GNSS Jamming and Spoofing under National and International Law

*Ingo Baumann and Erik Pellander**

Abstract

Jamming and spoofing can pose significant threats to space-based assets and the services provided by them. Global navigation satellite systems (GNSS) are specifically vulnerable in this respect, considering the very low power of their signals and services. Numerous incidents of GNSS jamming and spoofing have already been reported. Cases of jamming are often not intentional and regularly have only short-term and geographically limited impacts. However, there are also intentional cases of jamming and spoofing is intentional by default. Due to their importance for military operations, for critical national infrastructure and key economic sectors, GNSS constitute primary targets of intentional jamming and spoofing. The paper analyses remedies in response to jamming and spoofing under international law as well as aspects of national law in relation to jamming and spoofing of GNSS signals.

Keywords: Jamming, Spoofing, International Law, GNSS, Electronic Warfare

1. Introduction

Disrupting GNSS signals may have severe effects on military operations, critical national infrastructure and key economic sectors. GNSS are specifically vulnerable due to the very low power of their signals and services. As warfare is increasingly shifting from physical to virtual, GNSS may therefore constitute primary targets in future warfare.

In theory, there are many different ways how to disrupt GNSS systems and the signals provided by them. In practice, jamming and spoofing of GNSS signals are the prevailing causes for such disruption. These practices are not directed to the satellite system as such, but against the signals emitted.

* Dr. Ingo Baumann, BHO Legal, Hohenstaufenring 29-37, 50674 Cologne, Germany; ingo.baumann@bho-legal.com.
Erik Pellander, BHO Legal, Hohenstaufenring 29-37, 50674 Cologne, Germany; erik.pellander@bho-legal.com.

Jamming refers to disrupting radio communications by overpowering the signals being sent to or from the transmitting station by using a signal at the same frequency and higher power. Spoofing mimics the characteristics of a true signal so that the user receives the fake (or spoofed) signal instead of the real one.

Already in 2001, the US Department of Transportation (DoT) released a report warning that the US Global Positioning System GPS, "becomes an increasingly tempting target that could be exploited by malicious persons or countries". The report found that "[t]he potential for denying GPS service by jamming exists. The potential for inducing a GPS receiver to produce misleading information exists" and that "[t]he GPS signal is subject to degradation and loss through attacks by hostile interests."

GNSS is embedded in a wide range of economic, public and social functions, including critical infrastructure and services. According to a 2012 National Risk Estimate conducted by the US Department of Homeland Security, "US critical infrastructure sectors are increasingly at risk from a growing dependency on the Global Positioning System (GPS) for space-based position, navigation, and timing (PNT)". A 2017 study undertaken by London Economics on the economic impact to the UK of a disruption to GNSS found that "[a]ll critical national infrastructures (CNI) rely on GNSS to some extent".

All infrastructures and activities using GNSS are generally vulnerable for disruptions through jamming and spoofing. However, dependencies vary from sector to sector and may range from total, i.e. GNSS is required to operate at all, to low, i.e. the sector is only inconvenienced by the loss of GNSS signals.

In the following, the legal analyses addresses potential remedies under international law as well as aspects of national law in relation to jamming and spoofing of GNSS signals.

2. Remedies Under International Law

2.1. ITU Law

GNSS transmits positioning and timing information via radio frequencies which are governed by the legal framework of the International Telecommunication Union (ITU). The main ITU instruments relevant to management of these radio frequencies are the Constitution (CS), and, most importantly, the Radio Regulations (RR).

In terms of ITU law, GNSS falls under the radionavigation-satellite service (RNSS) category. For this service, the following frequency bands are currently allocated: 1164-1215 MHz; 1215-1300 MHz; 1559-1610 MHz; 2483.5-2500 MHz; 5000-5030 MHz.

As with all types of frequency allocations, RNSS enjoy a certain level of protection against interference as determined by the RR. Interference above these levels is considered harmful under the ITU legal framework, to the extent that it endangers the functioning of the radio communications service in question. The following definitions and provisions come into play when assessing whether and to what extent jamming and spoofing is to be considered as harmful interference.

Under No. 1.166 of the RR, interference is defined as the "effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."

GNSS jamming and spoofing fall under this definition, as they are the effect of unwanted energy, i.e. the jamming/spoofing signal, are manifested by performance degradation (e.g. service outage due to jamming), misinterpretation (e.g. false data in case of spoofing), or loss of information (e.g. loss of information based on service outage due to jamming).

As provided by No 1.169 RR, interference is harmful, if it "endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations [emphasis added]." Jamming and spoofing always have the potential of endangering the functioning of a radionavigation service and, in most cases, lead to degradations or interruptions. Jamming and spoofing of frequency bands allocated to radionavigation services are, accordingly, regularly to be considered as harmful interference in terms of international telecommunications law. The definition of harmful interference does not distinguish between unintentional or intentional interference. Unintentional interference through accidental jamming of radiofrequencies used for radionavigation satellite services therefore also falls under the definition of harmful interference.

Article 45 (1) of the ITU CS generally prohibits harmful interference by stipulating that "*[a]ll stations […] must be established and operated in such a manner as not to cause harmful interference to the radio services [...] of other member states or recognized operating agencies or other duly authorized operating agencies, which carry on a radio service, and which operate in accordance with the provisions of the Radio regulations.*" In order to adhere with this provision, States shall ensure that stations licensed by them shall not cause harmful interference (Article 45 (2) CS) and shall take all practicable steps to prevent the operation of electrical apparatus and installations of all kinds from causing harmful interference (Article 45 (3) CS).

This general obligation is further specified by detailed RR provisions on the avoidance of harmful interference and on the procedures to be applied in case of harmful interference.

As for the avoidance of harmful interference, No 4 of the RR sets conditions on the assignment and use of frequencies. It recognizes a special status of radionavigation services by placing additional obligations on administrations to ensure that the frequency bands used for these services are free from interference. According to No 4.10 of the RR, "*Member States recognize that the safety aspects of radionavigation and other safety services require special measures to ensure their freedom from harmful interference; it is necessary therefore to take this factor into account in the assignment and use of frequencies.*"

No 15.1 to 15.21 of the RR set special conditions on the avoidance of harmful interference. In relation to jamming, No 15.1 of the RR stipulates that "*[a]ll stations are forbidden to carry out unnecessary transmissions, or the transmission of superfluous signals […]*". As regards spoofing, No 15.1 of the RR provides that "*[a]ll stations are forbidden to carry out […] the transmission of false and misleading signals […]*". Finally, jamming and spoofing is contrary to the ITU legal framework on the ground that, under No. 19.2 of the RR, "*[a]ll transmissions with false or misleading identification are prohibited.*"

Procedures in case of harmful interference are primarily laid down in No. 15.22 et seq. and No. 13.2 f. of the RR. Under this framework, "*Member States exercise the utmost goodwill and mutual assistance in the application of the provisions of Article 45 of the Constitution and of this Section to the settlement of problems of harmful interference*" (15.22 RR). In resolving cases of harmful interference, States may seek assistance from the ITU's Radiocommunication Bureau which may, according to No 13.2 of the RR, "*help in identifying the source of the interference and seek the cooperation of the responsible administration in order to resolve the matter, and prepare a report for consideration by the Board, including draft recommendations to the administrations concerned.*" Cases of unintentional interference can regularly be solved between the administrations concerned, as necessary through intervention of the Radiocommunication Bureau (BR) and the Radio Regulations Board (RRB). However, the ITU bodies lack appropriate enforcement measures of any decisions taken in case of intentional jamming or spoofing.

2.2. ICAO Legal Framework

In accordance with its mandate stipulated in Article 44 of the Convention on International Civil Aviation[1] (Chicago Convention) to "*develop the principles and techniques of international air navigation and to foster the planning and*

1 Convention on International Civil Aviation, 15 UNTS 295.

development of international air transport" the International Civil Aviation Organization (ICAO) has extensively dealt with developing a framework on the implementation of GNSS in international air navigation.

In 1993, the ICAO GNSS Panel (subsequently renamed Navigation Systems Panel – NSP) was established to develop standards and recommended practices (SARPs) for GNSS in international air navigation which are set down in Annex 10 to the Chicago Convention. Among other matters, these SARPs require that GNSS shall comply with certain performance requirements in the presence of interference meeting the thresholds defined in Appendix B to Annex 10 Volume 1 of the Chicago Convention.[2]

The ICAO Global Navigation Satellite System (GNSS) Manual (Doc 9849) provides information on the operational implementation of GNSS. In its 2017 edition,[3] the manual has a dedicated chapter on GNSS vulnerability (Chapter 5).

As regards intentional interference through jamming and spoofing, Chapter 5 of the manual highlights that

- as long as conventional navigation aids remain in service and all aircraft are equipped to use them, there is little motivation to intentionally interfere with GNSS-based aviation services;
- *"as reliance on GNSS increases* […] *the threat of intentional interference could increase* […];
- *mitigation will be required when disruption is deemed to be possible and would have a significant impact* […]*;*
- *the spoofing of GNSS is less likely than the spoofing of traditional aids because it is technically much more complex* […]*;*
- *a State may adopt a mitigation strategy, if it determines that the risk of intentional interference is unacceptable in certain areas of its airspace and that States should be ready to inform users and deploy reactive measures as described in Appendix F if outage events are detected and reported"*.

As for the matter of national regulation, the manual requires that *"States should prohibit all actions that lead to disruptions of GNSS signals"*. For this purpose, they should develop and enforce a strong regulatory framework governing the use of spoofers and jammers.

In addition to the SARPs provided under Annex 10 Vol 1 to the Chicago Convention and the guidance material provided in the ICAO GNSS Manual, the recommendations 6/7 and 6/8 adopted by the Twelfth Air Navigation Conference in 2012 are of particular concern when it comes to jamming and

2 Section 3.74 of Annex 10 to the Chicago Convention.

3 ICAO, Global Navigation Satellite Systems (GNSS) Manual, Doc 9849, Third Edition, 2017.

spoofing of GNSS signals. Recommendation 6/7 provides that States shall develop a mechanism with the ITU and other appropriate UN bodies to address specific cases of harmful interference of GNSS signals reported by States to ICAO. According to Recommendation 6/8, it is the responsibility of ICAO Member States to

- *"assess the likelihood and effects of GNSS vulnerabilities in their airspace and apply, as necessary, recognized and available mitigation methods;*
- *provide effective spectrum management and protection of GNSS frequencies to reduce the likelihood of unintentional interference or degradation of GNSS performance;*
- *report to ICAO cases of harmful interference with GNSS that may have an impact on international civil aviation operations;*
- *develop and enforce a strong regulatory framework governing the use of GNSS repeaters, pseudolites, spoofers, and jammers."*

On 28 August 2020, the ICAO Secretary General issued a State letter on strengthening of communications, navigation, and surveillance (CNS) systems resilience and mitigation of interference to global navigation satellite systems.[4] The letter requests to *"note the criticality of the issue and the importance of action by States to address it by making use of the ICAO guidance provided in Doc 9849 [ICAO GNSS Manual], and by taking any other measures, as appropriate."* These requests are based on the actions agreed by the 40th session of the ICAO Assembly to strengthen CNS systems resilience and mitigate interference to GNSS.

Under international air law, another legal instrument which comes into play in relation to jamming and spoofing GNSS signals is the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal Convention).[5] Under Article 3 of the Convention, *"[e]ach Contracting State undertakes to make the offences mentioned in Article 1 punishable by severe penalties"*. Offences in terms of the Convention are defined in Article 1 and include interference with the operation of air navigation facilities, as well as the communication of false information endangering the safety of an aircraft in flight.

2.3. IMO Legal Framework

As with ICAO for international air navigation, the International Maritime Organization (IMO) is responsible for the implementation of GNSS in international maritime navigation. IMO has the mandate to oversee the

4 ICAO, State Letter AN7/5-20/89, 28.08.2020.

5 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 974 UNTS 177.

International Convention for the Safety of Life at Sea (SOLAS)[6] by setting carriage requirements, operational requirements and performance standards for world shipping.

In accordance with this mandate, IMO recognizes navigation systems which can be used by international shipping. IMO Assembly Resolution A.1046(27) - Worldwide Radionavigation System determines IMO's policy for recognizing radionavigation systems for ship's navigation. The Resolution requests the IMO Maritime Safety Committee to recognize systems conforming to IMO requirements. Such recognition implies that the system is capable of providing adequate position information within its coverage area and that the carriage of receiving equipment for use with the system satisfies the relevant requirements of the SOLAS Convention. IMO currently recognizes the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS), BeiDou Navigation Satellite System (BDS) and Galileo Global Navigation Satellite System. The Indian Regional Navigation Satellite System (IRNSS) is awaiting final approval.

IMO further oversees the SOLAS Chapter V referring to the safety of navigation for all vessels at sea. Since 2002, SOLAS Regulation V/19.2.16 requires all ships irrespective of size to *"have a receiver for a global navigation satellite system or a terrestrial radio navigation system, or other means, suitable for use at all times throughout the intended voyage to establish and update the ship's position by automatic means"*.

In order to comply with the SOLAS, such receivers shall meet certain performance standards developed by the IMO Maritime Safety Committee. At the time of writing, performance standards are in force for: (GPS) Receiver Equipment (MSC.112(73)), GLONASS Receiver Equipment (MSC.113(73)), DGPS and DGLONASS Maritime Radio Beacon Receiver Equipment (MSC.114(73)), GPS/GLONASS Receiver Equipment (MSC.115(73)), BeiDou Satellite Navigation System (BDS) Receiver Equipment (MSC.379(93)), Multi-System Radionavigation Receivers (MSC.401(95), amended by MSC.432(98)), and Indian Regional Navigation Satellite System (IRNSS) Receiver Equipment (MSC.449(99)).

IMO performance standards are important tools to prevent and mitigate the effects of GNSS jamming and spoofing. As an example, the performance standards for multi-system radionavigation receivers provide that *"[a]n improved resistance to intentional and unintentional radio frequency interference is achieved when two or more independent or frequency diverse radionavigation systems are used"*. Moreover, a failure analyses is required considering the impact of *"jamming, etc."*. In 2017, the Maritime Safety Committee has published guidelines to these performance standards (MSC.1/Circ.1575).

6 International Convention for the Safety of Life at Sea, 1185 UNTS 2.

In June 2019, 14 maritime organizations filed a letter to the Commandant of the US Coast Guard requesting to propose an IMO Council resolution at the 122nd session of the IMO Council in July 2019 that includes:

- *"GNSS signals are important to safety of navigation*
- *Member states should enact measures to prevent unauthorized transmissions on GNSS frequencies*
- *Member states should refrain from interfering with GNSS signals as much as possible, except when required for security reasons.*
- *Member states interfering with GNSS signals for security reasons should issue notices to mariners specifying the time periods and areas impacted to help minimize negative effects on maritime operations."*[7]

According to the report of the 122nd session of the IMO Council, the Council did not (yet) agree on adopting such resolution.

2.4. International Law on the Prevention of War

2.4.1. Threat or Use of Force

Article 2 (4) of the UN Charter states that *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."*

On the meaning of this provision, the International Court of Justice (ICJ) held in the *Legality of the Threat or Use of Nuclear Weapons* Case that the rules governing the use of force *"apply to any use of force, regardless of the weapons employed."*[8] The rules governing the use of force may, accordingly, also apply to jamming and spoofing of GNSS signals.

The question is therefore not *whether* the prohibition of the threat or use of force is applicable but, rather, *when* it applies. The Tallinn Manual,[9] which was prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, provides guidance on this matter. The expert group found that *"it is not the instrument used that determines whether the use of force threshold has been crossed, but rather (…) the consequences of the operations and its surrounding circumstances."* In line with these findings, cyber operations may *"constitute a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"*. In absence of a conclusive definitional threshold, several factors were determined for assessing whether

7 A copy of the letter is available under https://rntfnd.org/wp-content/uploads/Multi-sig-Ltr-to-USCG-IMO-GNSS-Jamming.pdf (accessed 14.01.2020).

8 International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p.226.

9 Schmitt/Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge, 2017.

to qualify cyber operations as a use of force. These factors include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.

The potential effects of jamming and spoofing of GNSS signals, especially on national critical infrastructures, can have such scale and effects that they can reach a threshold comparable to the use of conventional weapons rising to the level of a use of force. This needs to be carefully considered on a case-by-case basis, bearing in mind the above factors.

In case of jamming and spoofing events, there are however several practical hurdles regarding their qualification as a threat or use of force. In some cases, it might already be difficult to identify the originator of the jamming or spoofing operations. In case such operations are undertaken by non-State actors, attribution of the action to a State may also not be easy. Furthermore, damages are often not a direct consequence of jamming and spoofing.

2.4.2. Armed Attack and the Right of Self-Defence

The qualification of jamming and spoofing as a threat or use of force is not tantamount to an armed attack. Only the latter would grant the State affected the right to self-defense. Within the framework of the right of self-defence, a State can react to an armed attack with its own use of force, without itself violating the prohibition of the use of force. As the ICJ held in the *Military and Paramilitary Activities in and against Nicaragua* Case, an armed attack must constitute the *"most grave forms of the use of force"*. In other words, an armed attack *"only exists when force is used on a relatively large scale, is of a sufficient gravity, and has a substantial effect."*[10]

Whether this threshold for an armed attack is exceeded is subject to consideration in each individual case. However, an armed attack can be assumed if: *"an act or the beginning of a series of acts of armed force of considerable magnitude and intensity […] which have as their consequence […] the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, i.e. its political independence, as well as damage to or deprivation of its physical element namely, its territory"* occurs.[11]

In order to cross the threshold of an armed attack, the relevant act(s) must therefore have significant and immediate destructive effects, such as e.g. considerable loss of life and/or extensive destruction of property. When assessing whether the threshold of an armed attack is reached, it should be

10 International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I.C.J. Reports 1986, p.14.

11 A. Constantinou, The Right of Self-Defense under Customary International Law and Article 51 of the UN Charter, 2000.

taken into account that the right of self-defense is one of the rare exceptions of the prohibition to use force under international law and therefore requires a narrow interpretation. An armed attack through jamming or spoofing of GNSS signals can therefore be assumed only in extreme circumstances. In any case, jamming/spoofing that merely leads to a brief or periodic interruption of non-essential services does not qualify as an armed attack.

2.4.3. Countermeasures

A State may always initiate countermeasures in response to jamming or spoofing of GNSS signals short of an armed attack, when it constitutes a threat or use of force or otherwise a violation of an international obligation (internationally wrongful act). On the potential use of countermeasures in response to threats against space assets, an U.S. Air Force official stated that *"below an armed attack, the most applicable response is a countermeasure"*.[12]

Countermeasures are acts or omissions of the injured State against the responsible State which, in principle, would violate international obligations of the former towards the latter, but are justified as countermeasures because of the internationally wrongful act.[13] An injured State may therefore be entitled to act contrary to its international law obligations to ensure that the originator refrains from actions in breach of international law. Limitations on the use of countermeasures include that countermeasures may only be taken against *States*; that the State must be responsible for the violation (attribution of acts and omissions of non-State actors are of particular concern in this context); that the countermeasures are taken in order to persuade the responsible State to resume compliance with its international obligations; and that the countermeasures must be proportionate to the injury to which they respond.[14]

The State resorting to countermeasures must notify the responsible State of such measures and offer negotiations. Additionally, States shall not resort to the right of countermeasures when the internationally wrongful act has already ended. Accordingly, it is required that an event of jamming or spoofing is still ongoing or is likely to be repeated.

2.4.4. Collective Security

If the UN Security Council determines that there is a threat to peace, a breach of peace or an attack, it will decide which measures are to be taken to

12 S. Erwin, Sorry Sci-Fi Fans, Real Wars in Space Not the Stuff of Hollywood, Space News, 02.01.2018, https://spacenews.com/sorry-sci-fi-fans-real-wars-in-space-not-the-stuff-of-hollywood/ (accessed 14.01.2021).

13 International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Annex to General Assembly resolution 56/83 of 12 December 2001.

14 Ibid.

maintain or restore international peace and security. Within this context, the UN Security Council may authorize measures, which may not necessarily involve the deployment of armed forces or measures by air, sea or land.
Depending on the individual case and its specific implications, the UN Security Council may determine that jamming or spoofing of GNSS signals poses a threat to peace, a breach of peace or an act of aggression.
Even though the UN Security Council did so far not qualify jamming or spoofing of GNSS signals accordingly, it would be within its authority. In view of the above-mentioned cases, it can however be doubted whether the UN Security Council will ever reach such decision with its current composition.

3. Remedies Under National Law

The above-mentioned international legal frameworks are applicable among States. Private individuals are not directly bound by them. In order to ensure conformity with its international obligations under these frameworks, a State needs to transform its international obligations into national law.
As for the ITU legal framework, this in particular concerns national telecommunications law ensuring that frequency assignments and their use are undertaken in conformity with the ITU legal framework. In this regard, the obligation not to cause harmful interference as well as the prohibition of transmissions with false or misleading identification may come into play.
ICAO's standards and recommended practices on the use of GNSS in civil aviation need to be applied by national aviation authorities. Further, Recommendation 6/8 adopted by the Twelfth Air Navigation Conference in 2012 and the ICAO Global Navigation Satellite System (GNSS) Manual require a strong national regulatory framework governing the use of jammers and spoofers. Under the Montreal Convention, States are obliged to make interference with the operation of air navigation facilities, as well as the communication of false information endangering the safety of an aircraft in flight punishable by severe penalties. For example, several US laws relevant to jamming and spoofing of civil aviation GNSS applications were enacted to satisfy obligations under the Montreal Convention.
Adherence to performance standards adopted by the IMO Maritime Committee is to be ensured by the flag State exercising jurisdiction and control over the vessel in question through the application of its national laws.
National laws regulating market access and/or the use of jamming and spoofing devices are eminent examples for the implementation of international obligations of a State in relation to the prevention and mitigation of disruptions of GNSS signals and services. Though approaches differ in detail, most jurisdictions make placing jamming and spoofing

devices on the market and/or using jamming and spoofing devices subject to an administrative, or even criminal offence.
US authorities have taken major enforcement action by in response to placing jamming devices on the market and the use of such devices.[15]

4. Summary and Conclusions

Jamming and spoofing of GNSS signals are serious threats to critical infrastructures and a broad range of economic activities and public services. Together with the dependencies on GNSS, vulnerabilities are growing.
Remedies under international and national law range from preventive measures, to mitigation measures, to measures in response to jamming and spoofing of GNSS signals.
The ITU legal framework protects the radio frequencies used of radionavigation-satellite services against harmful interference and prohibits the transmission of signals without identifications. While States are obliged to eliminate harmful interference through jamming and spoofing of GNSS signals, the ITU however lacks effective enforcement measures.
The ICAO legal framework provides for elaborate standards and recommended practices on the use of GNSS in international aviation, as well as guidance material requiring States to implement appropriate preventive and mitigation measures in response to jamming and spoofing of GNSS signals. Under the Montreal Convention, States shall make jamming and spoofing of GNSS signals punishable.
As with ICAO for air navigation, IMO has developed performance standards on the use of GNSS in maritime navigation. These standards serve as important tools to prevent, detect, and mitigate the effects of jamming and spoofing of GNSS signals.
The ITU legal framework, the ICAO legal framework, as well as the IMO legal framework require appropriate implementation at national level, through national laws on the import, sale, and use of jamming and spoofing devices in general, and through national laws applicable to telecommunications, air navigation, and maritime navigation.
The application of the laws on the prevention of war strongly depends on the concrete effects of the jamming and spoofing of GNSS signals in the individual case. In this regard, the effects of jamming and spoofing should not be overestimated. As with the use of conventional weapons, only activities with most severe impacts may qualify as armed attacks conferring the right to self-defence. Nor are such activities necessarily a threat to the peace, breach of the peace, or act of aggression potentially giving rise to

15 An overview on these enforcement actions is available under https://www.gps.gov/spectrum/jamming/ (accessed 14.01.2021).

collective action authorized by the UN Security Council. Below the level of an armed attack or a threat to the peace, breach of the peace, or act of aggression, jamming and spoofing of GNSS signals may however be qualified as threat or use of force or as the breach of any other international obligation. In such case, the State affected may take countermeasures within the limits of proportionality.

Overall, remedies under international law are limited, to the extent that their scope is limited to States and that it requires appropriate implementation at national level to prevent or counter jamming and spoofing undertaken by individuals or other non-State actors. Remedies under national law are in turn limited, to the extent that they are not applicable to State action. Due to these limitations, an interplay between international and national law is required to cope with the threats caused by jamming and spoofing of GNSS signals.

In practice, attribution of jamming and spoofing to a given State may be difficult and enforcement measures against States are often limited in effect. Therefore, preventive and mitigation measures such as performance standards requiring fall-back options in case of disruptions of GNSS signals, methods to detect jamming and spoofing, or procedures on notices to stakeholders concerned by a disruption are of particular importance.