides to its character. On the one hand, it is quite effective in preventing GPS-guided missile attacks, while on the other hand, Israeli defences are at a disadvantage without GPS signals within its territory. Thus, hostilities employing GPS between Israel and Iran demonstrated the critical necessity of GPS and its jamming after the Hamas attack in October 2023 aggravated the Israel-Palestine conflict [33].

3 LEGAL STRUCTURES OF REGULATIONS AGAINST GPS JAMMING

The regulation or prohibition of GPS jamming and spoofing is apparently beneficial to the safe operation of critical infrastructures; those functions are reliant upon GPS.

At the same time, jamming was characterised in the beginning as a justifiable reprisal in response to illegal acts previously committed by foreign governments, such as an intentional unauthorised, often political, broadcast. A territorial state receiving those illegal broadcasts needs to send stronger signals to jam them. It is also useful to jam the frequency for explosives, such as RC-IED, within unstable regions such as Iraq and Afghanistan. Thus, it is used as a protective measure as well as a tool of wrongdoing. Consequently, jamming had not been defined as an illegal act or terrorism. Defining GPS jamming is the most difficult part of the codification process.

3.1 *Historical Status of GPS Jamming in International Law*

An international legal basis for the regulation of jamming was firstly constructed within the framework of ITU's frequency allocations. The ITU is charged with extending international cooperation and promoting

development of technical facilities. To achieve this, the ITU assigns bands of radio frequencies so that unintentional harmful interference will be less likely between different states [34]. Thus, the ITU contributes to efficiency of telecommunication services and prevents accidental entanglement—multiple signals sharing one frequency—but does not specialise in controlling intentional illegal jamming. The ITU conferences discussed the legal status and regulation of jamming in the context of freedom of information but did not reach an international agreement [35].

In addition to the regulations of the ITU, the Law of the Sea and maritime law are also able to partially regulate spoofing, since the safe operation of navigation depends highly upon the AIS, which is a system where signals transmitted from vessels show their position by GPS. The IMO is an authoritative entity that controls the safety of navigation and ship operation by preventing collisions via AIS.

The Law of War has slowly and historically developed its forms and contents. First, state practices with respect to the means and methods used in combat have accumulated and been recognised as fragmented and unwritten customary rules. Among them, some rules were codified as multilateral conventions to the extent that states explicitly agree. The miscellaneous rules thus established are basically characterised in two categories; regulations on the means of combat, such as the prohibition of chemical weapons and on the methods of combat, such as the prohibition of attacks on nuclear power plants.

In contrast to this classical law, which has a long history and is still often called jus in bello in Latin, GPS and its interferences is one of the latest combat techniques. Therefore, GPS spoofing or, more generally, cyber-attacks, are not simply or directly regulated by the classical legal instrument, the Law of War.

The issue of how the laws of the sea and war - in other words, rules of naval engagement - regulate spoofing in light of the traditional principles of freedom of navigation and the safety at sea should be immediately clarified.

Thus, considering the historical context, a complete prohibition of spoofing is not feasible. Meanwhile, limits to justifiable jamming and the prohibition of harmful jamming against the safety of life must be established.

In light of the necessity of jamming as a legitimate countermeasure against illegal broadcasts, regulations for jamming are not sufficient when compared to the detailed international technical standards for the design of facilities and equipment that enable GPS receivers to detect and exclude fake signals and ensure safe operation.

Technical standards in international law are mainly codified through the IMO's Maritime Safety Committees. Filters are required to be built into DPSs to avoid and exclude false signals. Some particular types of vessel must have a backup DPS to provide redundancy and resiliency in case of malfunction in the main system. Mandatory regulations have not yet been established to manoeuvre DPSs by certified DP operators but are intended. All these regulations and standards aim to prevent accidents caused by DPSs that depend on GPS signals.

The issue, therefore, is finding concrete methods to prohibit and prevent hazardous jamming, while tolerating justifiable jamming as countermeasures against terrorism.

3.2 *Jamming as Countermeasures and a Cyber-attack*

A dichotomous characteristic of GPS jamming is that legitimate countermeasures and illegal cyber-attacks coexist in the sphere of jamming. As a result, this causes difficulties in defining the legal status and prohibition of jamming and spoofing.

Indeed, the Center for Advanced Defense Studies (C4ADS) published a report in 2019 which detected 9,883 instances of GPS spoofing across the entire Russian Federation, its occupied territories, and overseas military facilities that affected 1,311 civilian vessel navigation systems since February 2016 [36]. According to the report, this spoofing was considered a serious threat to global security, but was also being used as a defence mechanism to protect people and locations from drone attacks.

3.2.1 *Targeted Killing*

Targeted killing is one of the most controversial acts that is supported and realised by GPS technologies. They are defined as "the use of lethal force attributable to a subject of international law with the intent, premeditation and deliberation to kill individually selected persons who are not in the custody of those targeting them." [37] Targeted killing itself is not necessarily a new phenomenon, and state-sponsored killing has been practised throughout history, in the form of assassination as a countermeasure or self-defence.

In the modern era, UAVs enable user states to control remotely, to acquire visually and to ultimately attack targets without casualties of their own. The public has become more aware of targeted killing by UAVs since the beginning of the Russian invasion of Ukraine in 2022 and the current Israel-Palestine conflict.

After the September 11th terrorist attack against the US in 2001, the US and international community became more tolerant of targeted killing than they had ever been before. At a glance, targeted killing was practised by governments, but criticised and discussed by various groups in the US, including the New York South District Court, and finally accepted to some extent by international law.

The most complicated argument regarding targeted killing is whether it should be categorised as self-defence in wartime or as law enforcement against crime. If it is the former, international humanitarian law and the law of war will be applied. Under this legal scheme, enemy combatants can be targeted and killed when they commit hostile activities against civilians or military allies.

On the other hand, in the case of the latter, terrorists should be brought to court and judged as criminals with due process in accordance with the national constitution of that country. Additionally, law

enforcement jurisdiction is based on the territorial principle in contrast to the more extensive realm of UAVs' flight range.

The territorial principle is the most fundamental basis on which to exercise jurisdictions. Under this principle, each state restrains from exercising such rights within other states' territories so that multiple states' jurisdictions do not overlap or conflict with each other. From this standpoint, as extraterritorial search, seizure, investigation, interrogation, and arrest activities are problematic, targeted killing is also an issue.

Indeed, the Parliamentary Assembly of the Council of Europe adopted Resolution 2051 in 2015, in which the use of armed drones for targeted killings raises serious questions in terms of human rights and other branches of international law [38].

Since there are many intricate issues to solve single-handedly, it is imperative to analyse each case individually. Targeted killings have been carried out to neutralise terrorists, such as Al-Qaeda operatives. In this case, one of the issues is whether the 'war on terror', 'special military operations', or other armed conflicts are categorised as a war or a form of law enforcement. Also, it is questionable whether the law of war or domestic laws legally allow a government to kill terrorists.

A recent concern in the US is whether American citizens can be targeted if or when they were members of Al-Qaeda. Not only for combatting such terrorist organisations, drones are also used to search for drug traffickers around the southern US border with Mexico. This is clearly a domestic use of UAVs supported by GPS.

Discussing targeted killing is, therefore, to distinguish the subject, object, purpose, and location before determining its legality. While anti-terrorism measures are a positive aspect of GPS use, jamming will simultaneously be worthwhile in preventing illegal attacks that use GPS and drones. In this regard, the focus of discussion on the precise legal justification or illegal use of GPS and targeted killings are parallel. The US administration concluded that it is lawful for US government employees or contractors to target persons for killing, including US citizens, who are suspected of ties to Al-Qaeda or other terrorist groups. This created a foundation, such as the right to self-defence, for the legality of the use of GPS jamming as a countermeasure or cyber-attack.

3.2.2 *The Right to Self-Defence*

From the broader framework of the right to self-defence rather than targeted killings, Article 51 of the UN Charter stipulates that the right to self-defence arises if an armed attack occurs. According to this provision, three requirements must be satisfied for the justification of the use of force as an exercise of the right of self-defence. First, an armed attack must occur to enable the victim state to legally use force as an exercise of the right of self-defence. This condition relates to the prohibition of anticipatory self-defence. Second, the preceding use of force must fall into the scope or range of an armed attack, which is the most serious category of the use of force. Third, a balanced use of force to defend the state from a pressing illegal armed attack is required.

Besides kinetic attacks—typically destructive, direct-ascent anti-satellite (ASAT) missiles—non-kinetic attacks, such as GPS interference against vessels navigating within narrow international straits, are serious threats to safe navigation and often detected by the US Coast Guard Navigation Center (NAVCEN).

Having considered these conditions provided by Article 51, traditional international law theory defines the right of self-defence as the inherent right of a state to use force in response to an armed attack. This is an exception to the prohibition of the use of force in Article 2, paragraph 4 of the UN Charter.

Based on the legal framework of the right to self-defence, safety and protection of merchant vessels in strategic water courses such as the Hormuz Strait, the Black Sea or Taiwan Strait, the concept of armed attack and the time of occurrence of the armed attack are interconnected issues. Merchant vessels are located far from their flag states and they are private actors. Therefore, even if a vessel is attacked, it cannot necessarily be identified as an armed attack against its flag state. In addition to this, the scale of the armed attack should be examined and discussed to decide whether the attack—even on a single merchant vessel— can still be categorised as a most serious use of force against the flag state.

The issue of the scale of attack on merchant vessels influences the issue of the level of armed attack on satellites. Jamming the uplink between the control segment and satellites, and the downlink between satellites and receivers cannot be unconditionally categorised as an armed attack that legitimises the right to self-defence. On the other hand, sending stronger radio signals to override jamming can be considered a legally accepted countermeasure.

In a recent case, the Israel Defence Forces and its home front command division use specific radio frequencies around Tel Aviv and Haifa to jam GPS-guided missiles launched from the southern part of Lebanon. At the same time, it affects Israeli civilians, who receive information regarding the likely landing point of missiles on their mobile phones. Jamming confuses the information of location, navigation, and communication systems. The IDF invented and introduced a new method to alert civilians by sending messages via cellular towers instead of GPS frequencies [39].

Having considered cases related to targeted killings and the right to self-defence, it is clear that GPS can be used as a tool of targeted killings, justifiable or not, and legitimate defence. In other words, GPS and its jamming have a dichotomous nature.

4 LEGAL FOUNDATION OF JAMMING IN THE LAW OF WAR

GPS, the latest technology that is not involved within the traditional scope of law of the sea and war, needs its legal status to be clarified. This chapter will examine the significant meaning of the basic legal scheme of the

sea for safe navigation and shipping during naval battles with respect to GPS.

4.1 *Historical Development of the Use of the Sea and the Law of War*

At this moment, when the Coronavirus pandemic is disrupting the global supply chain, the significance of borders that exclude external threats from entering territories has been revisited. In this regard, quarantine functioned to prevent the intrusion of emerging infectious diseases. In much the same way, blockades are one of the most effective methods to destroy an enemies' maritime trade during wartime.

At the same time, the continuation of maritime commerce between neutral states and belligerents, as well as freedom of navigation of neutral states are guaranteed by the Law of War. Consequently, equilibrium of stringent conditions between belligerents waging war and neutral states continuing maritime commerce was historically sought, adjusted and settled on in order to legalise blockades.

As a prime example, in the 1987 case of Amerada Hess Shipping v. Argentine Republic, the US court judged that international conventions recognise the right of a neutral ship to free passage on the high seas [40].

During the Falklands War, both belligerent states—the UK and Argentina—declared 200 nautical miles around the islands as 'exclusion zones' and would attack foreign ships entering these zones. Therefore, on June 3, the United States Maritime Administration sent a list of US flagged vessels and US interest Liberian tankers, including Hercules, to both the UK and Argentina to ensure that these neutral vessels would not be attacked.

Amerada Hess used Hercules to carry oil from Alaska, around the southern tip of South America, to its refinery in the US Virgin Islands. On May 25, 1982, Hercules embarked from the Virgin Islands, fueled but without cargo, headed for Alaska. On June 8, the ship was navigating about 300 nautical miles off the Argentine coast and 200 nautical miles from the Falkland Islands, in international waters outside the exclusion zones, when it was attacked without warning by Argentine aircraft.

International recognition of the rights and protection of ships bearing the flag of a neutral state can be found in paragraphs three and four of the Declaration Respecting Maritime Law of 1856 (the 'Paris Declaration'). Paragraph three declares that, "neutral goods, with the exception of contraband of war, are not liable to capture under enemy's flag". Paragraph four continues that, "blockades, in order to be binding, must be effective, that is to say, maintained by a force sufficient really to prevent access to the coast of the enemy." [41]

Thus, in order to be effective, a blockade must be enforced by vessels being in physical proximity to the enemy port(s). However, under paragraph three, trade and navigation by neutral ships will not be unnecessarily deterred or hindered by the blockade. This is an exact point of equilibrium between belligerents and neutral states. In disregard of these rights, an oil tanker used by Amerada Hess was attacked on the high seas by Argentine military aircraft in 1982.

The court referred in the judgement to a contemporary statement of international concern and accord on the protection of neutral ships. It upheld the Geneva Convention on the High Seas of 1958 (the High Seas Convention), in which the rights of neutral ships are considered established by international law, and to which the US and Argentina were signatories. The High Seas Convention codified the practice of nations with respect to the rights of neutral ships in time of war. Article 22 of the High Seas Convention provides that a warship encountering a foreign merchant ship on the high seas may not board her without suitable grounds for suspecting piracy, slave trading or use of false flags. Even when there are grounds for suspicion, proper procedure is not to attack, but rather investigate by sending a party to inspect the ship and her documents. If an inspection fails to support the suspicions, the merchant ship shall "be compensated for any loss or damage that may have been sustained."

This conflict and adjustment of interests is not unique to sea battles, but common to other ocean management and schemes as well. The ocean is a potential battleground for the extraction and ownership of natural resources as well as the right to free navigation. In terms of the rights of coastal states to explore continental shelves, Article 77, paragraph 1 of UNCLOS says that these states may exercise their sovereign rights over their continental shelf for the purpose of exploring it and exploiting its natural resources. Their exclusive rights stretch at least 200 nautical miles from their coastline as a natural extension of their land territories.

Thus, the Law of the Sea allocates the sovereign rights to natural resources to the state in whose territorial jurisdiction they are discovered. Consequently, maritime delimitation disputes can occur in order to obtain those resources. As a result, rights to freedom of navigation to other states can be threatened. In this regard, Ukraine had some claims about the delimitation of the Black Sea, similar to the border dispute between Israel and Lebanon around the Leviathan gas field.

A case concerning the limits of the EEZ between Romania and Ukraine was submitted to the International Court of Justice (ICJ) by Romania. Romania and Ukraine agreed a treaty on Good Neighbourliness and Co-operation and the Additional Agreement in 1997, which has a provision to negotiate the delimitation of their EEZ and continental shelves. According to paragraph 4 of the Additional Agreement, the parties may submit cases to the ICJ if negotiations fail. Consequently, Romania brought a case against Ukraine before the ICJ in 2004. In this case, Ukraine asserted some special circumstances to achieve equitable delimitation. For example, the fact that it has already given oil concessions to petroleum companies within the waters being disputed. Although the ICJ refused to adjust the delimitation line by oil concessions, a discovery of natural resources can be a cause of maritime delimitation disputes. As a result, the Olimpiskoye gas field is exploited by Romania, to whom the area belongs.

Ukraine had another dispute with regard to the Black Sea. In 2016, it served on Russia a Notification

and Statement of Claim under Annex VII to UNCLOS, referring to a dispute concerning coastal state rights in the Black Sea, Sea of Azov and Kerch Strait [42]. Ukraine presented its position before the Permanent Court of Arbitration (PCA) in October 2024. Ukraine asserted that the PCA must order Russia to remove the Kerch Bridge to restore passage for the vessels of all states following UNCLOS. During this war, the Law of the Sea can be referred to in court as a foundation for the use of the sea.

Furthermore, a newly emerging dispute is a 135 billion cubic metre (bcm) natural gas reserve that Turkey found in 2020 at a depth of 2,100 metres in Sakarya field, within its EEZ. The field is located in the southwestern part of the Black Sea, 100 nautical miles from the Zonguldak province of Turkey. This case might have an impact on the area near the intersection of Romanian, Bulgarian, and Turkish waters [43].

From the standpoint of the Law of the Sea, the management of the sea and seabed has experienced a period of transition from complete "dominion" to functional jurisdiction. Developing countries demand "fair distribution" of the benefits from these activities because they have had their continental shelves and their natural resources plundered by foreign entities even though, according to UNCLOS, they are protected under the sovereign rights of producing countries. The point is that the developed countries, which contribute to the techniques for exploration and exploitation of the seabed, are required to share the revenue from development of the seabed based on their physical and financial risks of seabed exploitation.

Therefore, this sort of confrontation for resources can not immediately reach an agreement on the fair sharing of revenue among the global community. However, identifying common interests and constructing real partnerships with neighbouring countries materialise the core and common value of safe navigation.

Due to an insufficiency in enforceability, the Law of the Sea is limited in its ability to eliminate GPS jamming at present. However, states know that none can deal with or solve global issues such as freedom of navigation on the high seas and safety of shipping by acting alone. Thus, states need to discuss, negotiate, and agree on these issues which are emerging in the global arena. The Law of the Sea often provides useful frameworks and a common ground for sovereign states to build robust foundations of a new legal order for the use of GPS to be applied to the ocean and space. This would be a breakthrough for a transition in the legal status of GPS jamming within the framework of the freedom of navigation, which is an established principle.

4.2 *Law of War and Diplomatic Protection*

From the viewpoint of international law, state responsibility will become an issue to solve newly emerging problems regarding GPS jamming in both military and civilian contexts. Industry and the military are increasingly reliant on GPS. Since it has both offensive and defensive functions, legal schemes are required that allow the legitimate use of GPS while prohibiting illegal attacks.

However a common understanding regarding the illegality of jamming GPS cannot be agreed upon between sovereign states, which strongly insist on maintaining their right to use force against belligerents. As a result, GPS jamming is not yet regulated by the Law of War. The concepts of C4ISR (command, control, communication, computer, intelligence, surveillance, reconnaissance) and C5ISR (C4ISR plus 'cyber') are now focusing on making the military more effective in the context of martial evolution [44]. From this standpoint, the stability and integrity of GPS is a critical factor. To operate and control UAVs, and—vice versa—to prevent incoming GPS-guided missiles, GPS has an indispensable role in offensive and defensive operations.

In addition to military activities, international law has a number of important established principles for industry, one of them being the diplomatic protection of nationals. This principle often becomes an issue because not only do people have a nationality, but vessels have one as well, i.e., the flag it raises. However, the ocean is an international crossroads and indeed a single vessel is an international complex which consists of its flag state, owner, consigner, nationality of the crew, etc. The principle of diplomatic protection, established as a customary international law, has two issues concerning strict conditions for the application of diplomatic protection.

The first one is the nationality rule, which is generally stated as follows: from the time of the incident(s) until the ruling, the claim must belong to persons having the nationality of the claimant state and not the defendant state. In other words, states may exercise diplomatic protection only for their nationals.

Therefore, in the case of I'm Alone, the Commissioners were concerned with the ship's owners, whose nationality was not Canadian (the claimant), but American (the defendant). As a result, the arbitral ruling decided that the Canadian government could not claim that the US was responsible for the sinking of I'm Alone.

The right to diplomatic protection allows a state to present an international claim against a wrongdoing state on behalf of its national, when the national is injured, or their property is confiscated without compensation, in breach of due diligence towards the treatment of foreign nationals. In other words, international law requires states to treat foreign nationals and their property properly. If they do not, the victim's country may be entitled to exercise diplomatic protection.

In fact, the cases brought before the ICJ and other international proceedings are not limited to ones of individuals, but also corporations. When a ship is hit and sunk because of the exercise of force during hot pursuit, such as the case of I'm Alone, the flag state can bring an international claim against the state undertaking the hot pursuit [45].

Therefore, diplomatic protection is problematic where a ship flying a foreign flag is actually hired by nationals whose nationalities are identical to the state which caused damage to the ship and cargo. Since the vessel can be considered to have the nationality of the foreign state and be treated as its own national, nationals should obtain satisfaction through ordinary

domestic procedures. This was the case of the arbitral sentence in the case of Amerada Hess and the case of *I'm Alone*.

I'm Alone was a British vessel, registered in Canada, used for running rum to the USA in breach of the Volstead Act, which had prohibited the production and import of alcoholic beverages in the 1920s. She was sunk on the high seas on March 22, 1929 by the US revenue cutter *Dexter*.

In this case, one of the issues that should have been resolved was the implication of ownership and control of the vessel, and the shares of the corporation owning the vessel. Answering this question, the Commissioners decided that *I'm Alone*, a British ship of Canadian registry, was de facto owned and controlled by US citizens for illegal purposes, contravening US law. In conclusion, the Commissioners denied the necessity of compensation by the US to His Majesty's Canadian Government for the loss of the ship and cargo.

This case thus raised the issue of whether the formal nationality might be of no importance but the de facto ownership might be more significant for the claimant of indemnity or compensation. The complexity of nationalities of ships is the cause of the ambiguous nature of state responsibility regarding damage of ships through GPS jamming.

Recently, private multinational enterprises' activities cross territorial borders, so the traditional principles of international law, such as diplomatic protection, should adapt their approach to fit the swift movement of people and finances. As a result, not only states and militaries, but also private industries, such as maritime shipping companies, must be protected against GPS jamming and illegal attacks on the sea.

5 CONCLUSION

This paper examined cases of GPS interference and the past and current discussions concerning the safety and security measures used to build a legal order to regulate GPS jamming for safe navigation. GPS jamming has been classified as both a legal countermeasure and illegal activity, as discussed by the ITU member states. As a result, even though GPS jamming is critically dangerous to the safety of life at sea and, in a broader context, social economy, these acts are not formally prohibited by international agreement in current legal structures.

Indeed, the cases in the Black Sea ports in Ukraine and Ben Gurion International Airport in Israel illustrate how easily entities depending on GPS signals are interfered with. At the same time, the targeted killings, even though they are controversial, were successfully executed depending on the accuracy of GPS. Preventing UAVs' attacks are also a positive outcome of GPS jamming.

Such opacity and versatility of the role and legal status of GPS jamming is depicted in this paper through the analysis of cases and legal instruments.

One of these instruments—the Law of the Sea—provides a legitimate order to guarantee the right of freedom of navigation, which can potentially provide a legal basis against illegal GPS jamming. Secondly, the Law of War also strictly requires the preconditions of armed attack, necessity and balanced counterattack to legitimise self-defence.

Based on these two fundamental legal instruments, this paper has tried to clarify the legal and technical issues related to the use of GPS in both peacetime and wartime. It compared the positive aspects of GPS jamming as a defensive measure or neutralising other states' defence systems with the negative aspects of wrongdoing. Although GPS and its jamming have an indispensable function on the battlefield, legal definition of GPS jamming is not yet fully developed due to its dichotomous nature.

In comparison, the recent nature of armed conflict has been evolving. UAVs steered by GPS have demonstrated their capabilities as weapons. Their remarkable results in military operations are closely tied to GPS. This is an example of how constant efforts in developing defence technologies bring success.

GPS jamming and spoofing on a massive scale is generally not committed by civilians due to the large and expensive equipment necessary for such activities. Rather, armed forces depend on GPS and its jamming to defend essential infrastructure from GPS-guided UAVs and missile attacks.

As a result, countries that make use of GPS jamming did not agree with its prohibition. But frequent jamming instances have made governments aware of how influential it can be in preventing attacks. Thus, governments are beginning to recognise that other states are committing GPS jamming or spoofing. The analysis of practices and establishment of legal theories concerning due diligence of states who should prevent GPS jamming and spoofing, will be a leitmotif in the near future [46].

From the law of war, to be successful in the optimal management and use of GPS, it is worthwhile to establish legal and technical standards with neighbouring countries during peacetime. In wartime, while belligerents adhere to established norms that protect neutral states' interests, they must also achieve their own military goals.

It is no exaggeration to say that, since ancient times, states and individuals who control navigation, shipping and logistics control the world. The earliest example is the Egyptian civilisation, which has benefited greatly from navigation since 2500 B.C. In those days, a stable current and winds allowed them to manage the shipping of goods and people along the Nile River. The same civilization left records dating to around 1500 B.C., which depict a large sea-going three-masted ship.

Thus, waterborne transport was the earliest and the most efficient means of commerce. Consequently, legal disputes have inevitably emerged as the result of conflicts of interest. In light of the necessity of dispute settlement for the continuation of safe navigation and stable trade, mechanisms, procedures, and rules for the fair demarcation and burden of damages were developed in each coastal area. These rules gave rise to what is now known as Maritime Law.

The Law of the Sea, which originated with maritime law and merchant customs, is now facing a world

where the legitimacy of the rule of law is questionable both de jure and de facto in contrast with its origin. From a broader and more long-term perspective, there is a need to establish legal norms to control and regulate GPS technologies—including jamming and its countermeasures—and ensure that these laws have adapted to and caught up with technical progress. It is imperative to attach greater importance to the consideration for the safety of navigation as well as the right to jamming.

REFERENCES

[1] US Federal Aviation Administration: Satellite Navigation - Global Positioning System (GPS). https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps; European Union Agency for the Space Programme: What is GNSS? https://www.euspa.europa.eu/european-space/eu-space-programme/what-gnss. (2024.11.6).

[2] European Global Navigation Satellite Systems Agency: Glossary, 2018, p. 6. https://www.euspa.europa.eu/simplecount_pdf/tracker?file=gps-test-app-definition.pdf. (2024.11.6).

[3] S. Ricciardi and C. Souque: Modern Electromagnetic Spectrum Battlefield from EMS Global Supremacy to Local Superiority, Prism, Vol. 9, No. 3, 2021, p. 132.

[4] S. M. Mountin: The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals, International Law Studies, US Naval War College, Vol. 90, 2014, p. 129.

[5] European Union Aviation Safety Agency: Global Navigation Satellite System (GNSS) Outages and Alterations, Safety Information Bulletin, 2024, p. 1; NATO Shipping Centre: GNSS Electronic Interference.https://shipping.nato.int/nsc/operations/news/2021/gnss-electronic-interference-in-the-mediterranean. (2025.3.22).

[6] J. S. Warner et al.: GPS Spoofing Countermeasures, Vulnerability Assessment, Los Alamos National Laboratory, 2007.

[7] International Maritime Organization: IMO MSC.1/Circ. 645; MSC.1/Circ. 738 Rev. 2; MSC.1/Circ. 1580.

[8] U.S. Coast Guard National Center of Expertise: Introduction to Dynamic Positioning (DP) Systems, 2019, p. 1.

[9] J. Bhatti and T. E. Humphreys: Hostile Control of Ships via False GPS Signals: Demonstration and Detection, Navigation, Vol. 64, Issue 1, 2017, p. 51.

[10] US Department of Defense, Ukraine Map. https://www.defense.gov/Multimedia/Photos/igphoto/2002988295/. (2024.11.6).

[11] NATO Shipping Centre: Electronic interference. https://shipping.nato.int/nsc/operations/news/-2022/situation-on-the-black-sea-and-the-sea-of-azov.

[12] G. V. Galdorisi and K. R. Vienna: Beyond the Law of the Sea: New Directions for U.S. Oceans Policy, Praeger Publishing, 1997, p. 81.

[13] W. J. Aceves: Diplomacy at Sea: U.S. Freedom of Navigation Operations in the Black Sea, Naval War College Review, Vol. 46, No. 2, 1993, p. 63.

[14] Maritime Delimitation in the Black Sea (Romania v. Ukraine), Judgement of 3 February 2009, ICJ Reports 2009.

[15] Dispute Concerning Coastal State Rights in the Black Sea, Sea of Azov, and Kerch Strait (Ukraine v. the Russian Federation), Permanent Court of Arbitration, Case Number 2017-06.

[16] R. Pedrozo: Russia-Ukraine Conflict: The War at Sea, International Law Studies, Vol. 100. 2023, p. 14; H. I. Sutton, Positions of Two NATO Ships were Falsified near Russian Black Sea Naval Base, US Naval Institute News, 2021. https://news.usni.org/2021/06/21/positions-of-twonato-ships-were-falsified-near-russian-black-sea-naval-base. (2024.11.10).

[17] Ministry of Defense of Ukraine: Ukraine Returned under Control «Boyko Towers», 11 September 2023. https://gur.gov.ua/en/content/ukraina-povernula-pid-kontrol-t-zv-vyshkamy-boika.html. (2024.11.20); M. Bugriy: The Cost to Ukraine of Crimea's Annexation, Jamestown Foundation, Eurasia Daily Monitor, Vol. 11, Issue 70, 2014.

[18] US Department of Transportation: 2022-005-Various-GPS Interference & AIS Spoofing. https://www.maritime.dot.gov/msci/2022-005-various-gps-interference-ais-spoofing; ibid., Maritime Administration, MSCI Advisory, at https://www.maritime.dot.gov/msci/2022-003-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-gulf-aden-bab-al-mandeb-strait-red. (2024.11.6).

[19] Navigation Center, US Coast Guard: GPS Problem Status. https://navcen.uscg.gov/gps-problem-report-status. (2024.3.20).

[20] R. B. Peele: Maritime Chokepoints: Key Sea Lines of Communication (SLOCs) and Strategy, US Army War College, Strategy Research Project, 1997, p. 19.

[21] IMO: A 29/Res. 1106, p. 3, para. 3.

[22] S. C. Neff: The Rights and Duties of Neutrals, a general history, Manchester University Press, 2000, p. 98.

[23] State of Israel, Prime Minister's Office, National Cyber Directorate: Israel National Cyber Security Strategy in Brief, September 2017. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf. (2024.11.10).

[24] The Government Secretary of Israel: Government Resolution No. 2444 of February 15, 2015, Advancing the National Preparedness for Cyber Security, p. 1, para. 3. https://nsarchive.gwu.edu/sites/default/files/documents/5989653/National-Security-Archive-Israeli-Government.pdf. (2024.11.10).

[25] M. N. Schmitt: Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, Vol. 56, 2011, p. 575.

[26] International Maritime Contractors Association, GPS systems – Warning of interference. https://www.imca-int.com/information-notes/gps-systems-warning-of-interference/. (2024.11.10).

[27] The case between Guyana and Suriname is symbolic. A private contractor hired by Guyana was exploring the continental shelf in the disputed area with permission from the Guyanese government. Patrol vessels from Suriname requested, under threat of use of force, that the contractor leave the area. An arbitral tribunal based on UNCLOS held that this action verged on threats of military action, as defined by paragraph 4 of Article 2 of the UN Charter, rather than law enforcement activities. Guyana and Suriname, Arbitral Award.

[28] US Energy Information Agency, https://www.eia.gov/todayinenergy/detail.php?id=12611

[29] O. Mizrahi and O. Eran: The Negotiations between Israel and Lebanon on the Maritime Border, Institute for National Security Studies, INSS Insight, No. 1180, June 24, 2019, p. 4.

[30] C. Bauer, H. Ghaddar and A. Orion: Iran's Precision Missile Project Moves to Lebanon, Washington Institute for Near East Policy, Policy Note, Vol. 56, 2018, p. 2; S. Henderson: The Obstacles Still Facing Israel's Leviathan Gas Field, Policy Alert, Washington Institute for Near East Policy, 2019.

[31] NewMed Energy, Operations of Leviathan. https://newmedenergy.com/operations/leviathan/. (2024.11.20).

[32] I. Klotsman: Iran's Threat to Attack Israel's Gas Platforms, Times of Israel, August 8, 2024; Y. Lappin, Z. Haimovich and S. Shohat: Can Israel Defeat Iran's Precision Guided Missile Threat? Commentary, Mir Yam Institute, 2022.

[33] See also, S. Peterson and P. Faramarzi: Exclusive: Iran hijacked US drone, says Iranian engineer, Christian Science Monitor, 2011.
[34] P. Sands and P. Klein: Bowett's Law of International Institutions, 6th ed., Sweet & Maxwell, 2009, p. 105.
[35] L'institut de droit international: Annuaire de l'institut de droit international, Tome 50-I, 1963, p. 413.
[36] Center for Advanced Defense Studies: Above Us Only Stars, Exposing GPS Spoofing in Russia and Syria, 2019, p. 24.
[37] T. B. Hunter: Targeted Killing, Self-defense, preemption, and the War on Terrorism, booksurge, 2009, p. 33.
[38] Parliamentary Assembly of the Council of Europe: Drones and targeted killings: the need to uphold human rights and international law, 2015.
[39] Israel Defense Forces: Home Front Command's Guidelines; B. Diakun: War zone GPS jamming sees more ships show up at airports, Lloyd's List, 2024.
[40] Amerada Hess is a US oil company, which registered an office in Liberia and entered a long-term time-charter agreement with United Carriers (UC) in 1977 for use of the oil tanker Hercules. The ship was registered in Liberia and flew a Liberian flag.
[41] Amerada Hess Shipping v. Argentine Republic, 830 F.2d 421, 428-29 (2d Cir. 1987).
[42] Dispute Concerning Coastal State Rights in the Black Sea, Sea of Azov, and Kerch Strait (Ukraine v. the Russian Federation).
[43] W. C. Ackerman: Turkey: A new emerging gas player with resources and infrastructure, Middle East Institute, 15 June 2022.
[44] US Army Combat Capabilities Development Command: C5ISR. https://c5isrcenter.devcom.army.mil/activities/. (2024.12.6).
[45] S. S. I'm Alone (Canada v. United States), Reports of International Arbitral Awards, 30 June 1933 and 5 January 1935, Vol. III, pp. 1609-1618.
[46] M. N. Schmitt: In Defense of Due Diligence in Cyberspace, Yale Law Journal Forum, Vol. 125, 2015; S. Besson: La due diligence en droit international, Martinus Nijhoff, 2021, p. 269.