FOIL
FORUM OF INSURANCE LAWYERS

Informing Progress - Shaping the Future

FOIL Update 12th August 2025

Navigating Cyber Threats at Sea: Implications for Shipping and Maritime Insurance

Approximately 80% of the world's trade is transported by sea, making shipping a driving force behind the global economy. The efficient and cost-effective transportation of over 12 billion tonnes of goods, ranging from raw materials to manufactured products, has made maritime transportation integral to international commerce. With the industry projected to grow at more than 2% each year to 2029, its importance to global supply chains is set to increase.

Despite facing challenges arising from geopolitical instability, pandemics, climate change and other disturbances, the global shipping industry is undergoing a digital transformation driven by the integration of complex navigation systems, increased connectivity, and reliance on automated technologies. While these have delivered greater operational and cost efficiencies, it has also exposed the industry to significant cyber threats.

Among the most alarming are attacks on Global Navigation Satellite Systems (GNSS), which are satellite constellations that provide positioning, navigation and timing on a global scale, enabling vessels to track their location, speed and time. Notable GNSS systems include GPS (US), Galileo (Europe), GLONASS (Russia) and BeiDou (China). Utilising such systems offers significant benefits to the safety, efficiency and accuracy of maritime transport and operations worldwide.

However, malicious acts designed to undermine GNSS are becoming increasingly sophisticated. Spoofing and jamming, for example, create considerable risk and compromise the safety, security and commercial viability of maritime operations. These developments

pose complex underwriting challenges for insurers and demand a fresh approach to how cyber risk is assessed and managed within marine policies.

Increased Digital Dependency

Modern global shipping relies heavily on digital infrastructure to deliver the transformative efficiencies that ship owners, operators, cargo owners, port authorities and other stakeholders need throughout their operations to stay competitive.

Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), and Integrated Bridge Systems (IBS) all represent crucial components of maritime navigation that significantly impact efficiency and enable vessels to navigate international waters with safety and precision.

ECDIS replaces traditional paper charts with digital versions, offering accurate details of a ship's positioning and surroundings through real-time data integration. AIS enables the automatic exchange of crucial vessel information, helping to improve situational awareness and collision avoidance. IBS integrates various bridge systems, such as propulsion, navigation and communication, to offer centralised control and streamlined operations with enhanced safety.

However, the increased interconnectivity of digital onboard systems alongside the industry's growing dependence on satellite-based navigation has made the attack surface for malicious actors much larger. Cyber threats are no longer limited to corporate IT but have migrated into the operational technologies (OT) that oversee ship and port operations.

Spoofing and Jamming

Spoofing involves broadcasting fake GNSS signals to deceive a ship's navigation system into believing it is in a different location. Jamming, however, uses powerful radio signals emitted on the same frequency as navigation satellites to interfere with transmissions and render the GNSS data unavailable.

These practices are of particular concern due to the low set-up costs available and their high potential for severely disrupting navigation and safety. Spoofing can cause a vessel to deviate from its intended course, potentially causing groundings, collisions or illegal entry into restricted or dangerous waters. Jamming, on the other hand, can force crews to rely on manual navigation methods, increasing the risk of human error in high-traffic or geopolitically sensitive regions.

Recent incidents in high-risk areas around the world have demonstrated the growing frequency and sophistication of attacks using spoofing or jamming, prompting the International Maritime Organisation (IMO) and regional maritime authorities to issue warnings about the risk of GNSS interference in areas such as the Persian Gulf, the Eastern Mediterranean, and the South China Sea.

The increased number of incidents has an impact on military and civilian activities, suggesting misuse directed at disrupting or compromising GNSS systems to either protect or further national interests or alliances. Maritime cybersecurity experts have suggested many

more incidents may go unreported due to reputational concerns or limited onboard capabilities.

Broader Vulnerabilities

GNSS and other onboard systems are exposed to a wide range of cyber and other risks. GNSS signals travel vast distances between satellites and receivers, causing signal degradation and exposure to interference. However, signal degradation can also arise due to solar weather or satellite malfunctions, which can sometimes be mistaken for deliberate attacks.

Cyber intrusions into vessel infrastructures and networks, such as phishing attacks or malware programmes, can allow attackers to manipulate or disable GNSS receivers or bridge system inputs. Further vulnerabilities exist where malicious actors, sometimes posing as legitimate users, compromise insecure elements in the wider supply chain. This can involve navigation or communication components and systems being compromised before installation, leaving them exposed to data breaches or unauthorised access.

A lack of redundancy means many vessels have no robust contingencies to a loss of GNSS, such as inertial navigation systems or terrestrial radio navigation, leaving them unable to accurately record their position. These threats can lead to loss of situational awareness, increased navigational error, and amplified system failures, all outcomes that present multiple technical, legal and financial exposures.

An Essential Element Throughout a Vessel's Lifecycle

Integrating cybersecurity into every phase of a vessel's lifecycle is no longer optional but essential, as increased digitalisation and connectivity continue to raise new risks to maritime operations. From the earliest stages of vessel design, cybersecurity must be embedded as a core component rather than as a costly, complex retrofit. The International Association of Classification Societies (IACS) has formalised this through Unified Requirements E26 and E27, which assign shared responsibility for cyber resilience to shipyards, OEMs and shipowners.

However, current data suggests only 32% of shipowners include cybersecurity specialists in their newbuild teams, and just 17% of shipyards report sufficient in-house expertise. This lack of integration at the design stage jeopardises a vessel's future operational resilience and can also lead to non-compliance with emerging regulatory standards, undermine contractual obligations and complicate insurance coverage. Stakeholders must collaborate early to mitigate such risks and embed cybersecurity throughout a vessel's architecture to ensure a future-proofed design.

Operational resilience to cyber threats depends on decisions made during design and construction, yet many shipowners are left managing fragmented security measures across mixed fleets due to inconsistent adoption. Research highlights that only 1 in 6 shipowners know what to look for in terms of cybersecurity during vessel handover, and 93% of crew feel ill-equipped to handle real-world cyber threats.

To address this, a lifecycle-wide approach is critical, where real-time risk monitoring, robust training, incident response protocols and continuous alignment with OEMs and insurers are embedded from the outset and maintained through operation. Cybersecurity should not be treated a one-off exercise, but as a continuous effort lasting across a vessel's lifespan.

Implications for the Insurance Sector

Marine insurers must consider the challenges presented by the emerging cyber threat landscape. Among these is the need to bring greater clarity to policies to remove ambiguity. Under clause CL380, marine policies have traditionally excluded direct or indirect losses stemming from the use of computer systems as a means of inflicting harm, including under war or terrorism.

However, distinguishing between cyber attacks, criminal activities, and system failures is becoming increasingly difficult. The recent adoption of the LMA5403 and similar cyber clauses seeks to clarify these exclusions, but significant grey areas remain, particularly where spoofing or jamming relates to the launch, guidance or firing mechanism of any weapon or missile.

Coordinated cyber attacks increase the risk of accumulation across fleets, ports and global supply chains, giving rise to silent cyber exposures for many policies. This is where cyber risks are not factored into the premium or underwritten. This leaves insurers vulnerable to unexpected or unquantified claims across multiple lines of business.

The lack of relevant historical data or an established reporting format both create difficulties for insurers in modelling cyber risks. The result is that GNSS-related incidents can be underreported or misclassified, hindering the development of actuarial models and risk pricing. Additionally, technological change often outpaces regulatory and underwriting frameworks, necessitating enhanced risk assessment and innovative product development.

The dynamic nature of GNSS-related cyber threats requires proactive risk management by shipowners, operators, and insurers. Cyber defences should be multilayered in IT and OT systems, and regular audits of GNSS should be in place to assess the vulnerability to attack. The adoption of navigation redundancy will also assist in maintaining vessel navigation and safety should an incident occur.

Underwriters must assess a vessel's cyber defences and the skill levels of its crew, both in modern techniques and traditional methods, to safeguard operations in the event of GNSS issues. The vast differences in the age and technical sophistication of ships make creating uniform risk profiles very challenging. Perhaps risk assessments could feature in insurance underwriting, with premium incentives offered for vessels that demonstrate strong cyber resilience.

Regulators and the industry are beginning to address the issue; for example, the IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) mandates that cyber risk management be incorporated into the International Safety Management (ISM) Code. In addition, the United Kingdom Maritime Trade Operations (UKMTO) and the European Maritime Safety Agency (EMSA) have issued alerts and guidance on GPS

interference, particularly in regions with heightened tensions and reported increases in electronic interference.

From an industry perspective, global independent classification societies such as DNV, ABS and Lloyd's Register now provide cyber certifications and a range of services, including training, gap analysis and audits, to assist shipowners in meeting emerging standards and insurer expectations.

As the global shipping industry becomes increasingly reliant on digital systems, the threat of cyber attacks exposes vessels to heightened physical, operational, and reputational risks that can spread across global supply chains. Insurers must therefore re-examine their coverage language, pricing strategies and risk modelling approaches to help anticipate and prepare for digital threats. Any risk mitigation will require close collaboration between shipowners, underwriters, regulatory bodies and cyber experts to ensure its lasting effectiveness.