Journal on Baltic Security, 2023; 9(1): 69-97

Research Article

Open Access
https://doi.org/10.57767/jobs_2023_003

Tegg Westbrook *

Radiofrequency Interference Strategies Targeting Marine Navigation Systems: Political Motives and Consequences

Received: 22 February 2023
Accepted: 18 May 2023

Abstract: Maritime traffic from the Baltic Sea and Black Sea to the Strait of Hormuz has experienced frequent and prolonged instances of radiofrequency interference which has been attributed to military exercises, anti-drone defence, and political motives. Whilst the technical vulnerabilities to maritime systems have been identified, academia has yet to contextualise those vulnerabilities when considering ongoing geopolitical tensions notably between Russia, Iran, and 'the West'. The findings of this research indicate that spoofing vessels can complement five main strategies: (1) making navies appear more provocative than they are; (2) revealing security vulnerabilities; (3) hostage diplomacy; (4) evading sanctions; and (5) reconnaissance and sabotage. It concludes with a discussion of future scenarios and provides suggestions for countermeasures.

Keywords: Maritime Security, Electronic Warfare, Information Warfare, Jamming, Spoofing.

* **Corresponding author:** Tegg Westbrook, Ph.D, e-mail: tegg.westbrook@uis.no. University of Stavanger, Faculty of Science and Technology, Department of Safety, Economics, and Planning.

Introduction

The opening scenes of the 1997 James Bond film *Tomorrow Never Dies* shows terrorists in a stealth ship coercing a British Navy Destroyer into Chinese territorial waters, prompting a response from the Chinese Air Force. The waterborne assailants – collaborating with a corrupt global media organisation – then stage a fight between the two countries by sinking the British ship, shooting all survivors in the water, and shooting down a Chinese response plane. The front-page newspapers the next day are suspiciously detailed about the story. War seems inevitable. The narrative thereafter (avoiding spoilers) involves Bond searching for a spoofing device with the aid of dalliances, punches, kicks, and high-tech gadgets.

While such fictional references are entertaining, instances of strategic, politically motivated Global Navigation Satellite System (GNSS) interference have been reported worldwide in the maritime domain. This interference can result in lost or inaccurate GNSS signals affecting bridge navigation, GNSS-based timing, and communications equipment (U.S. Department of Transportation Maritime Administration, 2022). It has also, evidently, led to serious diplomatic disputes that have directly impacted the delicate fabric of international security.

GNSS is vulnerable to jamming and spoofing from both military and civilian users. Jamming degrades the reliable use of GNSS data, while spoofing creates inaccurate position and velocity readings that poses a serious hazard for marine navigation. When used tactically, spoofing, to an end, can enable the attacker to achieve certain strategic ends that could (re)balance otherwise imbalanced political dynamics between adversaries. This tactical use of radiofrequency interference (RFI), much of which happens in politically precarious waters, requires further insight and contextualisation.

It is vitally important to consider the political motives behind RFI strategies and their respective consequences not only for maritime security and awareness but its potential impacts on global stability more broadly. The aim of this research is to explore the motives behind and consequences resulting

from strategic interference of marine navigation systems. It considers the future implications of such actions and proposes some countermeasures.

At this time of great global instability, the main challenge posed due to RFI is the misdirection of civilian and military users of GNSS for political gains. This could create potential escalation in tit-for-tat confrontations, particularly considering sanctions against and seizures of Russian and Iranian assets. Taking inspiration from a taxonomy of jamming and spoofing tactics (Westbrook, 2023, in press), the article explores how RFI strategies could be exploited in the pursuit of elevating political tensions. Based on previous analyses of the jamming and spoofing of marine systems, the article draws on 'choke points,' namely the Baltic Sea, the Black Sea, and the Strait of Hormuz. It finds that the most likely RFI strategies by Russia or Iran will be to make navies appear more provocative than they are, to reveal security vulnerabilities, for hostage diplomacy (with either military personnel or assets), to evade sanctions, and to enable sabotage and reconnaissance of critical infrastructure.

Hereafter, the article is structured as follows. It first provides an overview of the technical vulnerabilities of marine vessels, as well as the geopolitical factors that put safe navigation at sea at risk. It then explores what, based on those technical vulnerabilities, cyber-physical manifestations may result due to those interferences based on known or suspected instances of cyber or electronic intrusions. Thereafter, it postulates about future implications, focusing on the interface between GNSS and geopolitics, and explores several conventional countermeasures.

The methodology of this study involves a literature review situating EW activities worldwide and how they have affected military and civilian use of GNSS. The data was coded into themes relating to the possible means and ends objectives of the likely threat actors. The themes were based on a taxonomy of spoofing and jamming tactics and motives, which includes 11 tactics and 8 motives (Westbrook, 2023). The limitations of the taxonomy is that it investigates non-state actors, not state militaries. The tactical use of RFI

was thus contextualized based on the political rivalries between the suspected attacker – most of which are state militaries – and the stated victim. Further expansion of the real, hypothetical, and future implications added richness to the data.

Background

For this study, Russia and Iran have been identified as the most likely actors to use RFI to achieve certain political ends. One main concern about RFI is the potential that actors could spoof vessels into Russian or Iranian waters in real terms but also via pilot's and observer's digital interfaces (Westbrook, 2023a, under peer review), complementing narratives of NATO intrusion and 'Western aggression.' Russia, for example, has consistently used alternative media narratives to justify its unprovoked invasion of Ukraine. These narratives are targeted towards its own population and populations of sympathetic states (Westbrook, 2023a, under peer review). RFI strategies are thus part and parcel with online-to-online, cyber-enabled information warfare, which requires a much wider analysis and contextualisation.

The Automatic Identification Systems (AIS) is used for tracking vessels and transmits a coded message to satellites and land-based receivers. AIS provides information about the vessel's identity such as its name, ship type, size, and call sign (Cutlip, 2016). The codes are open, unencrypted, and unprotected radio systems intended to operate on non-secure VHF-FM channels. As such, AIS signals can be spoofed, resulting in incorrect or missing AIS data (U.S. Department of Transportation Maritime Administration, 2022; Cutlip, 2016).

AIS lacks any authentication or encryption and is considered simple software to manipulate (Simonite, 2013). Existing research highlights the technical vulnerabilities of AIS (Katsilieris et al, 2013; Cutlip, 2016; Kontopoulos et al, 2018; Medina et al, 2019; Andrej et al, 2021). Among the findings, research has found, for example, that it is possible to cause fake vessels to appear on AIS, real ones to disappear, and issue false emergency alerts with cheap spoofing equipment (Simonite, 2013). Using AIS, nefarious actors can not only locate the whereabouts of hundreds of thousands of vessels, lighthouses, buoys and other marine features at any given time, but with this information

they can, as researchers have found, 'stage spoof emergencies' such as collision warnings and place false vehicles, boundaries, and hazardous features in the paths of other vehicles, influencing hazardous decision-making, leading to situations that are sometimes favourable to the attacker. It could, for example, influence a vessel to enter borders, providing a pretext for seizure.

It is not only AIS that is vulnerable. There are many digital systems that are vulnerable to other cyber-attacks such as ransomware. However, the satellites that are connected to the satellite links are also connected with other navigation systems onboard, meaning that jamming could cause almost a total denial of service (DoS). Indeed, interference with weak signals will not only leave position data inaccurate, but it will also likely compromise Chart Display systems, as well as GPS receivers, GPS compasses, gyrocompasses, steering systems, radar/ARPAs, echo sounders, and DSC VHF radios unless a secondary positioning source is immediately available which is unaffected (Moskoff, 2014).

Other studies have focussed on the consequences of injecting false data into velocity readings through both jamming and spoofing. Indeed, The University of Nottingham and Royal Norwegian Naval Academy found in their research that momentary jamming of vessels for up to ten seconds could lead to dangerous situations, especially in narrow straits. The researchers found that the Global Positioning System (GPS) receiver 'gave false readings in the on-board navigation system with positional data moving more than 10 metres' (University of Nottingham, 2016). Similar results were also found in 2009, when the UK's Ministry of Defence 'conducted trials of GPS jamming against the THV Galatea, a buoy tender, in an area of sea near South Shields in the north of England' (Espiner, 2012). The worrying conclusion here was that the autopilot function followed the miscalculated location readings. During the trial where the vessel was jammed, it "gradually lost position, and the autopilot told the ship to move off course" (*Ibid.*).

One of the most prominent demonstrations of spoofing was when a team from the University of Texas at Austin demonstrated that they could coerce a multimillion dollar, 213-foot yacht off its course with a ready-assembled spoofing device (University of Texas News, 2013). The spoofing induced a location discrepancy on the ship's navigation system, and "the crew initiated a course correction". It was explained that "each course correction was setting the ship slightly off its course line", and ultimately, the yacht was following a track hundreds of metres from its intended route (*Ibid.*).

Huge deviations can theoretically happen in vast oceans and in poor weather conditions. It has been hypothesised that only a small deviation will see a vessel travelling from Madagascar on route to the Malacca Straits ending up 220 nautical miles away, offshore, a sparsely populated, 'lightly governed' part of Indonesia (Goward, 2017). A spoofer could divert a 'ship's course slightly more than five degrees' and encourage a 'speed increase of two knots' (*Ibid.*). After the University of Texas at Austin's tests, it was also hypothesised that a vessel travelling in the relative safety of the Mediterranean could easily find itself in Libyan waters this way. Another objective of the attacker(s) might be to run the vessel aground in shallow waters or hit rocky shoals.

Such studies are important with respect to global security and the global economy at large. The maritime freight sector accounts for most of all freight in the world. Specific locations where political tensions are high, such as the Strait of Hormuz, some 1,250 vessels, including up to 600 tankers and 20 million barrels a day of crude and petroleum, transit monthly. Any interference in this area that degrades maritime navigation could have a spill-over effect in global markets (Bockmann, 2019). Similarly, it is conceived that up to and beyond one-sixth of the world's cargo traffic passes through the Baltic Sea (Baltic Lines, 2016).

RFI can thus have significant effects in localised areas that can be felt globally. Vessels that are "unnecessarily idling at sea" could cost companies "millions in extra fuel and operational expenses" (Lo, 2019), as well as delayed shipments, as in the case of the *Ever Given* debacle (BBC News, 2021). Research has found that jamming from nearby cliffs could seriously affect shipping traffic, causing "…the maritime equivalent of a motorway pile-up"

(University of Nottingham, 2016). In 2016, hundreds of fishing vessels in South Korea returned early to port after GPS signals were jammed by North Korea, which denied responsibility (Saul, 2017). The UK Government research concluded that a five-day loss of GNSS would cost its maritime economy over a billion pounds in 2017 (Sadlier, Flytkjær, Sabri, and Herr, 2017).

The maritime sector is particularly vulnerable because whilst, comparatively, most airliners have backup systems and pilot training to deal with such scenarios, not all vessels have these protections in place. In many of the world's oceans "navigational errors account for half of accidents" (University of Nottingham, 2016). The scalability of the threat against vessels may increase, as the number of vessels in 'the high seas has quadrupled over the past 25 years' (Woody, 2017). Hundreds of reports (predominantly) from the United States indicate frequent interferences around the world, with no explanation, including no recorded space weather and authorised military jamming tests (United States Coast Guard, no date). Intentional or collateral interference are likely to be reasons for some of these events.

Geopolitical Tensions: The GNSS factor

Tensions between the West and Russia need no expansion here. As a result of Russia's invasion of Ukraine, Western states have imposed numerous sanctions, including the seizure of luxury yachts from Russian oligarchs and the banning of most Russian vessels from EU, Norwegian, and UK ports (Safety4Sea, 2022; Regjeringen, 2022; U.K. Government, 2022). The Baltic Sea is an area where tensions have especially risen, where Nord Stream pipelines from Russia to Europe has been a point of heated tension (Burgess, 2022).

These tensions follow continuous radio interferences in the Black Sea during NATO exercises (C4ADS, 2019). Other recorded instances have been identified in Suez Canal, Cyprus, Malta, and Istanbul, in the Persian Gulf near Dammam, and off the coast of Brazil (although all have not been attributed

to Russian interference) (U.S. Department of Transportation Maritime Administration, 2022). The motivations for Russian RFI in the Baltic area, the Black Sea, and the Mediterranean has been documented before (Westbrook, 2019; C4ADS, 2019; Goward, 2016; Goward, 2017; Goward, 2019; Goward, 2021). Some events have not intentionally targeted maritime navigation systems but affected them without discrimination. Indeed, since 2016, DoS spoofing has been used to conceal the true locations of key Russian officials and Russian military units, which has affected all constellations (even Russia's own GLONASS). In 2019 alone, there were up to 10,000 jamming and spoofing events, some of which were within Russian territory but affected marine systems beyond their borders (Strategy Page, 2019). AIS spoofing, electronic interference, and cyber-attacks in the mined Black Sea (expanded later) is considered highly likely during the ongoing Russian invasion of Ukraine (MaritimeLink, 2022).

Drawing on cyber events in the past, Russia, Iranian, or North Korean EW units may use jamming or spoofing in a variety of ways to coerce governments, bypass sanctions, and intimidate populations. As 'force multipliers', the tactics, targets, and broader objectives depend on factors such as the *political dynamics*, particularly hastened under stringent time pressures i.e., where a creative, if not dubious, solution might be warranted to gain leverage in otherwise imbalanced and time-sensitive negotiations. The *target* may also be selected based on a tit-for-tat motive if, for example, nuclear negotiations in Iran are tainted, or there are further sanctions or seizure of Russian assets. Furthermore, the targets' *countermeasures* and the attackers' *capabilities* are also factors considered in the likelihood of attacker success (Westbrook, 2023a, under peer review).

We have explored the technical vulnerabilities, some geopolitical tensions relating to the radio spectrum, and drawn on how RFI indirectly interferes with marine navigation systems. Hereafter we thematise several intentional and tactical political and criminal motives behind spoofing and jamming, and later we consider future implications in this domain.

Findings

Hostage Diplomacy (The Incarceration of Military Personnel)

On the afternoon of 12 January 2016, the day of President Barack Obama's State of Union Speech, two US Navy patrol boats were on a routine transit from Kuwait to Bahrain. They were 'scheduled to rendezvous with the U.S. Coast Guard Cutter Monomoy for refueling' later that evening. According to available details, the rendezvous never took place (Lyons, 2016). The two boats apparently went 50 miles off route. It was speculated that either Iran spoofed the US sailors into Iranian territory or based on the official US account, the sailors "made a navigational error that mistakenly took them into Iranian territorial waters" to Farsi Island, a naval base of the Iranian Revolutionary Guards Corps (Greenwald, 2016). One media outlet and indeed some politicians have argued that the official explanation seemed implausible, and that Iran, having recently backtracked its nuclear programme following Western pressure (in exchange for lifting Western sanctions), had the motive to get back at the United States in some way (Goward, 2016). Whether the boats experienced 'mechanical failure' and drifted into Iranian waters (Greenwald, 2016), the timing of the nuclear agreement, and Obama's address, is interesting.

Adding to this, the Iranians reportedly confiscated the boat's GPS navigation equipment before the sailors were released 24 hours later (Goward, 2016). They also removed the chips in the sailor's satellite phones. On the contrary, according to one source, it seemed unlikely the crew "misnavigated" because typically small navy vessels like those used by the US Navy "have multiple and redundant systems, and usually travel in pairs or small groups specifically to avoid having a single point of failure threaten their mission" (*Ibid.*).

There are many scenarios within which the US sailors could have been spoofed to believe that they were in a different location. The sailors could have been using the easier-to-spoof civilian GPS system, as is sometimes the tendency when using not-very-user-friendly military navigation systems (Lee,

2018). Other explanations from news outlets speculate that a sailor put in the wrong GPS coordinates, that the crew tried to take a shortcut through Iranian waters, and on top of this, that the crew lost radio contact and thus could not seek help (Greenwald, 2016). Fundamentally, beyond the motive to 'humiliate' the United States (as one Iranian commander stated without restraint (Tasmin News Agency, 2016)), the seizure of other military patrols on the pretext of territorial infringement is a common feature of Iranian maritime behaviour.

Indeed, the 2004 seizure of three Royal Navy patrol boats and eight personnel was on the pretext that the boat stayed from the Iraqi side of the Shatt al-Arab waterway into Iranian side during bad weather. After reportedly experiencing mock executions and being forced to give 'confessions' on international media channels, the British personnel were released three days later. The UK's official account is that the Naval boats never strayed into Iranian territory and that Iran twice changed its account of where the sailors were detained. Similarly, in March 2007, the Navy of the Iranian Revolutionary Guards detained fifteen Royal Navy personnel (again paraded and forced to give 'confessions' on international media) from the HMS Cornwall on similar pretexts in 'disputed waters'. After considerable international pressure, the personnel were released, but navigational equipment was not returned (Durham University (2007).

Hostage Diplomacy (with assets)

During the Persian Gulf Crisis between 2019-2020, the United States, under President Donald Trump's administration, were at logger heads with Iran over its military and proxy activities in the Middle East. Iran was accused of funding and aiding Hezbollah and Houthi rebels who attacked the US Embassy in Baghdad and a Saudi oil facility (among other targets). They were also accused of killing a US contractor, of attacking merchant shipping in the Persian Gulf, and of shooting down an US surveillance drone flying over the Strait of Hormuz. The United States, in response, withdrew from the so-called Iran nuclear deal, imposed sanctions, designated the IRCG as a terrorist organisation, increased its military presence in the Middle East, conducted airstrikes against Hezbollah's facilities in Iraq and Syria, and assassinated

Qasem Soleimani, commander of IRGC's Quds Force, as well as Popular Mobilisation Forces (PMF) commander Abu Mahdi al-Muhandis, via drone strikes. All the while, a small group of countries, including the United States, the United Kingdom, and Saudi Arabia, formed the International Maritime Security Construct, tasked with maintaining order in Iran's maritime areas of interest. This was in response to Iran's reputed, and successful, attempts to bomb and seize merchant shipping operating in the area, and spoofing vessels operating in the rocky, busy, and at times, precariously narrow Persian Gulf.

During the Crisis, Iran seized the British-owned cargo ship *Stena Impero* following the latter's seizure of Iranian-owned oil tanker *Grace 1* in Gibraltar, which was believed to be supplying Bashar al-Assad's government in Syria. Emerging evidence indicated that the seizure was enabled by spoofing the ship into Iranian waters (Hughes and Selby, 2019). The purpose was to leverage concessions by the British authorities, including the release of *Grace I*. A similar seizure of the South Korean oil tanker *Hankuk Chemi* bears similar hallmarks of using spoofing to complement hostage diplomacy (Dudley, 2021). This was in response to the Seoul's freezing of $7 billion worth of Iranian assets in South Korean banks in response to US sanctions (ibid.). Further seizures of two Greek oil tankers during another tense period in Iran's nuclear negotiations, which had their transceivers turned off, shows that GPS, and its degradation, plays a huge part in geopolitics at sea.

Regarding the *Stena Impero*, one account described how the crew had to constantly "repair the route of the ship and that is what usually happens when you're being slowly spoofed away. The ship is showing it's straying off course, and you are constantly correcting the course, and that's when you physically move the ship off course" (Roi Mit in Bockmann, 2019). Indeed, AIS sources show that the *Stena Impero* undertook a sudden 120 degrees (approx.) starboard turn whilst passing through the Strait of Hormuz. This happened within a similar 45-minute window when another British-flagged oil vessel, the *Mesdar*, too, took a sharp turn towards Iranian waters and seized (but was later released). It is unclear where exactly the vessels were seized, but some media

sources, based on British claims, show the *Stena Impero* being seized in Omani waters (BBC News, 2022). It is unclear, however, whether the 120-degree turn was prior to, or after, Iran's seizure, based on available AIS data and published chronologies of the events. In the end, the capture was used to add pressure on the British government to release *Grace 1*, which it subsequently acquiesced to after weeks of negotiated stalemate.

Sanctions Evasion (as well as Environmental Crime and Migration)

Spoofing-assisted crime is frequently seen in the oceans and is getting more sophisticated. Spoofing can be used for waste discharge, to avert sanctions, or avert responsibility from other environmental damages. For example, EU fishing vessels have reportedly spoofed their locations to avoid new EU fishing regulations and profit accordingly (Commission Regulation EC No 2244/2003) (Ungerleider, 2014). Spoofing can also be done to avert criminal investigations with falsified GPS data.

Iran has consistently been accused of jamming and spoofing in the Strait of Hormuz (Cozzens, 2019; Pickrell, 2022). US officials have accused the Iranian Navy and the Iranian Revolutionary Guard Corps (IRGC) of spoofing merchant ship's AIS 'to make themselves look like commercial shipping vessels' to avoid sanctions, as well as claiming to be US or coalition warships (U.S. Department of Transportation, Maritime Administration, 2019; Browne and Starr, 2019).

Similar spoofing methods can enable vessels to engage in "smuggling and covert military uses" (Ungerleider, 2014). 'Aggressive GPS spoofing' which reportedly has been impacting shipping in over 20 Chinese coastal sites during 2019, has raised some suspicions. According to one report, most of the recorded spoofing occurred in oil terminals, mostly near North Korea (Bergman, 2021). 'The timing of the spoofing, imposition of sanctions on purchase of Iranian oil by the United States, and observations by others of Iranian oil being received by China, suggests that some of the spoofing may be designed to help conceal these transactions' (Goward, 2019). Reportedly, according to one media outlet, Iran is using a combination of spoofing, 'flag

hopping' and other techniques to deliver materials to and from China, which is reportedly helping to 'bankroll its secret nuclear programme' (Ryan, 2021).

'Environmental criminals' hiding from the Chinese state have reportedly spoofed their ship's location to illegally steal sand from water banks, probably for the construction industry (Hoffmann, 2020). Reports of illegal metal scavenging of sunken warships may involve AIS spoofing (Booth, 2016). Authorities and other agencies usually cross-check suspicious activities with satellite imagery. Indeed, the turning off of AIS was (and still is) a contentious topic during the migrant crisis in Europe in 2015, where rescue boats, European Navies, and smugglers had many useful (and self-explanatory) reasons not to be spotted (Heller and Pezzani, 2019).

AIS spoofing has thus concealed the transactions of sanctioned materials worldwide, as well as concealed the exploitation of people and for drug smuggling. In the height of the global food crisis, exacerbated by poor global crop yields, Russian forces in occupied areas of Ukraine have been stealing grain, agricultural equipment, trucks, and fertiliser from Ukrainian farmers at scale. Some of the said equipment have GPS trackers fitted, and data has indicated that the stolen goods has found its way back into Russia (Beake, Korenyuk, and Reality Check team, 2022). Some of the vessels transporting the grain and equipment have reportedly turned off their AIS (Diakun, 2022).

Making Vessels Appear Provocative

Military vessels will routinely turn their AIS off, but there are instances of AIS spoofing from which neither the perpetrator nor their intentions are known. Prior to the HMS Defenders' voyage through Russian-controlled Ukrainian waters in 2021, which prompted an aggressive response from the Russian Airforce and Navy, amongst many speculations, prior to the voyage, the UK., US, Dutch, and Swedish Navy could have been spoofed by Russia or hackers (Goward, 2021). One source has also theorised that AIS spoofing could be weaponised by Russia "to make western navies appear more provocative than they really are. The results are "evidence" meant to embarrass the navies […]

and falsified data [can be used] to back up Russian claims of territorial violations at sea" (Mizokami, 2021). Reports of other suspicious AIS manipulations have been identified by SkyTruth and Global Fish Watch, including false sailboat races, military manoeuvres, and even US warships inside Russian territorial waters (Bergman, 2021).

Although it is normal that navy vessels transit through territorial waters of other states, there are many instances where the route or context is unlikely, sparking suspicions from observers. Among other less serious cases of AIS spoofing, SkyTruth and media outlets have identified 11 NATO and NATO allied warships near Kaliningrad, Murmansk, and in the Kerch Strait near Crimea between 2020 and 2021 (ibid.). It was noted that considerable care was taken into making some of the observed data falsification seem plausible, for example in 'locations where naval vessels would be expected to broadcast AIS.' Reversely, suspected false tracks of Russian warships entering Polish territorial waters in July 2021 has also been identified (ibid.).

Spoofing to Reveal Security Vulnerabilities

In extreme cases, it is possible that cyber interference has led to serious and unexplained incidents at sea. As in the case of the cargo vessel *ACX Crystal* colliding with the USS Fitzgerald, it is likely that the pilot set an automatic course direction. Having collided with the navy ship, the vessel corrected its path and continued its original route for 15 minutes before the crew realised what had happened and returned to the collision location (Lo, 2019). While there is no official account about what happened, such events demonstrated the ease by which a tampered autopilot, or a spoofer, could lead a ship into precarious situations.

The US Navy and US intelligence considered a cyberattack as reasons for a serious collision between Destroyer USS John S McCain – involved in Freedom of Navigation Operations in the South China Sea – and a 600-foot Liberian oil tanker. Seemingly, by coincidence, this happened only two months after the USS Fitzgerald collided with a crate ship in the Sea of Japan – another area disputed by North Korea and South Korea. These collisions left a total of 17 sailors dead. Human error was subsequently blamed for the McCain

collision, resulting in the relieving of its commander. Nevertheless, the results of military-on-military tests (testing electronic warfare capabilities), for example, could lead to a similar situation of civilian vessels being inadvertently affected.

Reconnaissance and Sabotage

Russia has reportedly sent military and spy vessels to offshore wind farms and communication cables located in the North Sea, near the United Kingdom, Belgium, and the Netherlands (The Maritime Executive, 2023; Corera, 2023). Some of these ships are disguised as civilian vessels. In the case of the Nord Stream pipeline explosion in the Baltic Sea on 26 September 2022, several commentators have argued that so-called 'dark ships' loitered around the area days before the explosion took place. It is suspected that the vessels involved had turned their AIS off. As is usually the practice, some vessels will spoof their AIS to another location to avert suspicion. Other potential areas of suspicious activities near undersea cables in the Shetland Islands and the Adriatic Sea (using AIS data) has been explored (Soldi et al, 2023).

Future Implications and Countermeasures

The overriding conclusion here is that a combination of poor environmental conditions, lack of governance, target attractability, attacker capability, combined with insufficient countermeasures, are factors heightening the risk of tactical spoofing-enabled exploitation. Regardless, the possibility of such events happening are, nevertheless, hard to predict. Conceivably, for intentional attacks, the ideal locations for some actors to deploy spoofing tactics will be where political tensions exists between national borders, at 'choke points', and in perilous waters where precise navigation combined with good weather are favourable, and/or where legal structures and enforcement is largely absent (e.g., in pirated waters, or near failed states or rogue states). Attackers can take advantage of poor security hygiene on board (Zorz, 2018) or in areas where established maritime rules are not completely followed.

Attacks can exploit certain opportunities relative to the location of vessels, including "vessel characteristics, crew manning, weather, proximity to land" and density of vessels in one area (Demchak, Patton, and Tangredi, 2017).

All told, several future implications can be understood from these themes. The Black Sea, the Straits of Hormuz, and the Baltic Sea could be described as favourable locations for tactical RFI because of their proximity to the likely threat actors. This is since Iran and Russia are incapacitated diplomatically, isolated globally, and rely on false narratives to justify their disregard for international norms. Ultimately, this increases the chances of seizures and sanctions evasions. Some consequences are immediate and tangible, others might arise over time, or indeed extend hostilities.

There are several immediate problems to be drawn. Following the Russian invasion, there have been many cases of floating mines in the Black Sea endangering civilian shipping (The Maritime Executive, 2023a). This, combined with frequent RFI events in this area (affecting not only navigation data, but communication between vessels), compounded by poor weather conditions, could cause serious issues. Emergency call outs to other vessels of dangers can be degraded by widescale, indiscriminate jamming. Disasters could furthermore lead to environmental damages. Other areas where World War Two mines are located, such as the Baltic Sea, are also prone to RFI from Russian units. In some areas of the Baltic Sea, large vessels are not able to navigate effectively (Burgess, 2022).

As for false narratives, if tensions escalate, spoofing can complement false flagging operations, or indeed enable the reconnaissance and sabotage of critical infrastructure. Indeed, many Russian citizens believe that the invasion of Ukraine is justified based on its government's narratives of NATO aggression, Ukrainian 'Nazis', and its apparent nuclear ambitions. False narratives legitimise Russian actions (based on Russian President Vladimir Putin's perceived historical grievances), potentially extending the length of the conflict, and reducing the chances of regime change. Sanctions evasions, too, undermines the work of both preventative and punitive diplomatic responses, which ultimately fuels the war, extends suffering, inflation, and economic hardships within and beyond Ukraine's borders.

In extreme cases, armed confrontations due to seizures, including the seizures of secret military technologies, are not beyond comprehension. Public figures, such as Dick Cheney and Donald Trump, have considered, or carried out, offensive actions in response to seizures and other provocations by Iran (Westbrook, 2019; Westbrook, 2023, in press). The risk of confrontations is heightened when opposing parties are pushed into corners, under pressure from their citizens to act, and are disadvantaged diplomatically. The degenerative practices of taking human hostages have also proven to be effective for prisoner swaps or for the release of sanctioned assets. Indeed, the practice of arbitrary detentions has experienced a comeback recently, leading to an international initiative: (the) Declaration Against Arbitrary Detention in State-to-State Relations (Government of Canada, 2023).

The question therefore is how to take necessary measures to reduce the risks. GPS receivers are 'naïve' to spoofing. Without countermeasures, they will accept fake signals thousands of times stronger than those from real satellites and "overlook certain abnormal, artificial characteristics of GPS signals generated by standard GPS satellite simulators" (Johnston and Warner, 2004). Since the 2000s, work on the detection of spoofing still has not solved all the problems because even if spoofing is detected, "it still won't be able to show you the actual position" (Todd Humphreys in: Lied, 2017) Some solutions, such as using "several antenna elements to create reception beams in different directions, nulling out the signals from the spoofer" works only if the attacker "is transmitting from only one or two locations" (ibid.). Relatively cheap, retrofitted software and hardware fixes, which include detecting suspect shifts in signal strengths, position shifts, the angle and direction of arrival of signals, time anomalies, and loss of lock notifications (Tippenhauer et al, 2011), are other countermeasures out there. Many of the present civilian GNSS receivers by 2010 were not equipped with such specialised measures (Wesson, Shepard, and Humphreys, 2012). Many of the proposed technical countermeasures were also largely aimed at unsophisticated attacks.

Other proposed anti-jam and anti-spoof methods include obscuring the antennas from public view to make it harder for the attacker to locate them. Other methods (among many others) include providing decoy antennas, 'blocking antennas', placing antennas in an area that ground-based signals cannot target them, or speeding up detection. Another is using receivers that receive signals from multiple constellations or from multiple frequencies. Some systems have been developed to switch frequencies every second. On the latter point, training programmes are proposed in some countries to help seafarers identify spoofing. In all detection methods, however, there are ways in which unsophisticated (but mostly sophisticated) attacks could evade them, and they are not measures that could be implemented overnight. Security threats remain understandably confidential and not eagerly shared. Furthermore, some of the mentioned systems can produce many false positives, which means that operators might ignore them or turn them off.

Fundamentally, many of the countermeasures proposed are not intended to stop spoofing and jamming attacks, but they decrease the odds that a spoofing attack and its intended consequences could succeed (Warner and Johnston, 2002). Using multiple countermeasures alongside back-up navigation systems also in itself acts as a deterrent. However still, whilst anti-spoofing measures might pick up attacks it has yet to "…progress to the point where not only can we tell it's a false signal, but we can also say, 'Here is the true signal; here is the true position'" (Cameron, 2014). The question is whether countermeasures will lead to more innovations that enable attackers to exploit weaknesses. If, for example, countermeasures can pick up obvious discrepancies in information, will there be a turn towards making subtle, hard-to-identify discrepancies that cannot be identified? Artificial intelligence may be able to pick up subtle discrepancies and suspicious AIS tracks in real-time which will be invaluable for seafarers and observers alike.

There are also numerous measures to ensure more assured position, navigation, and timing information from other sources. Multifrequency antennae is one possible solution. As for ground-based solutions, the governments of South Korea, China, Saudi Arabia, Iran, and the United Kingdom have invested in upgrading their existing LORAN-type systems

(LOng RAnge Navigation signals emitted from ground-based towers) to more, enhanced "eLORAN" systems with stronger signals. eLORAN uses long-wave signals from fixed positions on land to aid navigation at sea (McCaney, 2013) (the Russian have their own named eChayka). The 'unjammable' high power signals are 1.3 million times more powerful than GPS signals (Inside GNSS, 2013).

Conclusion

The article has established, based on historic accounts, that the likely motivations for intentional RFI is to enable hostage diplomacy, to test adversaries' systems in peacetime, for sanctions evasion, and for reconnaissance and sabotage. From a broader geopolitical perspective, it is clear that jamming and spoofing could escalate tensions between states as a result of misinterpretation or miscalculations of intentions (Westbrook, 2023a, under review). Evidently, spoofing – the turning of lies into truths – can complement alternative news and feed false narratives, something that Iran may have done over recent years to marine systems with falsified location data. This form of 'sub-threshold warfare', operating in a grey zone below the threshold of war without direct conflict, is now part and parcel with modern digital life.

There is a clear interface between geopolitics and the GNSS. Focus on the activities of malign actors in the electromagnetic (as opposed to the cyber) domain reveals equal if not more serious implications for international security, and this is not limited to marine navigations systems. The exploitation of navigation systems in aviation, for example, brings about different understandings of actors, their stated or unstated intentions, and possible consequences for civilian users. As for marine systems, focusing on Russia and Iran is necessary at this time of global tension. References to RFI in China's and North Korea's spheres of interest, though evident, has received limited overview. As some examples in this article demonstrate, the focus on choke points is also limiting. The geographical proximities of RFI are not static;

portable and concealable RFI devices can be smuggled on board vessels, or be directed from other aerial and surface vehicles. Finally, technology in the form of countermeasures is not an antidote to this problem. Awareness and training are also vitally important, as well as reliable access to secure satellite signals.

Bibliography

Andrej, Androjna, Perkovič, Marko, Pavic, Ivica and Mišković, Jakša. (2021) 'AIS Data Vulnerability Indicated by a Spoofing Case-Study', *Applied Sciences* 11(11), 5015. Available at: https://doi.org/10.3390/app11115015.

Baltic Lines. (2016) 'Shipping in the Baltic Sea – Past, present and future developments relevant for Maritime Spatial Planning', *Project Report I*. [Online]. p.1 – 35. Available at: https://vasab.org/wp-content/uploads/2018/06/Baltic-LINes-Shipping_Report-20122016.pdf.

BBC News. (2021) 'Ever Given: Cargo ship returns through Suez Canal it blocked', [Online] 20 August. Available at: www.bbc.com/news/world-middle-east-58288512 (Accessed: 17 March, 2023).

BBC News. (2022) 'How it happened: Stena Impero's route through the Strait of Hormuz', [Online]. Image file available at: https://c.files.bbci.co.uk/7CCB/production/_107974913_stena_bulk_tanker_route_v1_640-nc.png (Accessed: 6 July 2022).

Beake, Nick, Korenyuk, Maria, and Reality Check team. (2022) 'Tracking where Russia is taking Ukraine's stolen grain', *BBC News*, [Online] 27 June 2020. Available at: www.bbc.com/news/61790625 (Accessed: 17 March 2023).

Bergman, Bjorn. (2021) 'Systematic data analysis reveals false vessel tracks', *SkyTruth,* [Online] July 29. Available at: https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/ (Accessed: 21 March 2023).

Blake, Tanya. (2017) 'Hackers took 'full control' of container ship's navigation systems for 10 hours', *Resilient Navigation and Timing Foundation*, [Online] November 22. Available at: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/ (Accessed: 21 March 2023).

Bockmann, Michelle Wiese. (2019) 'Seized UK tanker likely 'spoofed' by Iran', *Lloyd's List,* [Online] August 16. Available at:

https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran (Accessed: 17 March 2023).

Booth, Robert. (2016) 'Battle of Jutland war graves 'vandalised' by illegal metal scavengers', *The Guardian*, [Online] 18 September. Available at: www.theguardian.com/world/2016/sep/18/battle-jutland-war-graves-hms-warrior-metal-scavengers-royal-navy (Accessed: 25 April 2023).

Browne, Ryan and Starr, Barbara. (2019) 'US government warns of Iranian threats to commercial shipping, including GPS interference', *CNN News*, [Online] August 07. Available at: https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/ (Accessed: 17 March 2023).

Burgess, Matt. (2022) "Dark Ships' Emerge From the Shadows of the Nord Stream Mystery', *Wired*, [Online] 11 November. Available at: www.wired.co.uk/article/nord-stream-pipeline-explosion-dark-ships (Accessed: 17 March 2023).

C4ADS. (2019) Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. *University of Texas at Austin, Resilient Navigation and Timing Foundation*, pp. 1 – 66. [Online]. Available at: https://www.c4reports.org/aboveusonlystars (Accessed: 17 March 2023).

Cameron, Alan. (2014) 'Spoofer and Detector: Battle of the Titans at Sea', *GPS World* [Online]. 5 August 2014. Available at: www.gpsworld.com/spoofer-and-detector-battle-of-the-titans-at-sea/ (Accessed: 23 March 2023). Quoting Mark Psiaki.

Corera, Gordon. (2023) 'Ukraine war: The Russian ships accused of North Sea sabotage', *BBC News*, [Online] 19 April 2020. Available at: www.bbc.com/news/world-europe-65309687 (Accessed 25 April 2023).

Cozzens, Tracy. (2019) 'Iran jams GPS on ships in Strait of Hormuz', *GPS World*, [Online] 09 August 2019. Available at: www.gpsworld.com/iran-jams-gps-on-ships-in-strait-of-hormuz/ (Accessed: 17 March 2023).

Cutlip, Kimbra. (2016) 'Spoofing: One Identity Shared by Multiple Vessels', *Global Fish Watch*, July 25. Available at: https://globalfishingwatch.org/data/spoofing-one-identity-shared-by-multiple-vessels/ (Accessed: 21 March 2023).

Demchak, Chris, Patton, Keith, and Tangredi, Sam J. (2017) 'Why Are Our Ships Crashing? Competence, Overload, and Cyber Considerations', *Center for International Maritime Security*, [Online] 25 August 2017. Available at: https://cimsec.org/ships-crashing-competence-overload-cyber-considerations/ (Accessed: 21 March 2023).

Diakun, Bridget. (2022) 'Russia accused of shipping stolen Ukrainian grain via Crimea', *Lloyd's List*, [Online] 21 June 2022. Available at: https://lloydslist.maritimeintelligence.informa.com/LL1141291/Russia-accused-of-shipping-stolen-Ukrainian-grain-via-Crimea (Accessed: 17 March 2023).

Dudley, Dominic. (2021) 'South Korea Agrees To Unfreeze $1 Billion In Iranian Assets, Following Tanker Seizure By Tehran', *Forbes*, [Online] 24 February 2021. Available at: https://www.forbes.com/sites/dominicdudley/2021/02/24/south-korea-agrees-to-unfreeze-1-billion-in-iranian-assets-following-tanker-seizure-by-tehran/?sh=66ea285c1386 (Accessed 17 March 2023).

Durham University. (2007) 'Notes on the Iran-Iraq maritime boundary', *Centre for Borders Research*, [Online] circa 2 April 2007. Available at: www.dur.ac.uk/ibru/resources/iran-iraq/ (Accessed: 21 March 2023).

Espiner, Tom. (2012) 'UK Sentinel study reveals GPS jammer use', *ZDNET*, February 22. Available at: www.zdnet.com/article/uk-sentinel-study-reveals-gps-jammer-use/, citing the words of Professor David Last, speaking at "GNSS Vulnerability: Present Dangers, Future Threats 2012" conference, [Online] https://www.nottingham.ac.uk/grace/events/eventsarticles/gnss-vulnerability-present-dangers,-future-threats-2012.aspx (All accessed: 21 March 2023).

Government of Canada. (2023) 'Initiative against arbitrary detention in state-to-state relations', [Online] 18 April 2023. Available at: www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/arbitrary_detention-detention_arbitraire.aspx?lang=eng (Accessed: 25 April 2023).

Goward, Dana. (2016) 'Opinion: Were US sailors 'spoofed' into Iranian waters?' *Christian Science Monitor*, [Online] 15 January 2016. Available at: www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0115/Opinion-Were-US-sailors-spoofed-into-Iranian-waters (Accessed: 21 March 2023).

Goward, Dana. (2017) 'How to Steal a Ship', *The Maritime Executive*, [Online] 6 February 2017. Available at: www.maritime-executive.com/editorials/how-to-steal-a-ship (Accessed: 21 March 2023).

Goward, Dana. (2019) 'Patterns of GPS Spoofing at Chinese Ports', *The Maritime Executive,* [Online] 12 December 2019. Available at: www.maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports (Accessed: 21 March 2023).

Goward, Dana. (2021) 'Who "Moved" the Position of a U.S. Navy Ship From Odessa to Crimea?' *The Maritime Executive*, [Online] 6 July 2021. Available at: www.maritime-

executive.com/editorials/who-moved-the-position-of-a-u-s-navy-ship-from-odessa-to-crimea (Accessed: 21 March, 2023).

Greenwald, Glenn. (2016) 'U.S. Radically Changes Its Story of the Boats in Iranian Waters: to an Even More Suspicious Version', *The Intercept,* [Online] 15 January 2016. Available at: theintercept.com/2016/01/15/the-u-s-radically-changes-its-story-of-the-boats-in-iranian-waters-to-an-even-more-suspicious-version/ (Accessed: 21 March 2023).

Heller, Charles, and Pezzani, Lorenzo. (2019) 'AIS Politics: The Contested Use of Vessel Tracking at the EU's Maritime Frontier', *Science, Technology, & Human Values* 44 (5). pp. 881-899. [Online] Available at: https://doi.org/10.1177/0162243919852672.

Hoffmann, Michael. (2020) Roving bandits and looted coastlines: How the global appetite for sand is fuelling a crisis, *The Conversation*, [Online] 3 May 2020. Available at: https://theconversation.com/roving-bandits-and-looted-coastlines-how-the-global-appetite-for-sand-is-fuelling-a-crisis-132412 (Accessed: 21 March, 2023).

Hughes, Chris and Selby, Alan. (2019) 'Iran tanker crisis: MI6 probe link to Putin after British ship is seized', *The Mirror,* [Online] 20 July 2019. Available at: www.mirror.co.uk/news/world-news/iran-tanker-crisis-mi6-probe-18458279 (Accessed 17 March, 2023).

IHS Markit. (2017?) 'Navigating Maritime Risks in a sea of New and Emerging Challenges: An Insurers' Perspective', [Online]. Available at: https://ihsmarkit.com/events/navigating-maritime-risks-in-a-sea-of-new-and-emerging-risks-an-insurers-perspective/overview.html (Accessed: 6 July 2022).

Inside GNSS. (2013) 'New Foundation Formed to Pursue eLoran as Backup for GPS', [Online] 7 November 2013. Available at: https://insidegnss.com/new-foundation-formed-to-pursue-eloran-as-backup-for-gps/ (Accessed: 23 March 2023).

Johnston Roger G., and Warner, Jon S. (2004) Think GPS Cargo Tracking = High Security? Think Again. *Business Contingency Planning Conference, Las Vegas, NV,* (May 23-27), p.4.

Katsilieris, Fotios, Braca, Paolo, Coraluppi, Stefano. (2013) 'Detection of malicious AIS position spoofing by exploiting radar information', *Proceedings of the 16th International Conference on Information Fusion*, Istanbul, Turkey, pp. 1196-1203.

Kontopoulos, Ioannis, Spiliopoulos, Giannis, Zissis, Dimitrios, Chatzikokolakis, Konstantinos, Artikis, Alexander. (2018) 'Countering Real-Time Stream Poisoning: An Architecture for Detecting Vessel Spoofing in Streams of AIS

Data,' *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing*, *16th International Conference on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*. Athens, Greece, pp. 981-986. Available at: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00139.

Lee, Connie. (2018) 'Spoofing Risks Prompt Military to Update GPS Devices', *National Defense*, [Online] 1 April 2018. Available at: https://www.nationaldefensemagazine.org/articles/2018/1/4/spoofing-risks-prompt-military-to-update-gps-devices (Accessed: 21 March 2023).

Lied, Henrik. (2017) 'GPS freaking out? Maybe you're too close to Putin', *NRK*, September 18. Available at: https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/ (Accessed: 21 March 2023). Quoting Todd Humphreys.

Lo, Chris. (2019) 'GPS spoofing: what's the risk for ship navigation?' *Ship Technology*, [Online] 15 April 2019. Available at: www.ship-technology.com/features/ship-navigation-risks/ (Accessed: 17 March 2023).

Lyons, James. (2016) 'Seagoing coincidence?' *The Washington Times*, [Online] 26 January 2016. Available at: www.washingtontimes.com/news/2016/jan/26/james-lyons-navys-iran-mishap-boosts-image-of-obam/ (Accessed: 21 March 2023).

MaritimeLink. (2022) 'From Mines to AIS Spoofing, Assessing the Risks to Shipping in the Black Sea', [Online] 3 March 2022. Available at: www.marinelink.com/news/mines-ais-spoofing-assessing-risks-494729 (Accessed: 17 March 2023).

McCaney, Kevin. (2013) 'Yacht hijacking shows the potential power of GPS spoofing', *GCN*, [Online] 1 August 2013. Available at: https://gcn.com/articles/2013/08/01/gps-spoofing.aspx (Accessed: 23 March 2023).

Medina, Daniel, Lass, Christoph, Marcos, Emilio Pérez, Ziebold, Ralf, Closas, Pau, García, Jesús. (2019) 'On GNSS Jamming Threat from the Maritime Navigation Perspective', *2019 22th International Conference on Information Fusion (FUSION)*, Ottawa, ON, Canada, pp. 1-7. Available at: 10.23919/FUSION43075.2019.9011348.

Mizokami, Kyle. (2021) 'Someone Is Faking the Positions of NATO Warships at Sea. It Reeks of Russia', *Popular Mechanics*, [Online] 10 August 2021. Available at: www.popularmechanics.com/military/navy-ships/a37261561/ais-ship-location-data-spoofed/ (Accessed: 21 March 2023).

Moskoff, Capt. David B. (2014) 'GPS jammers a top concern in maritime cyber readiness', *Professional Mariner*, [Online] 3 June 2014. Available at: www.professionalmariner.com/gps-jammers-a-top-concern-in-maritime-cyber-readiness/ (Accessed: 21 March 2023).

Pickrell, Ryan. (2022) 'Iran is reportedly jamming ship GPS navigation systems to get them to wander into Iranian waters', *Business Insider*, [Online] 8 August 2022. Available at: www.businessinsider.com/iran-is-jamming-ship-gps-navigation-systems-to-seize-them-2019-8?r=US&IR=T (Accessed: 17 March 2023).

Regjeringen. (2022) 'Fastsettelse av forskrift om endring i forskrift 15. august 2014 nr. 1076 om restriktive tiltak vedrørende handlinger som undergraver eller truer Ukrainas territorielle integritet, suverenitet, uavhengighet og stabilitet', Original title [Determination of regulations on changes to regulations 15 August 2014 No. 1076 on restrictive measures regarding actions that undermine or threaten Ukraine's territorial integrity, sovereignty, independence and stability'] [Online] 29 April 2022. Available at: www.regjeringen.no/no/dokumenter/kglres_sanksjoner2/id2910739/ (Accessed: 17 March 2023).

Ryan, Jake. (2021) 'Revealed: Iran's 'ghost armada' of 123 sanction-busting tankers is selling black market oil to China to bankroll its secret nuclear programme', *The Daily Mail*, [Online] 20 June 2021. Available at: www.dailymail.co.uk/news/article-9704151/Irans-ghost-armada-tankers-selling-black-market-oil-China-bankroll-nuclear-programme.html?ns_mchannel=rss&ns_campaign=1490&ito=1490 (Accessed: 21 March 2023).

Sadlier, Greg, Flytkjær, Rasmus, Sabri, Farooq, and Herr, Daniel. (2017) *The economic impact on the UK of a disruption to GNSS*, Innovate UK, UK Space Agency, and Royal Institute of Navigation. [Online]. Available at: https://londoneconomics.co.uk/wp-content/uploads/2017/10/LE-IUK-Economic-impact-to-UK-of-a-disruption-to-GNSS-FULLredacted-PUBLISH-S2C190517.pdf (Accessed: 17 March 2023).

Safety4Sea. (2022) 'Ban of Russian ships in EU ports: Everything you need to know', [Online] 27 May 2022. Available at: https://safety4sea.com/ban-of-russian-ships-in-eu-ports-everything-you-need-to-know/ (Accessed: 17 March 2023).

Saul, Jonathan. (2017) 'Cyber threats prompt return of radio for ship navigation', *Reuters,* [Online] 7 August 2017. Available at: www.reuters.com/article/us-shipping-

gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT (Accessed: 17 March 2023).

Simonite, Tom. (2013) 'Ship Tracking Hack Makes Tankers Vanish from View', *MIT Technology Review*, [Online] 18 October 2013. Available at: www.technologyreview.com/2013/10/18/82918/ship-tracking-hack-makes-tankers-vanish-from-view/ (Accessed: 21 March 2023).

Soldi, Giovanni, *et al.* (2023) 'Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies', *Electrical Engineering and Systems Science, Signal Processing*. Available at: arXiv:2302.01817.

Strategy Page (2019) 'Electronic Weapons: Russia Takes A Victory Lap', [Online] 3 November 2019. Available at: www.strategypage.com/htmw/htecm/articles/20191103.aspx (Accessed: 17 March 2023).

Tasmin News Agency. (2016) '"Extensive Information" Obtained from US Sailors Captured by IRGC', [Online] 1 February 2016, www.tasnimnews.com/en/news/2016/02/01/987723/extensive-information-obtained-from-us-sailors-captured-by-irgc (Accessed: 21 March 2023).

The Maritime Executive. (2023) 'EU Plans New Patrols and Efforts to Increase Maritime Security', [Online] 10 March 2023. Available at: https://maritime-executive.com/article/eu-plans-new-patrols-and-efforts-to-increase-maritime-security (Accessed 17 March 2023).

The Maritime Executive. (2023a) 'Bulgarian Navy Detonates Two Drifting Naval Mines in the Black Sea', [Online] 24 January 2023. Available at: https://maritime-executive.com/article/bulgarian-navy-detonates-two-drifting-naval-mines-in-the-black-sea.

Tippenhauer, Nils Ole, Pöpper, Christina, Rasmussen, Kasper B., Capkun, Srdjan. (2011) 'On the Requirements for Successful GPS Spoofing Attacks', *CCS '11: Proceedings of the 18th ACM conference on Computer and communications security*, Chicago Illinois USA (October 17 - 21), www.cs.ox.ac.uk/files/6489/gps.pdf.

Tom Jowitt. (2011) 'MoD Halts GPS Jamming After Safety Complaints', *Silicon*, [Online] 11 October 2011. Available at: www.silicon.co.uk/workspace/mod-halts-gps-jamming-after-safety-complaints-42074 (Accessed: 21 March 2023).

U.K. Government. (2022) 'UK introduces new sanctions against Russia including ban on ships and fresh financial measures', [Online] 1 March 2022. Available at: www.gov.uk/government/news/uk-introduces-new-sanctions-against-russia-including-ban-on-ships-and-fresh-financial-

measures#:~:text=Russian%20ships%20have%20been%20banned,powers%20to%20detain%20Russian%20vessels (Accessed: 17 March 2023).

U.S. Department of Transportation, Maritime Administration. (2019) *2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and its Proxies*, [Online] 7 August 2019. Available at: www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels.

U.S. Department of Transportation Maritime Administration. (2022) *2022-005-Various-GPS Interference & AIS Spoofing*. [Online]. Available at: https://maritime.dot.gov/msci/2022-005-various-gps-interference-ais-spoofing (Accessed: 17 March 2023).

Ungerleider, Neal. (2014) 'Spoofed Satellite Feeds Trouble Google's Global Fishing Watch', *Fast Company*, [Online] 20 November 2014. Available at: www.fastcompany.com/3038863/spoofed-satellite-feeds-trouble-googles-global-fishing-watch (Accessed: 21 March 2023).

United States Coast Guard. (n. d.) *GPS Problem Report Status*, Navigation Center, U.S. Department of Homeland Security. [Online]. Available at: https://navcen.uscg.gov/gps-problem-report-status (Accessed: 17 March 2023).

University of Nottingham. (2016) 'GPS jamming: keeping ships on the 'strait' and narrow', *University of Nottingham News,* [Online] 21 July 2016. Available at: www.nottingham.ac.uk/news/pressreleases/2016/july/gps-jamming-keeping-ships-on-the-strait-and-narrow.aspx (Accessed: 17 March 2023).

University of Texas News. (2013) 'UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea', *University of Texas News,* [Online] 29 July 2013. Available at: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ (Accessed: 21 March 2023).

Warner Jon S. and Johnston, Roger G. (2002) 'A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing', *The Journal of Security Administration* 25, (2002), pp. 19-28. Available at: https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-2384.

Weinstein, Adam. (2017) 'There's a silent threat plaguing the Navy, and it may be related to recent accidents at sea', *Business Insider*, [Online] 24 August 2017. Available

at: www.businessinsider.com/sleep-deprivation-is-a-silent-threat-to-the-navy-related-to-accidents-2017-8?r=US&IR=T (Accessed: 21 March 2023).

Wesson, Kyle, Shepard, Daniel, and Humphreys, Todd E. (2012) 'Straight Talk on Anti-Spoofing Securing the Future of PNT', *GPS World*, January, pp. 32-63, p. 33. Available via University of Texas at Austin Radiology Laboratory publications, at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/antiSpoofStraightTalk_Wesson.pdf.

Westbrook, Tegg. (2019) 'The Global Positioning System and Military Jamming: The geographies of electronic warfare', *Journal of Strategic Security* 12(2), p. 1-6. Available at: 10.5038/1944-0472.12.2.1720.

Westbrook, Tegg. (2023) 'A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives', *Journal of Strategic Security* 17(2), In Press.

Westbrook, Tegg. (2023a) 'Political Motivations Behind Radiofrequency Interference Strategies Affecting Aircraft in Europe', *Scandinavian Journal of Military Studies*. Under peer review.

Woody, Christopher. (2017) 'The Navy's 4th accident this year is stirring concerns about hackers targeting US warships', *Business Insider*, [Online] 24 August 2017. www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?r=US&IR=T (Accessed 17 March 2023).

Zorz, Zeljka. (2018) 'Vulnerable ship systems: Many left exposed to hacking', *Help Net Security*, [Online] 7 June 2018. Available at: www.helpnetsecurity.com/2018/06/07/vulnerable-ship-systems/ (Accessed 21 March 2023).