6

Maritime Cyber Threats

Jamming and Spoofing of Commercial Vessels

Raul (Pete) Pedrozo

6.1 INTRODUCTION

The importance of high navigational standards for ships operating at sea goes without question. These standards ensure the safety of vessels, crews, and cargoes, as well as the protection of the marine environment. Ships rely heavily on types of the Global Navigation Satellite System (GNSS) – such as the NAVSTAR Global Positioning System (GPS), Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), BeiDou Navigation Satellite System (BDS), and Galileo[1] – for the safety of navigation. Position, navigation, and time (PNT) based on satellite input allow shipboard "receivers to determine location to a high degree of precision" (McCrystal 2018). Thus, GNSS as a source of PNT must be certain and protected from manipulation.

GNSS performance is assessed using four criteria: (1) accuracy, the difference between a receiver's measured and real position, speed, or time; (2) integrity, a system's capacity to provide a threshold of confidence and, in the event of an anomaly in the positioning data, an alarm; (3) continuity, a system's ability to function without interruption; and (4) availability, the percentage of time a signal fulfills the above accuracy, integrity, and continuity criteria (INTERTANKO 2019, 12).

The views expressed in this chapter are those of the author and do not represent the views of the Department of the Navy, the Department of Defense, or the US government.

[1] GPS (USA), GLONASS (Russia), BeiDou (China), and Galileo (EU) are all types of GNSS. GPS provides users with position, navigation, and time (PNT) services and has global coverage. The US Air Force develops, maintains, and operates the space and control segments. GLONASS is a "space-based satellite navigation system operating in the radionavigation-satellite service." It "provides an alternative to GPS and is the second navigational system in operation" with global coverage and comparable precision. BeiDou has been in operation in the Asia Pacific region since December 2012. Galileo provides "improved services relating to the use of dual frequency" (INTERTANKO 2019, 12–13).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

While some interference with GNSS-type systems is unintentional, there is a growing threat to these systems by malign actors (such as China, Iran, and Russia) that can adversely affect their use for safe navigation. Blocking, jamming, or seriously degrading services that rely on radio waves (that is, harmful interference) threaten "critical infrastructure and safety services used every day, from commercial aviation to energy distribution to satellite navigation systems" (ITU News 2022). Protecting the GNSS is therefore critical for ensuring the safe and efficient operation of manned, unmanned, and autonomous ships at sea that rely on positioning and navigation systems.

GNSS-type systems, however, are vulnerable to attack. State and non-State actors can attack PNT data "through electronic warfare (EW) capabilities" that can result in significant damage to (inter alia) military operations, as well as everyday commercial shipping activities (C4ADS 2019). Thus, the proliferation of new technologies and methodologies to interfere with GNSS has emerged "as a viable, disruptive strategic threat" that could "endanger everything from global navigational safety to civilian finances, logistics, and communication systems" (C4ADS 2019).

This chapter will discuss the various threats to the GNSS and how States can mitigate against disruption of services caused by jamming and spoofing. It will discuss the efforts at the International Maritime Organization (IMO) to mitigate threats to the GNSS. It will also review various measures taken by the US to protect the US maritime transportation system from cyber threats.

6.2 TERMINOLOGY

GPS is the premier provider of PNT service. It is comprised of three segments: ground control, space, and user equipment. The constellation of satellites that make up the space segment continuously broadcasts GPS signals and is under the command and control of the ground control segment. The user equipment segment consists of cards and receivers used by military aircraft, ships, land vehicles, munitions, and handheld devices that derive PNT data from the satellite signals (GAO 2024). PNT allows for the "determination of location (positioning), the ability to traverse to a new location along a path (navigation), and the knowledge of the current time (timing), all with a high level of precision" (NSTC 2021).

GNSS satellites provide signals that "transmit positioning and timing data to GNSS receivers," which are used to determine location (INTERTANKO 2019, 4). Because GNSS signals have low power compared to other radio signals, even a weak interference source can cause a GNSS receiver to fail or produce misleading information. Interference occurs when RF waveforms overwhelm the satellite signal, thereby degrading or denying the GNSS receiver's ability to operate (NSTC 2021, 3–4).

Jamming is caused by interfering with signals at GNSS frequencies. When done intentionally, jamming overpowers the weak GNSS signal receiver. As a result, a

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

vessel is unable to determine its exact location. Brute force jamming occurs "when an attacker generates noise-like signals at frequencies used by a GNSS system . . . to prevent GNSS receivers from tracking authentic signals" (C4ADS 2019, 9). Both military jammers and Personal Protection Devices (PPDs) can be used to jam GNSS receivers intentionally (INTERTANKO 2019).

GNSS spoofing attacks provide GNSS-like signals that are coded and transmitted locally to deceive a GNSS receiver "by broadcasting incorrect GNSS signals, structured to resemble a set of normal GNSS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time" (INTERTANKO 2019, 5; C4ADS 2019, 9). Spoofed signals may be altered by the attacker to cause the GNSS receiver to think its position is "somewhere other than where it actually is" or where it really is "but at a different time" (INTERTANKO 2019, 5). Measurement spoofing creates "signals that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change" (NSTC 2021, 4). Data spoofing applies "incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT" (3).

A common form of GNSS spoofing – a carry-off attack – begins by broadcasting synchronized signals with "genuine signals observed by the target receiver" (INTERTANKO 2019, 5). As the power of the counterfeit signals is gradually increased, the "vessel's GNSS receiver tracks the false signals," which are then "manipulated to report a different location to the genuine signals" (5). Spoofing attacks that are intended to remain undetected require military grade technology.

The International Telecommunication Union (ITU) Radio Regulations are the international treaty regulating the global use of the RF spectrum and satellite orbits. The Regulations provide that "all stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service" (ITU 2020, 0.4). Harmful interference occurs when interference "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 Radio Regulations" (1.169). Stations are prohibited from carrying out unnecessary transmissions or transmitting superfluous signals, false or misleading signals, or signals without identification (15.1).

6.2.1 *Jamming and Spoofing*

Cyberattacks against international shipping by State-sponsored hackers have risen dramatically over the past twenty years, increasing from zero in 2003 to three in 2013 to sixty-four in 2023. These attacks adversely affect safety at sea by interfering with a vessel's navigation and communication equipment. For example, an Automatic Identification System (AIS) can be easily spoofed to broadcast incorrect

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

data. Over 80 percent of these attacks have originated in China, Iran, North Korea, and Russia (Telling 2024). Given that China and Russia operate their own GNSS (BeiDou and GLONASS), they are more likely to manipulate GNSS for tactical and strategic advantages.

In May 2017, the US Director of National Intelligence reported to Congress that "the global threat of electronic warfare (EW) attacks against space systems will expand in the coming years in both number and types of weapons" (Coats 2017). These developments will "focus on jamming capabilities against dedicated military satellite communications (SATCOM), Synthetic Aperture Radar (SAR) imaging satellites, and enhanced capabilities against GNSS, such as the US Global Positioning System (GPS)" (Coats 2017). Malign States will blend EW and cyber-attack capabilities to develop "sophisticated means to deny and degrade information networks" (Coats 2017). Chinese researchers are working on "methods to enhance robust jamming capabilities with new systems to jam commonly used frequencies," and Russia will "modernize its EW forces and field a new generation of EW weapons by 2020" (Coats 2017). Additionally, Iran and North Korea are "enhancing their abilities to disrupt military communications and navigation" (Coats 2017).

6.2.1.1 China

Systematic GPS manipulation occurred in at least twenty locations along the Chinese coast during 2019. The sites include both oil terminals and government installations in Shanghai and Qingdao. Although the reason for the manipulation is uncertain, it may be associated with China's illicit import of UN-sanctioned Iranian crude oil. The anomaly – GPS spoofing circles – was first detected by the M/V *Manukai* in July 2019. As the US-flagged container ship entered the port of Shanghai, its AIS[2] appeared to malfunction: "vessels on the navigation screen appeared and disappeared without explanation and appeared to move when they were in fact stationary" (Bergman 2019).

A closer analysis by the Center for Advanced Defense Studies determined that hundreds of AIS vessel locations from ships navigating on the Huangpu River were appearing at false locations. Notably, vessel GPS locations were jumping from the river "to a ring of positions appearing on land" (Bergman 2019). When vessels approached the area of interference, their AIS broadcast positions jumped from their true locations to a point on land where the false broadcasts occurred in a ring about "200 meters in diameter" (Bergman 2019). Vessel speeds within the circle ranged from 21 to 31 knots, and their course varied depending on their location within the circle. Once a vessel was affected by the anomaly, it would broadcast a

[2] AIS transponders are designed to provide position, identification, and other information about the ship to other ships and to coastal authorities automatically to enhance situational awareness and promote safety at sea.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

random position within the ring "or from other high-speed positions scattered around it" (Bergman 2019). In all probability, the center of the ring marks the location of a GPS-disrupting device.

The locations affected by GPS manipulation were in six Chinese cities, with the focus (sixteen of the twenty) on oil terminals. Nonetheless, three government buildings in Shanghai and Qingdao were also affected – "the Industrial and Commercial Bank of China in Shanghai, the Qingdao tax administration office, and the Qingdao headquarters of the Qingjian industrial group" (Bergman 2019). Activation of the GPS-disrupting devices at these buildings was likely a security measure.

Deployment of GPS manipulation devices at oil terminals, however, may be an effort by China to mask imports of US-sanctioned Iranian crude oil. AIS tracking data indicates that Iranian tankers delivered oil to China in June and July and that Chinese tankers engaged in ship-to-ship transfers with Iranian tankers to circumvent US sanctions (Bergman 2019; Goward 2019; Sheppard et al. 2019; Singhi et al. 2019; Zeng Xiaojun 2021). For example, at an oil terminal east of Dalian, although the manipulation devices were unable to mask the position of all vessels approaching the terminal, their use "would make it impossible to reliably link a vessel's AIS track with satellite imagery of a vessel discharging crude at dock" (Bergman 2019; Goward 2019; Zeng Xiaojun 2021).

It is also not uncommon for Chinese vessels to disable their AIS or spoof their location to mask illegal, unreported, and unregulated fishing activities (Pedrozo 2022). In 2020, over 300 Chinese fishing vessels converged on the waters around the Galápagos Islands (a UNESCO World Heritage Site and an Ecuadorian national marine reserve) to fish for squid and other fish stocks. Although there is no direct evidence that any Chinese vessels entered the marine reserve, numerous ships went "dark" to conceal their actual location and identity (AFP 2020; Ramos Miranda 2020; Rust 2020).

A Virginia-based company – HawkEye 360 – did confirm that there were unidentified vessels operating within Ecuador's exclusive economic zone (EEZ) that coincided with Chinese fishing vessels going dark (Alberts 2020). Data collected between July 13 and August 13, 2020, reflects that Chinese fishing vessels turned off their AIS devices on forty-three occasions for an average of two days at a time (Alberts 2020). During that timeframe, HawkEye 360 determined that fourteen unidentified vessels were operating within the EEZ around the Galápagos, six of which were "immediately adjacent to the bulk of the Chinese DWF fleet, suggesting that they had broken away" from the main fleet and entered Ecuador's EEZ (Alberts 2020). Additionally, six Chinese vessels spoofed their true location, sending out false signals that "puts them between the Chatham Islands and New Zealand, about 10,000km away" (Satherley 2020). Satellite imagery was unable to confirm the presence of Chinese vessels in New Zealand's waters.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

6.2.2.2 Iran

Iran has publicly stated that it has the capacity to spoof GPS signals, which it appears to have used to interfere with shipping in the Persian Gulf (Goward 2020). In May, the Iranian Revolutionary Guard Corps (IRGC) seized the UK-flagged *Stena Impero* and the Liberian-flagged *Mesdar* after the vessels experienced interference with their GPS (Browne and Starr 2019). The US Maritime Administration (MARAD) subsequently issued a warning in August 2019 regarding Iranian threats to commercial shipping operating in the Strait of Hormuz, the Persian Gulf, and the Gulf of Oman. The administration warned that vessels operating in the region may "encounter GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming with little to no warning" (MARAD 2019). The warning indicated that the *Stena Impero* and *Mesdar* had experienced GPS interference prior to their seizure. Additionally, the administration warned that there had been reports that unknown entities were falsely claiming to be US or coalition warships via bridge-to-bridge communications (MARAD 2019).

Officials at US Central Command stated that GPS jammers have been placed at "Abu Musa Island, which lies in the Persian Gulf close to the entrance of the Strait of Hormuz." The IGRC uses the jammers to disrupt "ship navigation systems, hoping ships … will mistakenly wander into Iranian waters" while their GPS systems are malfunctioning, giving the IRGC a pretext to seize them (Browne and Starr 2019). The IRGC is additionally using spoofed communications to disguise their boats as merchant ships instead of IRGC or Iranian Navy vessels (Browne and Starr 2019).

Like China, Iran has also engaged in "circle spoofing." In March 2020, a user in Iran reported testing a GPS device. After ten minutes, the device showed the correct time but not the correct location – it was "moving around a big circle in Tehran" at a speed of 35 km per hour (Goward 2020). The circle was located near the Iran Army's Command and Staff College. A second location was reported around a "government complex that houses offices for several defense and technology-related organizations" (Goward 2020). One theory is that Iran may be interfering with GPS signals to disrupt "surveillance systems in the vicinity of sensitive government facilities" (Goward 2020).

In 2023, MARAD issued two additional maritime advisories due to heightened tensions in the region for the Persian Gulf and Strait of Hormuz regarding (inter alia) navigation and communications disruptions. MSCI Advisory 2023-11 warned that vessels operating in these areas could "encounter GPS interference (see Advisory 2023-005), AIS spoofing, bridge-to-bridge communications spoofing, and/or other communications jamming" (MARAD 2023b). The advisory further warned that "vessels have also reported bridge-to-bridge communications from unknown entities falsely claiming to be U.S. or coalition warships" (MARAD 2023b). MARAD

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

advised that "in addition to risks to navigation, confusion from such disruptions could be leveraged by bad actors to facilitate physical attacks," and that vessels should take additional precautions if they (or vessels in their vicinity) experience such disruptions (MARAD 2023b). US-flagged vessels were advised to notify the US Fifth Fleet Battle Watch immediately if they suspected that they were being "hailed from a source falsely claiming to be a U.S. or coalition naval vessel" or if they were "asked for positions or info on coalition military vessels or aircraft operating in the area" (MARAD 2023b). Any disruptions or anomalies regarding maritime GPS were to be reported immediately to the US Coast Guard (USCG) Navigation Center (NAVCEN).

MSCI Advisory 2023-005 similarly warned that there had been multiple instances of GPS interference reported in the Strait of Hormuz and that this interference could "result in lost or inaccurate GPS signals affecting bridge navigation, GPS-based timing, and communications equipment (including satellite communications equipment)" (MARAD 2023a). MARAD also advised that "AIS signals can be spoofed, resulting in or missing AIS data" because AIS operates on nonsecure VHF-FM channels using open, unencrypted, and unprotected radio systems (MARAD 2023a). Therefore, AIS "should never be solely relied upon for collision avoidance or navigational decision-making" (MARAD 2023a). Maritime GPS disruptions or anomalies should be reported immediately to the NAVCEN.

The UK Maritime Trade Operations (UKMTO) office has similarly reported on "electronic interference" incidents involving merchant ships in the Persian Gulf. For example, between April 2 and 3, 2024, the UKMTO received a report from a vessel that was experiencing disruption to its electronic navigation systems (GPS/AIS) 95 nautical miles east of Las Al Zour, Saudi Arabia (Schuler 2024).

6.2.2.3 Russia

Russia has the capability and technology to spoof GPS and may be assisting Iran in interfering with AIS transmissions in the Persian Gulf (Joffre 2019). Russia has also actively engaged in spoofing attacks in the Black Sea. In June 2020, more than twenty ships in the Black Sea, near Novorossiysk Commercial Sea Port, reported that their AIS was erroneously showing their position as Gelendzhik Airport, 32 km inland, and that the GPS considered the position to be safe within 100 m. MARAD issued a warning that GPS interference had been reported in the vicinity of 44-15.7N, 037-32.9E on June 22, 2017, and that ships should "exercise caution when transiting the area" (C4ADS 2019, 14; Goward 2017). Navigation experts concluded that the interference was a clear case of "spoofing or sending false signals to cause a receiver to provide false information" (Goward 2017). Although there was no official explanation for the disruption, it could be "attributed to Russian testing of satellite navigation spoofing technology" or to encourage the use of Russia's GLONASS instead of GPS (Goward 2017; Lo 2019).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

In June 2020, the positioning data of two NATO warships – HMS *Defender* and HNLMS *Evertsen* – showed the ships to be off the Crimean coast near Sevastopol when they were, in fact, moored 180 miles away in Odesa. The British destroyer and the Dutch frigate arrived in Odesa on June 18 after conducting an exercise in the Black Sea. The ships' AIS showed them leaving Odesa just before midnight on June 18, and then sailing directly to Sevastopol, coming to within 2 nautical miles of the Russian Black Sea Fleet's headquarters. Evidence from live webcam feeds shows that the warships never left Odesa (Sutton 2021).

Ukrainian authorities have also warned shipowners sailing to Odesa that satellite communication systems are being disrupted in the Black Sea. In June 2024, at least forty ships in the Black Sea were broadcasting compromised AIS locations. Over 33 percent of the ships reporting incorrect positions were loading Russian coal (Quinn 2024).

A 2024 report prepared by the Center for Advanced Defense Studies indicates that Russia has developed "a comparative advantage in the targeted use and development of GNSS spoofing capabilities to achieve tactical and strategic objectives at home and abroad" (C4ADS 2019, 9). Russia is developing "a comprehensive suite of asymmetrical EW systems designed to deceive, degrade, and deny military and civilian GNSS receivers" and has the "capability to create large GNSS denial-of-service spoofing environments" without targeting a single GNSS satellite (13).

The report identified nearly 10,000 instances "across 10 locations that affected 1,311 civilian vessel navigation systems" between 2016 and 2018 (C4ADS 2019, 13, 16, 20–21). In some cases, the Russian Federal Protective Service (FSO) is using mobile systems to spoof GNSS to protect very important persons. In other cases, Russian GNSS spoofing is used to protect strategic facilities in Moscow and protected facilities off the coast of Russia and Crimea in the Black Sea. Finally, Russia is also using GPS spoofing in active combat zones such as Syria "for airspace denial purposes" (13, 23–24, 26–28, 31–33, 44–46).

Many of these instances occur over brief periods of time in isolated locations, suggesting that "at least some of the devices used to conduct GNSS disruptions are mobile and can be temporarily deployed to create local areas of effect."[3] During President Putin's visit to the Kerch Bridge on May 15, 2018, twenty-four vessels anchored near the bridge "reported spoofed GNSS positioning information at the Anapa Airport more than 65 kilometers away."[4] Similar incidents occurred in September 8, 2017, and September 11, 2018, when Putin visited the Zvezda

[3] For example, GNSS spoofing activities in proximity to the Kerch Bridge on September 15, 2016, and May 15, 2018, coincided with a visit by President Vladimir Putin "to oversee the progress and completion of the Kerch Bridge" (C4ADS 2019, 26).

[4] The vessels were probably spoofed by a transmitter on one of the FSO vehicles accompanying Putin (C4ADS 2019, 27).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Shipyard, which is "located near the remote Russian Far East town of Bolshoy Kamen," 30 km from the port city of Vladivostok.[5]

GNSS spoofing devices used to protect strategic government residences owned and operated by the FSO and other sensitive facilities are stationary. Spoofing incidents at these facilities occur more frequently, affect "a greater number of vessels," and "interfere with receivers over a greater distance" (C4ADS 2019, 31). Vessels affected by spoofing report their "positions at local civilian airports" (31). Nearly 8,000 of the GNSS spoofing events occurred beyond the Russian territorial sea in the Black Sea and potentially posed a risk to the safety of navigation. Given the geographic extent and the nature of the events, some of the instances of interference also violated Article 15 of the Radio Regulations, which prohibit harmful interference with RFs (25).

6.3 MITIGATING RISKS

The importance of ensuring reliable PNT has prompted the concept of "Resilient PNT." Resilient PNT merges traditional PNT technology "with non-traditional and emerging technology to improve the reliability, performance, and safety of mission-critical applications, where the discrepancy in data accuracy, availability, and stability can impact the safety, security and economic viability of vessels at sea" (McCrystal 2018). By detecting, protecting, and authenticating vulnerabilities in GNSS (such as jamming and spoofing), vessels can be offered alternatives to existing PNT sources and provided PNT information they can trust (McCrystal 2018).

6.3.1 *International Maritime Organization Initiatives*

6.3.1.1 Maritime Safety Committee Resolution MSC.428(98)

In 2017, the Maritime Safety Committee adopted Resolution MSC.428(98) to raise awareness of cyber risk threats and vulnerabilities to support safe and secure shipping and encourage all maritime industry stakeholders to expedite work toward safeguarding shipping from current and emerging cyber threats and vulnerabilities. The resolution (inter alia) affirmed that an approved safety management system should consider cyber risk management and encouraged administrations to ensure that cyber risks are appropriately addressed in safety management systems (IMO 2017c).

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT. The Guidelines on Maritime Cyber Risk Management were first adopted in 2017 and have since been

[5] A vessel moored at the Zvezda Shipyard "reported spoofed positioning information at the Vladivostok International Airport" (C4ADS 2019, 28).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

revised twice (IMO 2017b).[6] They provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The guidelines also include functional elements that support effective cyber risk management (IMO 2022).

A "maritime cyber risk" refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event that may result in shipping-related operational, safety, or security failures because of information or systems being corrupted, lost, or compromised (IMO 2022, para. 2.1.1). Stakeholders are encouraged to take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to the digitization, integration, and automation of processes and systems in shipping (para. 1.2).

The guidelines are predicated on the goal of supporting safe and secure shipping that is operationally resilient to cyber risks (IMO 2022, paras. 1.5, 3.2). Risk management is fundamental to safe and secure shipping operations, and greater reliance on digitization, integration, automation, and network-based systems creates an increasing need for cyber risk management in the shipping industry (para. 1.4).

Vulnerabilities created by accessing, interconnecting, or networking shipboard systems that are critical to the safety and security of shipping can result in cyber risks that must be addressed. Vulnerable shipboard systems include (inter alia) bridge systems, cargo handling and management systems, propulsion and machinery management and power control systems, access control systems, passenger servicing and management systems, passenger-facing public networks, administrative and crew welfare systems, and communication systems (IMO 2022, para. 1.4).

The guidelines emphasize that there is a distinction between information technology and operational technology systems and that consideration should be given to the protection of information and data exchange within these systems. "Information technology systems" focus on the use of data as information. "Operational technology systems" focus on the use of data to control or monitor physical processes. These technologies and systems present risks to critical systems and processes associated with the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance, and design of cyber-related systems, or from intentional and unintentional cyber threats. The exploitation of operational and/or information technology vulnerabilities raises safety issues, particularly where critical systems (such as bridge navigation or main propulsion systems) are compromised (IMO 2022, paras. 2.1.2, 2.1.3, 2.1.5).

"Cyber risk management" is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating that risk to an acceptable level, considering the costs and benefits of actions

[6] A third revision was approved by the Maritime Safety Committee in September 2024 but has not yet been approved by the Facilitation Committee.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

taken by stakeholders (IMO 2022, para. 3.1). Functional elements that support effective cyber risk management should be incorporated concurrently and continuously into a risk management framework. These elements include the following:

1 **Identify:** Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations.
2 **Protect:** Implement risk control processes and measures, along with contingency planning, to protect against a cyber event and ensure the continuity of shipping operations.
3 **Detect:** Develop and implement the activities necessary to detect a cyber event in a timely manner.
4 **Respond:** Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.
5 **Recover:** Identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event (IMO 2022, para. 3.5).

These functional elements include activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange. They establish an ongoing process with effective feedback mechanisms (IMO 2022, para. 3.6). For cyber risk management to be effective, there must be an appropriate level of awareness of cyber risks at all levels of the organization (para. 3.7).

In addition to these guidelines, States should refer to State and Flag Administration requirements, as well as relevant international and industry standards and best practices, including (inter alia) the following:

1 The Guidelines on Cyber Security Onboard Ships produced and supported by the International Chamber of Shipping, the International Union of Marine Insurance, the Baltic and International Maritime Council (BIMCO), the Oil Companies International Marine Forum, the International Association of Independent Tanker Owners (INTERTANKO), the International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, the World Shipping Council, and the Superyatch Builders Association (SYBAss).
2 The consolidated IACS Recommendation on Cyber Resilience (No. 166).
3 ISO/IEC 27001: Information security, cybersecurity, and privacy protection – Information Security Management Systems – requirements.
4 The US National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.
5 The IAPH Cybersecurity Guidelines for Ports and Port Facilities (IMO 2022, paras. 4.1, 4.2).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

PERFORMANCE STANDARDS FOR MULTI-SYSTEM SHIPBORNE RADIONAVIGATION RECEIVERS. In 2015, the IMO adopted performance standards for multi-system shipborne radionavigation receivers (IMO 2015) to allow for the combined use of current and future radionavigation, as well as augmentation systems,[7] for the provision of position, velocity, and time data within the maritime navigation system (para. 1.4). A multi-system receiver that uses navigation signals from two or more GNSS-type systems, with or without augmentation, provides improved position, velocity, and time data, as well as improved resistance to intentional and unintentional RF interference. This combined approach also provides redundancy to mitigate the loss of a single system (para. 1.5).

A multi-system shipborne radionavigation receiver equipment should include the following minimum components and capabilities:

1 antennas capable of receiving all radionavigation signals required to support the functionality of the receiver equipment;
2 receiver(s) and processor(s) capable of processing the radionavigation signals required to support the functionality of the receiver equipment;
3 means of accessing the computed position, velocity, and time (PVT) information;
4 interface for supplying data controlling/configuring the receiver;
5 display;
6 raw data output for the provision of additional information, such as range measurements and the GNSS's navigation data;
7 an indication of the quality and reliability of the computed and distributed PVT data to the user; and
8 an indication of radionavigation systems currently used for the PVT information to the user (IMO 2015, para. 2.1).

The system should be capable of mitigating interference from authorized out–of-band sources. It should provide a means of integrity monitoring for each PVT source employed and multi-source autonomous integrity monitoring (IMO 2015, para. 2.3).

The equipment should operate using civil access navigation signals of at least two independent GNSS-type systems, provide PVT data with the necessary level of resilience and integrity, and have the facilities to process augmentation data (IMO 2015, paras. 3.1, 3.2, 3.4). The system should also have the capability to operate using terrestrial radionavigation systems signals if the use of such signals is anticipated, as well as the ability to select or deselect radionavigation and augmentation signals (paras. 3.3, 3.5).

[7] Augmentation systems use ground- or space-based transmitters to provide augmentation data to improve accuracy and integrity for specific service areas (such as harbor entrances, harbor approaches, and coastal waters) (IMO 2015, para. 1.3).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

The equipment should additionally be able to provide a single PVT solution, including:

1 position information of the consistent common reference point in latitude and longitude, with coordinates in degrees and minutes to a precision reflective of the accuracy of the position information, up to four decimal places;
2 course over ground (COG) of the consistent common reference point in degrees to a precision reflective of the accuracy of the calculated course information, relative to true north, up to one decimal place;
3 speed over ground (SOG) of the consistent common reference point in knots to a precision reflective of the accuracy of the calculated speed information, up to two decimal places; and
4 time, referenced to Universal Coordinated Time (UTC), to one-tenth of one second (IMO 2015, para. 3.6).

In addition, the system should be capable of providing the PVT solution to the required accuracy within five minutes where there is no valid satellite almanac data (cold start), within one minute where there is valid satellite almanac data (warm start), and within two minutes when subjected to a power interruption or loss of signals of <60 s (IMO 2015, para. 3.7). It should also provide time in UTC and be capable of meeting the requirements for the phases of navigation outlined in Assembly Resolution A.1046(27) (IMO 2011, 2015, paras. 3.8, 3.9).

The equipment should be able to generate a new PVT solution at least once every half second for high-speed craft (HSC) and at least once every second for conventional vessels (IMO 2015, para. 3.10). It should also be able to assess whether the performance of the PVT solution (such as accuracy and integrity) meets the requirements for each phase of navigation and to provide an alert when such assessment cannot be determined (para. 3.11). If the equipment is unable to assess the current achieved performance (such as accuracy and integrity) with respect to each navigation phase, it should provide a caution after two seconds for HSC and three seconds for conventional vessels (para. 3.12). It should additionally provide a warning if (after five seconds for HSC or seven seconds for conventional vessels) new PVT data has not been calculated (para. 3.13).

If it is not possible to provide a new position update at the next scheduled update, the system should output the last plausible position, SOG, COG, and the time of the last valid fix, until position update is resumed (IMO 2015, para. 3.14). The equipment should also provide an indication of augmentation status, including the receipt of augmentation signals; the validity of the signals received; whether augmentation is applied to the position in the PVT solution; and the identification of the augmentation signals (para. 3.15). The following information should be provided, in alphanumerical form, for the final PVT solution and for each individual source when requested, to a local display (or a separate interfaced display):

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

(1) position; (2) COG and SOG; (3) time; (4) the PVT solution sources; (5) the assessment of the navigation phases for which performance requirements are supported; (6) the identification of the augmentation signals applied to the position solution; and (7) any alert information (para. 3.16).

In addition, the equipment should provide the following interfaces:

1 at least one interface from which the PVT solution should be available in the WGS 84;
2 at least one interface from which data from all available sources can be provided;
3 an interface for alert management (that is, with the Bridge Alert Management); and
4 facilities to accept the input of augmentation signals from at least one source (IMO 2015, para. 4.1).

The system should be capable of operating satisfactorily under normal interference conditions, consistent with the requirements of IMO Resolution A.694(17) (IMO 1991), taking into account the typical electromagnetic and RF spectrum environment on board and from outside a vessel and ensuring that no permanent damage can result from an accidental short circuit or grounding of the antenna or any of its input or output connections or any of the inputs or outputs (IMO 2015, paras. 4.2, 4.3). Documentation for the equipment should be provided, preferably in an electronic format (para. 5).

6.3.1.2 Guidelines for Shipborne PNT Data Processing

In June 2017, the Maritime Safety Committee approved guidelines for shipborne PNT data processing (PNT-DP) to enhance the safety and efficiency of navigation by improving the provision of PNT data to bridge teams (including pilots) and shipboard applications (for example, AIS and ECDIS) (IMO 2017a, para. 1). Shipborne PNT-DP[8] is the core repository for principles and functions used for the provision of reliable and resilient PNT data (para. 2).

The guidelines aim to establish a modular framework for the further enhancement of shipborne PNT data provision by supporting:

1 the consolidation and standardization of requirements on shipborne PNT data provision considering the diversity of ship types, nautical tasks,

[8] PNT-DP is defined as a set of functions facilitating: (1) multiple sources of data provided by PNT-relevant sensors and services (for example, GNSS receiver and DGNSS corrections) and further onboard sensors and systems (for example, radar, gyro, speed and distance measuring equipment (SDME), and echo-sounder providing real-time data) to exploit existing redundancy in the PNT-relevant input data; and (2) multi-system and multi-sensor-based techniques for enhanced provision of PNT data (IMO 2017a, para. 3).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

nautical applications, and the changing complexity of situations up to customized levels of support;
2 the identification of dependencies between PNT-relevant data sources (sensors and services), applicable PNT data-processing techniques (methods and thresholds), and achievable performance levels of provided PNT data (accuracy, integrity, continuity, and availability);
3 the harmonization and improvement of onboard PNT data processing based on a modular approach to facilitate changing performance requirements in relation to nautical tasks, variety of ship types, and nautical applications, and under consideration of user needs (SN.1/Circ.274);
4 the consequent and coordinated introduction of data and system integrity as a smart means to protect PNT data generation against disturbances, errors, and malfunctions (safety), as well as intrusions by malicious actors; and
5 the standardization of PNT output data, including integrity and status data (IMO 2017a, para. 5).

The guidelines provide recommendations on how to handle differences regarding installed equipment, the current system in use, the feasibility of tasks and related functions, and the performance of data sources, as well as usability in specific regions and situations (IMO 2017a, para. 6). A structured approach for the stepwise introduction of integrity is developed to achieve resilient PNT data provision in relation to the application grades and supported performance levels (para. 7). The guidelines are designed to achieve standardized and integrity-tested PNT output data to enhance user awareness regarding the achieved performance level (para. 8).

The guidelines have a modular structure: (1) Module A, data input – sensors, services, and sources; (2) Module B, functional aspects; (3) Module C, operational aspects; (4) Module D, interfaces; and (5) Module E, documentation (IMO 2017a, para. 10). Definitions, abbreviations, and expected operational and technical requirements on PNT/Integrity (I) data output are contained in the three appendices (para. 11).

Shipborne PNT-DP comprises three functional blocks: (1) pre-processing; (2) main processing; and (3) post-processing (IMO 2017a, para. 15). The pre-processing function extracts, evaluates, selects, and synchronizes input (sensor and service) data (including the associated integrity data) to preselect the applicable techniques to determine PNT and integrity output data (para. 16). The main processing function generates the PNT output data and associated integrity and status data (para. 18). Finally, the post-processing function generates the output messages by coding the PNT output data (PNT, integrity, and status data) into specified data protocols (para. 19).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

6.3.2 *Industry Initiatives*

Several maritime groups provide industry guidelines, standards, and best practices on cyber security onboard ship – for example, the International Chamber of Shipping, BIMCO, the Oil Companies International Marine Forum, INTERTANKO, INTERCARGO, InterManager, the World Shipping Council, and SYBAss.

The INTERTANKO guidelines, for example, provide "guidance on the various types of GNSS, an introduction to threats associated with these systems and guidance on how to mitigate against these threats" (INTERTANKO 2019, 1). Guidelines for the ship's navigator include:

1 using radar and Electronic Chart Display and Information Systems (ECDIS) interlay (overlay or underlay) to detect GPS spoofing and jamming when land is visible on the radar;
2 verifying position at appropriate intervals;
3 observing significant difference between dead reckoning (DR) position (arrived with Gyro Course steered and distance by speed log) and GNSS fix; and
4 observing and verifying using an echo sounder to compare the depths when sailing in suitable depth areas (INTERTANKO 2019, 6).

If jamming and spoofing are detected, the navigator should take immediate action:

1 Manually select a secondary position sensor.
2 Select other GNSS input if provided and use a "GNSS divergence" alarm to check any marginal difference between positioning sources.
3 If a secondary sensor is unable to provide a vessel's position and no other means are available to input position fixing, the navigator should select the DR or estimated position (EP) mode.
4 Manually plot the ship's position if near enough to shore and seek greater sea room, if possible.
5 Use AIS with extreme caution, since it will also be affected by the jamming and spoofing attack.
6 If unable to ascertain vessel position relative to navigational hazards, stop the vessel (INTERTANKO 2019, 6).

When the situation is somewhat stable:

1 Check the vessel's GNSS position frequently to detect when the service is available again.
2 Report GNSS disruptions or anomalies to the authorities listed in Appendix A.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

3 Take note of critical information, such as the actual location (latitude/longitude), date/time, and duration of the outage or disruption.
4 When possible, provide photos or screenshots of equipment failures during a disruption to assist analysts with identifying a potential cause.
5 For vessels using paper charts, continue plotting with alternative position fixing or DR (INTERTANKO 2019, 7).

Ship owners/managers should ensure that the bridge navigation equipment complies with MSC.1/Circ.1575 (IMO 2017a; INTERTANKO 2019, 7). The ECDIS should have an alarm management function. A multi GNSS receiver will enhance the system, and the use of GNSS open signals that have Navigation Message Authentication will provide additional protection (INTERTANKO 2019, 7). Ship owners/managers should also consider using Loran/E-Loran receivers as a backup/part of the resilient system and a way to detect jamming and spoofing (7). Crew training should include regular GNSS failure drills to develop competency in the detection of GNSS jamming or spoofing and safe navigation practices that are independent of GNSS.

Multiple mitigation strategies are available to help overcome interference:

1 filter in the receiver;
2 aid the receiver with an inertial measurement unit (IMU);
3 use of an adaptive antenna array (such as controlled reception pattern antennas);
4 development of advanced mitigation techniques using wideband GNSS signals; and
5 use of E-Loran receivers as a backup (INTERTANKO 2019, 8).

With respect to jamming, various GNSS-type systems deliver different services at different frequencies. This will mitigate against an attack but does not mean that the system will work through it. An IMU and an appropriate alarm management plan can be used to aid the receiver/navigation equipment in detecting an attack (INTERTANKO 2019, 8).

Spoofing countermeasures include the use of array antennas, such as controlled reception pattern antennas (CRPA). Monitoring GNSS receiver KPIs (key performance indicators) – clock jumps, unusual or implausible signal-to-noise density ratios, or differences between code and carrier measurements – and cryptographic techniques can also be effective (INTERTANKO 2019, 8). Other countermeasures include:

1 use of an adaptive antenna array;
2 fly-wheel algorithms to prohibit the system from immediate jumps in location and time in the GNSS receiver (ECDIS or external PNT software);
3 limiting the jumps (location) – GNSS receiver;

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

4 aiding the receiver with an IMU (even a low-cost IMU would be very effective for this purpose); and
5 use of Loran/E-Loran receivers as a backup/part of the resilient system, where available (INTERTANKO 2019, 9).

Suspected jamming and spoofing attacks should be reported as soon as possible. The Interference Detection and Mitigation Task Force was established to coordinate international efforts regarding the detection and reporting of jamming and spoofing (INTERTANKO 2019, 10). Reports regarding degradations, disruptions, or other incidents or anomalies can also be sent to the NAVCEN. Before reporting an incident to the NAVCEN, the following steps should be taken:

1 Reset the device by cycling power to the unit.
2 Confirm the settings for the GPS unit or GPS application.
3 Refer to the equipment manual.
4 Update the equipment software or firmware and GPS-mapping software.
5 Contact the equipment manufacturer for additional assistance (INTERTANKO 2019, 10).

Reports can also be made to the European GNSS Service Centre. In addition, merchant ships and shipping companies can contact the NATO Shipping Centre.

6.3.3 *US Government Initiatives*

6.3.3.1 Executive Order 13905

In February 2020, then president Donald Trump issued Executive Order 13905, aimed at strengthening US PNT services.[9] Disruption or manipulation of PNT services can adversely affect US national and economic security. "PNT services" is defined as any system, network, or capability that provides a reference to calculate, or augment the calculation of, longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof (§2(a)). "Critical infrastructure" is defined as systems and assets, whether physical or virtual, so vital to the US that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters (§2(c)).

The executive order establishes US policy to ensure that the disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of US critical infrastructure. The federal government is tasked with increasing national awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services. The federal government is also tasked with ensuring

[9] Executive Order 13905, 85 Fed. Reg. 9359 (February 18, 2020).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

that critical infrastructure can withstand the disruption or manipulation of PNT services (§3).

The Secretary of Commerce, in coordination with other relevant federal agencies and private sector users, was tasked with developing PNT profiles and making them available to the relevant agencies and private users. These PNT profiles will be used to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. PNT profiles will be reviewed and updated every two years (§4(a)). The PNT profiles created for the Defense, Transportation, and Homeland Security Departments will be used in updates to the Federal Radionavigation Plan (§4(b)). Relevant information from the PNT profiles will also be included in government contracts for products, systems, and services that integrate or utilize PNT services (§§4(d), 4(e)).

The Secretary of Homeland Security, in coordination with other relevant federal agencies, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services and shall use the results of that test to inform updates to the PNT profiles (§4(c)). Additionally, the Transportation, Energy, and Homeland Security Departments shall engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services (§4(g)). Finally, the Director of the Office of Science and Technology Policy shall coordinate the development of a national plan for the research, development, and testing of additional, robust, and secure PNT services that are not dependent on GNSS (§4(h)).

6.3.3.2 Federal Radionavigation Plan (2021)

The Federal Radionavigation Plan reflects the federal government's official PNT policy and planning and covers both terrestrial- and space-based, common-use, federally operated PNT systems. It does not apply to systems used exclusively by the Department of Defense or systems used primarily to conduct surveillance and communications functions. Federal PNT systems are operated to enable safe transportation and to enable commerce within the US. PNT services are provided in a "resilient and cost-effective manner, balancing costs and needed safety, security, and efficient operational capabilities" (DoD et al. 2022, x).

The Department of Transportation is responsible "for ensuring safe and efficient transportation" (DoD et al. 2022, x). The Department of Defense is responsible for "maintaining aids to navigation required exclusively for national defense" and "providing for the sustainment and operation of GPS for peaceful civil, commercial, and scientific uses on a continuous, worldwide basis, free of direct user fees" (x). The Department of Homeland Security is responsible, in coordination with other federal agencies, for enhancing the security and resilience of US critical

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

infrastructure and for the detection and mitigation of "sources of GPS interference within the United States" (x).

US GPS Standard Positioning Services (SPS) are available worldwide for continuous use on a nondiscriminatory basis by the international community free of direct user fees (DoD et al. 2022, §§3.2.2.1, 5.1). The US has committed to taking "all necessary measures for the foreseeable future to maintain the integrity, reliability, and availability of the GPS SPS" (§§3.2.2.1, 5.1). Protected Positioning Service (PPS) is available to authorized US and allied military users (§§3.2.2.2, 5.1).

GPS PPS signals are continuously monitored in near-real time, twenty-four hours a day, by satellite operators at the Schriever Air Force Base. SPS signals are not continuously monitored; however, PPS monitoring can detect "most anomalies in service, including user range errors, providing satellite operators the necessary information to take action and protect users from anomalous signals" (DoD et al. 2022, §3.2.5).

GPS users must plan for potential disruptions and take necessary steps to authenticate the reliability of the received GPS data and ranging signal. GPS users must be aware of the impact of GPS interference, should consider using GPS receivers designed to mitigate the effects of the jamming and spoofing of signals, and incorporate alternative PNT sources to ensure continued operations (DoD et al. 2022, §§3.2.10, 5.1.2). The Secretary of Transportation, in coordination with the Secretary of Homeland Security, is "responsible for the development, acquisition, operation, and maintenance of backup PNT capabilities that can support critical transportation, homeland security, and other critical civil and commercial applications" (§5.1.2).

The Secretary of Defense (SECDEF) is responsible for improving navigation warfare (NAVWAR) capabilities to deny hostile use of US "space-based PNT services, without unduly disrupting civil and commercial access to civil PNT services outside an area of military or homeland security operations" (DoD et al. 2022, §3.2.3).[10] SECDEF will also "develop, acquire, operate, realistically test, evaluate, and maintain NAVWAR" and other capabilities required to (1) effectively use "GPS services in the event of an adversary or other jamming, disruption, or manipulation"; (2) "develop effective measures to counter adversary efforts to deny, disrupt, or manipulate PNT services"; and (3) "identify, locate, and mitigate," in coordination with other federal agencies, "any intentional disruption or manipulation that adversely affects use of GPS for military operations" (§3.2.3). The NAVWAR program is designed to "ensure that the U.S. retains a military advantage in the area of conflict by protecting authorized use of GPS; preventing the hostile

[10] NAVWAR is defined as the deliberate defensive and offensive action to assure and prevent PNT information through the coordinated employment of space, cyberspace, and electronic warfare. Desired effects are generated through the coordinated employment of components within information, space, and cyberspace operations, including electronic warfare, space control, space force enhancement, and computer network operations.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

use of GPS, its augmentations, or any other PNT service; and preserving peaceful civil GPS use outside an area of military operations" (§3.2.3).

The US has introduced three additional coded signals to support future civil applications. One of these (L1C) is at full operational capability for accuracy, integrity, continuity, and availability. The other two (L2C and L5) are operationally capable only for accuracy and integrity (DoD et al. 2022, §3.2.6.1). Military signals will be supplemented in the future with a next-generation GPS signal (M-code), which is encrypted and spectrally separated from civilian signals and other radionavigation satellite service signals. This will significantly improve exclusivity of access and enhance NAVWAR operations. When tracking encrypted military signals, military GPS receivers are "much more resistant to interference than commercial GPS equipment" (§3.2.6.2).

The Department of Defense has been modernizing its use of GPS for the past twenty years with M-code, a more jam-resistant, encrypted, military-specific signal, which is essential to maintain GPS "effectiveness in the face of adversary threats" (DoD et al. 2022, §5.1.1; GAO 2024, 1). M-code is designed to meet military PNT information needs and will help military users overcome attempts by adversaries to jam GPS signals "by using a more powerful signal with a broader radio frequency range" (GAO 2024, 3). M-code will also protect against spoofing "by providing enhanced encryption for the signal" (4).

M-code modernization requires a "ground control system that can enable the launch and control of existing and new, more powerful satellites" (GAO 2024, 4). The first satellite able to broadcast the M-code signal was launched by the US Air Force in 2005. As of May 2024, twenty-four of thirty-one "satellites in the GPS constellation were M-code-capable" (5). The Department of Defense will also need to "upgrade existing weapon systems and platforms with M-code capable" GPS receivers (6). In short, GPS enhancement efforts continue to include modernizing ground control systems, upgrading satellites, and integrating user equipment with platforms to receive the M-code signal, but significant challenges remain for each segment (6).

6.3.3.3 National Research and Development Plan for PNT Resilience

Numerous systems used in multiple sectors of US critical infrastructure rely solely on GNSS/GPS for PNT services. Many of these systems are not designed or tested to respond effectively to the disruption and manipulation of PNT services and are therefore at an elevated risk of interference. Such interference "could compromise national security, increase the risk of loss of life, severely impact the economy, and disrupt the daily activities of the American people" (NSTC 2021, 3). Interference or loss of PNT services can also potentially impede mitigation and recovery efforts.

To be resilient, a PNT enterprise must (1) use multiple, diverse sources of PNT and data paths; (2) use an architecture that minimizes "attack opportunities and

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

overlapping attack vectors that could reduce protections or result in single points of failure"; (3) apply defense-in-depth ("multiple layers of protections, mitigations, and responses"); and (4) integrate "modern cybersecurity principles into the greater PNT enterprise" (NSTC 2021, 3). The PNT enterprise must also be capable of (1) delivering and using PNT in "physically or electronically impeded environments"; (2) consistently providing "higher accuracy with greater assurance"; (3) providing "notification of degraded or misleading information"; (4) providing PNT services at high altitudes and in space; and (5) developing "adequate modeling and simulation capabilities, including capabilities to predict how PNT services are affected in urban environments" (NSTC 2021, 3).

The US R&D plan supports "three overarching goals for greater PNT service resilience and prioritizes fourteen R&D objectives for further R&D across these overarching goals" (NSTC 2021, 5). Agencies should:

1 characterize and model current and future PNT system and service capabilities, performance characteristics, vulnerabilities, and the projected future needs of PNT users (7–8);
2 work to improve and expand PNT services and capabilities across the enterprise by developing PNT equipment with better performance specifications (such as accuracy, availability, continuity, coverage, and integrity) to enable greater resilience, as well as innovations (such as size, weight, power consumption, and cost) to motivate its adoption (9–11); and
3 integrate and deploy resilient PNT architectures through the development of prototype systems and demonstrations (12–14).

6.3.3.4 Memorandum on Space Policy Directive 7

Space Policy Directive 7 provides implementation actions and guidance for US space-based PNT programs and activities for US national and homeland security, civil, commercial, and scientific purposes, including:

a the sustainment and modernization of the GPS and federally developed, owned, and operated systems used to augment or otherwise improve GPS;
b the implementation and operation of capabilities to protect US and allied access to and use of GPS for national, homeland, and economic security, and to deny adversaries from the use of US space-based PNT services; and
c US participation in international cooperative initiatives regarding foreign space-based PNT services and the foreign use of GPS and its augmentations (White House 2021).

The US will "improve and maintain GPS and its augmentations to meet growing national, homeland, and economic security requirements as well as other civil

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

requirements, and to enable diverse commercial and scientific applications" (White House 2021, §3). It will also "improve capabilities to deny adversary access to space-based PNT services, particularly including services that are openly available and can be readily used by adversaries or terrorists, to threaten the security of the United States." In addition, the US will encourage the responsible use of PNT service "acquisition, integration, and deployment across critical infrastructure" (§3). Additionally, the US is developing "alternative approaches to PNT services and security that can incorporate new technologies and services …, such as quantum sensing, relative navigation and private or publicly owned and operated alternative PNT services" (§3).

To maintain US leadership in service provision and the responsible use of GPS and foreign systems, the US shall (inter alia):

a provide continuous worldwide access to US space-based GPS services and government-provided augmentations, free of direct user fees, and provide open, free access to information necessary to develop and build equipment to use these services;
b improve NAVWAR capabilities to deny the hostile use of US space-based PNT services, without unduly disrupting civil and commercial access to civil PNT services outside an area of military or homeland security operations;
c improve the performance of US space-based PNT services, including developing more robust signals that are more resistant to disruptions and manipulations consistent with US and allied national security, homeland security, and civil purposes;
d improve the cybersecurity of GPS, its augmentations, and US-owned GPS-enabled devices, and foster private sector adoption of cyber-secure GPS-enabled systems through system upgrades and the incorporation of cybersecurity principles for space systems, interface specifications, and other guidance that prescribes cybersecurity for user equipment;
e protect the spectrum environment that is currently used by GPS and its augmentations, and work with US industry to investigate additional areas of the radio spectrum that could increase GPS and PNT resilience;
f invest in domestic capabilities and support international activities to detect, mitigate, and increase resilience to the harmful disruption or manipulation of GPS, and identify and implement alternative sources of PNT for critical infrastructure, key resources, and mission-essential functions;
g maintain GPS and its augmentations for use by US critical infrastructure to enhance safety of life functions and operational efficiency;
h engage with international GNSS providers to ensure compatibility, encourage interoperability with likeminded nations, promote transparency in civil service provision, and enable market access for US industry;

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

i encourage foreign development of PNT services and systems based on GPS and the inclusion of GPS as an essential element in systems that integrate multiple PNT services;
j seek to ensure that all foreign systems are compatible with GPS and its augmentations, that they do not interfere with GPS military and civil signals, and that mutual security concerns are addressed to prevent the hostile use of US space-based PNT services;
k promote the responsible use of US space-based PNT services and capabilities; and
l promote US technological leadership in the provision of space-based PNT services and in the development of secure and resilient end-user equipment (White House 2021, § 4).

The Secretary of Defense is responsible for (inter alia) (1) developing, acquiring, operating, testing, evaluating, and maintaining NAVWAR capabilities and other capabilities to allow for the effective use of GPS services "in the event of an adversary or other jamming, disruption, or manipulation"; (2) developing "effective measures to counter adversary efforts to deny, disrupt, or manipulate PNT services"; and (3) identifying, locating, and mitigating (in coordination with other agencies) any "intentional disruption or manipulation that adversely affects use of GPS for military operations" (White House 2021, §7).

The Secretary of Commerce shall (inter alia), in cooperation with other agencies, "develop guidelines to improve the cybersecurity of PNT devices, including their capability to detect and reject manipulated or counterfeit signals, and promote the responsible use of space-based PNT services and capabilities for applications that support national security, economic growth, transportation safety, and homeland security" (White House 2021, §7). The Secretary of Transportation shall (inter alia), in coordination with the Secretaries of Defense and Homeland Security and other agencies, implement federal "capabilities to monitor, identify, locate, and attribute space-based PNT service disruption and manipulations within the US that adversely affect use of space-based PNT for transportation safety, homeland security, civil, commercial, and scientific purposes" (§7).

The Secretary of Homeland Security – in coordination with the Secretaries of Defense and Transportation, and in cooperation with the Secretary of Commerce – is responsible for (inter alia) (1) ensuring that "mechanisms are in place to monitor, identify, locate, and attribute space-based PNT service disruptions and manipulations within the US that can cause significant disruption to United States critical infrastructure and scientific purposes"; and (2) developing procedures to notify all stakeholders when space-based services have "anticipated disruptions or are deemed to be no longer reliable" (White House 2021, §7). The Secretary of Homeland Security shall also, in coordination with the Secretaries of Defense, Commerce, and Transportation, "develop and maintain capabilities, procedures, and techniques

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

for, and routinely exercise, civil contingency responses to ensure continuity of operations in the event that access to GPS services are disrupted or manipulated" (§7). Additionally, the Secretary of Homeland Security shall, in coordination with the Secretaries of Defense and Transportation, and in cooperation with other agencies, "coordinate the use of existing and planned capabilities to identify, locate, and attribute any disruption or manipulation of GPS and its augmentations within the United States that significantly affects homeland security or critical infrastructure" (§7). Finally, the Secretary of Homeland Security is also responsible for notifying the interagency of any significant domestic or international disruption to or manipulation of US space-based PNT services "to enable appropriate investigation, notification, or enforcement action" (§7).

Any agency that detects or receives a report of harmful disruption or manipulation of US space-based PNT services shall provide a timely report to the Secretaries of Homeland Security, Defense, and Transportation, and to the Director of National Intelligence (White House 2021, §8). When notified, the Secretary of Commerce and the Chairman of the Federal Communications Commission (in cooperation with other federal agencies) shall take appropriate action to mitigate harmful disruption or manipulation of US space-based PNT services within the US. The Secretary of State is responsible for notifying foreign governments and international organizations when there is a harmful disruption or manipulation of US space-based PNT services caused by foreign government or commercial activities (§8).

6.3.3.5 National Security Memorandum NSM-22

The US is in an era of strategic competition with nations that target US critical infrastructure and enable malicious actions by non-State actors. If there is a crisis or conflict, US adversaries will increase their efforts to compromise critical infrastructure to undermine the will of the American public and threaten the projection of US military power. NSM-22 recognizes that the incapacity or destruction of US critical infrastructure will have a debilitating impact on national security, national economic security, and national public health or safety (White House 2024). The US will therefore increase its efforts to strengthen and maintain a secure, functioning, and resilient critical infrastructure.

Strengthening the security and resilience of America's critical infrastructure will be consistent with the following principles:

1 **Shared responsibility.** Safeguarding critical infrastructure is a shared responsibility among all stakeholders and requires public–private collaboration.
2 **Risk-based approach.** National efforts must be prioritized based on the relationship between specific infrastructure and national security, national economic security, national public health or safety, and the government's ability to perform essential functions and services. Risk assessments must consider all threats and hazards, likelihoods, vulnerabilities,

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

and consequences, including shocks and stressors – as well as the scope and scale of dependencies within and across critical infrastructure sectors, the immediate and long-term consequences, and the cascading effects.

3 **Minimum requirements.** All government entities are responsible for prioritizing the establishment and implementation of minimum requirements for risk management.
4 **Accountability.** Robust accountability and enforcement mechanisms from all government and private sector entities, as well as independent third parties, are essential for effective risk management for critical infrastructure.
5 **Information exchange.** The sharing of timely, actionable information among all stakeholders is essential for effective risk management, which will be facilitated by the federal government.
6 **Expertise and technical resources.** The federal government will leverage expertise and technical resources from all relevant federal departments and agencies to mature the capacity and capability of each federally led effort to manage sector-specific risk to secure US critical infrastructure.
7 **International engagement.** The federal government will work closely with international partners to strengthen the security and resilience of the international critical infrastructure on which the US depends.
8 **Policy alignment.** Efforts to safeguard critical infrastructure will be aligned with complementary federal policies and frameworks.

Objectives under the national effort to strengthen the security and resilience of US critical infrastructure include:

1 refine and clarify the roles and responsibilities of the federal government for critical infrastructure security, resilience, and risk management;
2 identify and prioritize critical infrastructure security and resilience based on risk and implement a coordinated national approach to assess and manage sector-specific and cross-sector risk;
3 establish minimum requirements and accountability mechanisms for the security and resilience of critical infrastructure, including through aligned and effective regulatory frameworks;
4 leverage federal government agreements, including grants, loans, and procurement processes, to require or encourage owners and operators to meet or exceed minimum security and resilience requirements;
5 enhance and improve the quality of intelligence collection and analysis pertaining to threats to critical infrastructure;
6 improve the real-time sharing of timely, actionable intelligence and information at the lowest possible classification level among federal,

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

State, local, Tribal, territorial, private sector, and international partners to facilitate risk mitigation to critical infrastructure;

7 promote timely and cost-effective investments in technologies and solutions that mitigate risk from evolving threats and hazards to critical infrastructure; and

8 strengthen the security and resilience of critical infrastructure by engaging international partners and allies to build situational awareness and capacity, facilitate operational collaboration, promote effective infrastructure risk management globally, and develop and promote international security and resilience recommendations.

The federal government will use a risk-based approach to reduce risk to critical infrastructure. Critical infrastructure risks will be assessed in terms of threats or hazards, vulnerability, and consequence. Risk management efforts will be prioritized by identifying the criticality of assets and systems within and across sectors. Nonfederal critical infrastructure owners and operators are primarily responsible for managing most risks to their operations and assets. The federal government shall support and guide the entities that own, operate, or otherwise control critical infrastructure assets and systems by providing these entities with the information, intelligence analysis, and other support to manage and mitigate asset-level risks.

The federal government, in coordination with owners and operators, will identify, assess, prioritize, mitigate, and monitor risks that may have a potentially debilitating impact on national security, national economic security, or public health or safety. These nationally significant risks may arise within and impact sectors or cut across multiple sectors. The federal government is responsible for identifying and mitigating national-level risk through a whole-of-government effort, led by the Department of Homeland Security in coordination with Sector Risk Management Agencies (SRMAs) and supported by other federal departments and agencies.

SRMAs are responsible for the day-to-day prioritization and coordination of efforts to mitigate risks within each sector, as part of the broader whole-of-government effort. The National Coordinator shall manage systemic and cross-sector risk by working with SRMAs, federal departments and agencies, and industry to identify, analyze, prioritize, and manage the most significant risks involving multiple sectors based on data provided by the SRMAs.

Effective risk management requires the adoption of minimum security and resilience requirements within and across critical infrastructure sectors. The Department of Homeland Security, including the National Coordinator, SRMAs, and regulators, shall coordinate to produce cross-sector and sector-specific guidance, performance goals and metrics, and requirements to adequately mitigate risk. SRMAs, in coordination with regulators, shall develop sector-specific minimum security and resilience requirements for each respective sector and a plan to use existing authorities or other tools to implement those requirements effectively. The National Coordinator shall

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

review proposed sector-specific security and resilience guidance, performance goals, and requirements in coordination with SRMAs, and in consultation with regulators, to facilitate the harmonization of these directives and recommendations at the national and cross-sector level.

The federal government will collaborate with private-sector partners; State, local, Tribal, and territorial governments; community organizations; and international partners that can take actions that provide resilience and security benefits to owners and operators in the US and other countries.

Every two years, the Secretary of Homeland Security shall develop and submit to the president a National Infrastructure Risk Management Plan, which shall be informed by (1) individual sector-specific risk assessments and risk management plans; and (2) a cross-sector risk assessment. Each SRMA shall develop sector-specific risk assessments and sector-specific risk management plans based on strategic directions provided by the Secretary of Homeland Security. Sector-specific risk assessments will identify the most significant critical infrastructure risks to their sector, including key cross-sector risks and interdependencies.

Sector-specific risk management plans will be developed or refreshed every two years to leverage individual SRMA tools and authorities, as well as other federal tools and authorities, to safeguard critical infrastructure in each sector from all threats and hazards, considering national-level priorities and guidance from the Secretary of Homeland Security. The National Coordinator shall develop a cross-sector risk assessment in coordination with SRMAs identifying the most significant cross-sector risks to US critical infrastructure.

Based on the sector-specific risk assessments and risk management plans and the cross-sector risk assessment, the Secretary of Homeland Security shall develop and submit to the president, through the assistant to the president and the Homeland Security Advisor, the National Infrastructure Risk Management Plan to guide the federal effort to mitigate cross-sector and other national risks to critical infrastructure. The plan shall prioritize specific cross-sector risks, with a focus on new and emerging threats to critical infrastructure, and shall identify innovative approaches to limit the risks from these new and emerging threats, particularly risk mitigation strategies for increasingly interdependent and interconnected assets and systems.

The National Coordinator shall regularly identify organizations (Significantly Important Entities – SIEs) that own, operate, or otherwise control critical infrastructure that is prioritized based on the potential for its disruption or malfunction to cause nationally significant and cascading negative impacts to national security, national economic security, or national public health or safety. The SIE list shall inform the prioritization of federal activities, including the provision of risk mitigation information and other operational resources to nonfederal entities.

Critical infrastructure risk management requires those who own or operate infrastructure to be informed of a wide range of threats that are manmade or result

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

from natural hazards, including by the actionable and timely intelligence and information available on those threats or hazards. To establish a comprehensive, integrated threat picture for US critical infrastructure, the Director of National Intelligence shall lead Intelligence Community efforts, in consultation with the Department of Homeland Security, including the National Coordinator, SRMAs, and relevant departments and agencies, to collect, integrate, analyze, and share information from intelligence reporting, data, and assessments to understand and identify threats to critical infrastructure and disseminate intelligence reports in an accessible, usable, and shareable format for nonfederal stakeholders.

The Director of National Intelligence shall also produce, receive, integrate, and share information, to include information from intelligence assessments and warnings, that enables federal department or agency leadership to consider the widest possible options for mitigating a risk or addressing a threat, including the coordinated balancing of national interests, stakeholder equities, and authorities. The Director of National Intelligence shall also establish, in coordination with the Department of Homeland Security and the Department of Justice, a process to ensure that Intelligence Community elements provide timely notification to appropriate federal elements, including the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and relevant SRMAs, when Intelligence Community elements are aware of specific and credible threats to US critical infrastructure.

6.3.3.6 Maritime Administration Guidance

To mitigate GNSS interference, MARAD advises ships operating in the Persian Gulf and the Strait of Hormuz to review security measures, ensure that AIS is always transmitting, and monitor VHF Channel 16. US-flagged vessels are also encouraged to register with the UKMTO, the International Maritime Security Construct (IMSC), and US Fifth Fleet Naval Cooperation and Guidance for Shipping (NCAGS) Watch (if activated) when entering the Indian Ocean Voluntary Reporting Area. Additionally, vessels are advised to provide their transit plans for the Strait of Hormuz and the Persian Gulf to the UKMTO, the IMSC, and NCAGS Watch to include the time of entering or exiting the Strait of Hormuz Traffic Separation Scheme, an outline of the navigation plan for operating in the strait and the gulf, and speed restrictions or other constraints.

In the event of an incident or suspicious activity (such as being hailed from a source falsely claiming to be a US or coalition naval vessel), vessels should call the UKMTO, the IMSC, or the US Fifth Fleet Battle Watch and activate the Ship Security Alert System immediately. In addition, all suspicious activities, breaches of security, and transportation security incident events must be reported to the USCG National Response Center (MARAD 2023a, 2023b). Maritime GPS disruptions or anomalies should be reported immediately to the USCG NAVCEN (MARAD 2023a, 2023b).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Prior to getting underway, ships should review the NAVCEN and NATO Shipping Center websites, which contain information regarding safe navigation practices for vessels experiencing GPS interference. The websites also provide useful guidance on reporting disruptions, which will generate further discussion within the maritime industry about disruption mitigation practices and procedures. Incidents of disruption should be reported in real time, noting the location (latitude and longitude), date, time, and duration of the outage/disruption and providing photographs or screenshots of equipment failures experienced to facilitate analysis (MARAD 2023a).

6.3.4 *Alternative Mitigation Systems and Technologies*

Satellite Time and Location (STL) is an alternative navigation system that operates on the Iridium satellites and offers "an encrypted signal, 1000 times stronger than GNSS that resists jamming and spoofing" (McCrystal 2018). STL is not as accurate as GNSS, but "it provides 30–50 meter accuracy which can serve as a check to the GNSS indicated position or time" (McCrystal 2018). STL therefore provides ships with an "additional signal authenticating tool" that can be used to validate communication and network access (McCrystal 2018). Because it uses an encrypted signal, "the vessel has an irrefutable PNT source" that can be trusted to reflect that the "vessel was in a certain location at a certain time and that communications to and from the vessel are genuine" (McCrystal 2018). STL can also be "combined with an Inertial Navigation System (INS)," which provides "valuable range and Doppler updates to the inertial measurements, reducing drift and maintaining a proper navigation solution, even during extended periods of GNSS denial" (McCrystal 2018).

Navigation Protection Devices (NPDs) include "a monitoring component, such as Orolia's NPD Broad Shield, which monitors GNSS receptions, analyses the signals, and alerts the pilot on the bridge" (McCrystal 2018). The device "is independent of the vessel's navigation system and interfaces with the ECDIS display . . . to give real time indication of alerts and positional discrepancies" (McCrystal 2018). Broad Shield is also capable of sending "alarms or warnings in other forms for vessels not equipped with an ECDIS" (McCrystal 2018).

If available, eLoran can provide an alternative signal for NPDs. GNSS and eLoran are at opposite ends of the spectrum – "low frequency instead of microwave; high-power pulse instead of low power spread spectrum; and terrestrial instead of space-based" (McCrystal 2018). Jammers used to block GNSS are different from those capable of blocking eLoran, thereby adding resiliency to navigation.

An NPD will activate if there are additional signals present in the GNSS band or there is an anomalous behavior of the signal; if the NPD determines that the "navigation solution does not match the ship's GNSS guidance solution due to equipment malfunction or malicious signals"; or if the NPD detects "that the navigation solution differs from the GNSS constellations and its alternatives sources, such as STL or eLoran" (McCrystal 2018).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Veripos GAJT-710MS, an anti-jamming technology developed by Hexagon Autonomy & Positioning, mitigates GPS interference by "creating nulls in the antenna gain pattern in the direction of the jammers" (Wingrove 2020). The hardened enclosure contains an antenna array and null-forming electronics and can be installed on a wide variety of vessels. Inertial instruments provide an additional alternative to GPS. Sonardyne International installed a Sprint-Nav hybrid inertial navigation instrument on a British Sea-Kit X-class unmanned surface vessel and tested it against local real-time kinematic GPS positioning.

A US company – Zephr – that specializes in developing tools to protect against GPS signal interference is conducting field tests in Ukraine using cell phones loaded with special software to locate Russian jamming equipment (Tucker 2024). The tests show that "by comparing the GPS reception of various phones" working together in a network, they could detect when one or more of the phones was being attacked (Tucker 2024). Zephr is also conducting field experiments to not only "detect jammers but triangulate their positions so the jammer can be avoided or eliminated" (Tucker 2024). The location of a jammer can be determined using three inputs:

1 localization by range inferred from power;
2 localization by area of effect; and
3 triangulation of jammers based on angle of arrival (Tucker 2024).

Laser can also be used to augment "GNSS services with measurements of range and bearing to a set of geographically referenced reflectors." The CyScan GeoLock sensor, produced by Wärtsilä's Guidance Marine, "provides position references without risk of spoofing, interference or loss of signal" by using lasers rather than satellites (Tucker 2024). The system is used to maneuver vessels in port, terminals, or offshore drilling rigs. As the ship approaches the port, the CyScan GeoLock sensor automatically starts tracking the vessel. The system then "compares the geometric pattern produced by its range and bearing measurements of detected reflectors with the corresponding geometric pattern of the surveyed reflectors in the configuration file" (Tucker 2024). Once a match is found, "the reflectors are accepted into the sensor's tracking solution" and the sensor produces a position reference (Tucker 2024).

The French are also experimenting with laser technology to mitigate against GPS jamming. In September 2024, a project funded by the French Defence Innovation Agency successfully used a laser to establish a stable link between a low-orbit nano satellite and an optical ground station for several minutes (Ruitenberg 2024). Lasers have the capability to transfer very large files (such as Earth images) quickly. Because of their point-to-point nature, lasers are "more secure than radio frequencies" and less susceptible to jamming (Ruitenberg 2024). Lasers have a low probability of detection and interception, so putting them on ships reduces the radio footprint of the ship that is normally associated with an RF antenna. The successful

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

test will allow France to integrate the laser technology on its future military satellites and use space-based laser communications on "mobile, land-based, naval and airborne platforms" (Ruitenberg 2024). A Defense Ministry spokesperson explained:

> Advantages of the optical link over the usual radio link are its speed, discretion and independence from regulations that coordinate the use of radio waves. Even if . . . [the] optical link can sometimes be perturbed by atmospheric turbulence, the . . . satellite is able to circumvent them . . . to achieve optimum transmission quality. (MacKenzie 2024)

China is also developing laser communication technology. In mid-September 2024, China successfully deployed a laser communication ground system with a 500-mm-caliber antenna, which will significantly enhance China's "capacity for massive satellite data transmission" (Xinhua 2024). Once the technology becomes fully operational, China will no longer have to rely "solely on microwave ground stations for satellite data reception" (Xinhua 2024). Satellite-to-ground laser communications have between ten and a thousand times wider bandwidth than microwave communications. The system is also smaller and lighter, and it consumes less power.

The Royal Navy and the US Department of Defense are conducting experiments to develop "quantum navigation." This new technology would allow for GPS-free navigation. Once perfected, quantum technologies will not be susceptible to spoofing or jamming, thus providing a 100 percent "resilient satellite-free capability" (MI News Network 2024; see also Advanced Navigation 2024; Tucker 2021; Vallance 2024).

An American company – SandboxAQ – has developed an AI-enabled navigation system (AQNav) that uses "quantum sensors to gather data from the Earth's crustal magnetic field" and AI algorithms that eliminate potential interference from jamming and spoofing.[11] This technology enables the system to "provide real-time navigation in areas where GPS signals are denied or unavailable" (Saballa 2024). AQNav can be installed on civilian or military air, land, and sea platforms and could be "used to improve autonomous vehicle control or aid in underground/underwater operations where GPS signals are unavailable" (Saballa 2024).

6.4 CONCLUSION

There is now a growing awareness of the vulnerability of GNSS, but it is not yet clear what to do about it. Although there is no single solution that can address all the vulnerabilities associated with GNSS, by combining several alternative methods, GNSS can be augmented and thereby "provide the resilience necessary for all critical operations" to include PNT for maritime navigation (McCrystal 2018).

[11] The Earth's crustal magnetic field is a "highly reliable data source for navigation" because it provides a persistent, passive external signal (Saballa 2024).

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Resilient PNT receivers can identify and operate through jamming and spoofing attacks, adjust to an additional PNT source that is not experiencing interference, provide longer PNT solutions without receiving updates from trusted PNT services, and thus avoid unacceptable degradation in performance (NSTC 2021, 4).

A resilient PNT enterprise will use various sources of PNT and data paths. The PNT architecture must be able to minimize attack opportunities and attack vectors that degrade services or result in a single point of failure. Defense-in-depth (numerous layers of protection, mitigation, and response) is essential, as well as the integration of "modern cybersecurity principles into the greater PNT enterprise" (NSTC 2021, 3). Resilient PNT enterprises must be able to deliver and use PNT in physically or electronically degraded environments. They must also consistently provide "higher accuracy with greater assurance" and provide "notification of degraded or misleading information" (3).

As intentional interference by rogue States and non-State actors continues to increase, cyber security designed to mitigate the disruption of PNT services used by navigation and communication systems is more important than ever to ensure safety at sea. Conducting regular risk assessments can identify system vulnerabilities and prioritize mitigation strategies. Having a clear incident response plan in place can also help respond to cyberattacks and "minimize damage and expedite recovery" (Chua 2024). The use of intrusion detection and prevention systems "allows for real-time monitoring of network activity and enables the detection of suspicious activity." It will also be important to leverage and deploy new and emerging technologies – such as M-code, quantum navigation, anti-jamming technology, and lasers – as they become available to mitigate or eliminate the threat of cyberattacks more effectively.

REFERENCES

Advanced Navigation. 2024. "The Future of Inertial Navigation Is Classical-Quantum Sensor Fusion." June 7. www.advancednavigation.com/tech-articles/the-future-of-inertial-navigation-is-classical-quantum-sensor-fusion.

AFP (Agence France Presse). 2020. "Ecuador Says Chinese Trawlers Turned Off Tracking System Near Galapagos." *Barron's*, August 18. www.barrons.com/news/ecuador-says-chinese-trawlers-turned-off-tracking-system-near-galapagos-01597802704.

Alberts, Elizabeth Claire. 2020. "New Evidence Suggests China's 'Dark' Vessels Poached in Galápagos Waters." *Mongabay*, October 9. www.news.mongabay.com/2020/10/new-evidence-suggests-chinas-dark-vessels-poached-in-galapagos-waters.

Bergman, Bjorn. 2019. "Systematic GPS Manipulation Occurring at Chinese Oil Terminals and Government Installations." *SkyTruth*, December 12. https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/.

Browne, Ryan, and Barbara Starr. 2019. "US Government Warns of Iranian Threats to Commercial Shipping, Including GPS Interference." *CNN*, August 7. https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/index.html.

C4ADS. 2019. "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria." https://c4ads.org/reports/above-us-only-stars/

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Chua, Joey. 2024. "Navigating through the Storm: Cybersecurity and Its Stakeholders." *Maritime Executive*, April 23. https://maritime-executive.com/editorials/navigating-through-the-storm-cybersecurity-and-its-stakeholders.

Coats, Daniel R. 2017. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence." May 11. www.intelligence.gov/assets/documents/archive/SASC%202017%20ATA%20SFR%20-%20FINAL.PDF

DoD, DoT and DHS (US Department of Defense, Department of Transportation, and Department of Homeland Security). 2022. "2021 Federal Radionavigation Plan." www.navcen.uscg.gov/sites/default/files/pdf/2021_Federal_Rdionavigation_Plan.pdf.

GAO (US Government Accountability Office). 2024. *GPS Modernization: Delays Continue in Delivering More Secure Capability for the Warfighter*. Report to Congressional Committees, GAO-24-106841.

Goward, Dana. 2017. "Mass GPS Spoofing Attack in Black Sea?" *Maritime Executive*, July 11. https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

2019. "Chinese GPS Spoofing Circles Could Hide Iran Oil Shipments." *GPS World*, December 17. www.gpsworld.com/chinese-gps-spoofing-circles-could-hide-iran-oil-shipments/.

2020. "GPS Circle Spoofing Discovered in Iran." *GPS World*, April 21. www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/.

IMO (International Maritime Organization). 1991. "General Requirements for Shipborne Radio Equipment Forming Part of the Global Maritime Distress and Safety System (GMDSS) and for Electronic Navigational Aids." A 17/Res.694 (November 25, 1991).

2011. "Worldwide Radionavigation System." A 27/Res.1046 (December 20, 2011).

2015. "Performance Standards for Multi-System Shipborne Radionavigation Receivers." MSC 95/22/Add.2, Annex 17 (June 8, 2015).

2017a. "Guidelines for Shipborne Position, Navigation, and Timing (PNT) Data Processing." MSC.1/Circ.1575 (June 16, 2017).

2017b. "Guidelines on Maritime Cyber Risk Management." MSC-FAL.1/Circ.3 (July 5, 2017).

2017c. "Maritime Cyber Risk Management in Safety Management Systems." MSC 98/23/Add.1, Annex 10 (June 16, 2017).

2022. "Guidelines on Maritime Cyber Risk Management." MSC-FAL.1/Circ.3/Rev.2 (June 7, 2022).

INTERTANKO. 2019. "Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)." www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf.

ITU (International Telecommunication Union). 2020. "Radio Regulations." www.itu.int/hub/2022/08/warning-harmful-interference-rnss/.

ITU News. 2022. "ITU Issues Warning on Interference with Radio Navigation Satellite Service." August 23. www.itu.int/hub/2022/08/warning-harmful-interference-rnss/.

Joffre, Tzvi. 2019. "U.S. Warns of GPS Interference, Communications Spoofing in Persian Gulf." *Jerusalem Post*, August 8. www.jpost.com/Middle-East/US-warns-of-GPS-interference-communications-spoofing-in-Persian-Gulf-597998.

Lo, Chris. 2019. "GPS Spoofing: What's the Risk for Ship Navigation?" *Ship Technology*, April 15. www.ship-technology.com/features/ship-navigation-risks/?cf-view.

MacKenzie, Cristina. 2024. "France Claims World's First Space-to-Earth Laser Comms." *Breaking Defense*, September 23. https://breakingdefense.com/2024/09/france-claims-worlds-first-space-to-earth-laser-comms/.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

MARAD (US Maritime Administration). 2019. "MSCI Advisory 2019-012 – Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea – Threats to Commercial Vessels by Iran and Its Proxies." www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels.

2023a. "MSCI Advisory 2023-005 – Various – GPS Interference & AIS Spoofing." www.maritime.dot.gov/msci/2023-005-various-gps-interference-ais-spoofing.

2023b. "MSCI Advisory 2023-011 – Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Gulf of Aden, Bab al Mandeb Strait, Red Sea, and Somali Basinx – Threats to Commercial Vessels." www.maritime.dot.gov/msci/2023-011-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-gulf-aden-bab-al-mandeb-strait-red.

McCrystal, Sean. 2018. "Detecting and Defeating GPS Jamming." *Maritime Executive*, February 16. https://maritime-executive.com/blog/detecting-and-defeating-gps-jamming.

MI News Network. 2024. "Royal Navy Works on GPS-Free Technology for Advanced Navigation at Sea." *Marine Insight*, February 21. www.marineinsight.com/shipping-news/royal-navy-works-on-gps-free-technology-for-advanced-navigation-at-sea/.

NSTC (National Science and Technology Council). 2021. "National Research and Development Plan for Positioning, Navigation, and Timing Resilience." https://bidenwhitehouse.archives.gov/wp-content/uploads/2021/08/Position_Navigation_Timing_RD_Plan-August-2021-1.pdf.

Pedrozo, Raul (Pete). 2022. "China's IUU Fishing Fleet: Pariah of the World's Oceans." *International Law Studies* 99: 319–353.

Quinn, Áine. 2024. "Ukraine Warns Ships of Scrambled GPS Navigation in Black Sea." *gCaptain*, June 20. https://gcaptain.com/ukraine-warns-ships-of-scrambled-gps-navigation-in-black-sea/.

Ramos Miranda, Natalia A. 2020. "Chile Keeps Eye on Chinese Fishing Fleet along South American Coast." *Reuters*, October 8. www.reuters.com/article/uschile-fishing-china-idUSKBN26T3IL.

Ruitenberg, Rudy. 2024. "France Tests Space Lasers for Secure Satellite Downlink in World First." *Defense News*, September 13. www.defensenews.com/global/europe/2024/09/13/france-tests-space-lasers-for-secure-satellite-downlink-in-world-first.

Rust, Susanne. 2020. "Tensions Rise in Ecuador and Peru as Chinese Fishing Fleet Moves South from Galapagos." *Los Angeles Times*, September 23. www.latimes.com/environment/story/2020-09-23/tensions-rise-in-ecuador-and-peru-as-chinese-fishing-fleetmoves-south-from-galapagos.

Saballa, Joe. 2024. "US Firm Develops AI-Enabled, Anti-GPS Jamming Navigation System." *Defense Post*, June 27. https://thedefensepost.com/2024/06/27/us-ai-navigation-system/.

Satherley, Dan. 2020. "Chinese Fishing Flotilla in Galapagos Accused of Pretending to Be in New Zealand." *Stuff*, August 6. www.stuff.co.nz/nz-news/350543267/chinese-fishing-flotilla-in-galapagos-accused-of-pretending-to-be-in-new-zealand.

Schuler, Mike. 2024. "Vessel Reports 'Electronic Interference' Incident in Persian Gulf." *gCaptain*, April 3. https://gcaptain.com/vessel-reports-electronic-interference-incident-in-persian-gulf/.

Sheppard, David, Demetri Sevastopulo, and Lucy Hornby. 2019. "US Identifies Chinese Tankers Carrying Iranian Oil." *Financial Times*, August 4. www.ft.com/content/62220484-b37c-11e9-8cb2-799a3a8cf37b.

Singhi, Anjali, Edward Wong, and Denise Lu. 2019. "Defying U.S. Sanctions, China and Others Take Oil from 12 Iranian Tankers." *New York Times*, August 3. www.nytimes.com/interactive/2019/08/03/world/middleeast/us-iran-sanctions-ships.html.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press

Sutton, H. I. 2021. "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base." *USNI News*, June 21. https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.

Telling, Oliver. 2024. "Cyber Attacks on Shipping Rise amid Geopolitical Tension." *Financial Times*, July 28. www.ft.com/content/c05c9b21-77bd-4ddf-82e1-02356acf0899.

Tucker, Patrick. 2021. "Quantum Sensor Breakthrough Paves Way for GPS-Free Navigation." *Defense One*, November 2. www.defenseone.com/technology/2021/11/quantum-sensor-breakthrough-paves-way-gps-free-navigation/186578/.

2024. "In Ukraine, a US Firm Tests a Promising Tool against GPS Jammers: Cell Phones." *Defense One*, September 30. www.defenseone.com/technology/2024/09/group-ukraine-testing-newest-weapon-against-gps-jammers-cell-phones/399952/.

Vallance, Chris. 2024. "Unjammable Navigation Tech Gets First Airborne Test." *BBC*, May 13. www.bbc.com/news/articles/cz744gpl1dpo.

White House. 2021. "Memorandum for the Vice President: Space Policy Directive 7, The United States Space-Based Positioning, Navigation, and Timing Policy." Trump White House, January 15. https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/.

2024. "National Security Memorandum on Critical Infrastructure Security and Resilience." NSM-22 (April 30, 2004). https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

Wingrove, Martyn. 2020. "How Shipping Mitigates GPS Jamming and Spoofing." *Riviera*, July 9. www.rivieramm.com/news-content-hub/news-content-hub/how-shipping-mitigates-gps-jamming-and-spoofing-60193.

Xinhua. 2024. "China Builds Laser Communication Ground Station for Massive Satellite Data Transmission." *Xinhua*, September 15. https://english.news.cn/20240915/2718ac48dea946ad9a9b6914ed02add3/c.html.

Zeng Xiaojun, Katie. 2021. "Background: GNSS Spoofing in China and Beyond." *Risk Intelligence*, June 29. www.riskintelligence.eu/background-and-guides/background-gnss-spoofing-in-china-and-beyond.

https://doi.org/10.1017/9781009760171.012 Published online by Cambridge University Press