INTERNATIONAL
MARITIME
ORGANIZATION

E

MARITIME SAFETY COMMITTEEE
110th session

MSC-B1
9 August 2025
Original: ENGLISH

·

Pre-session public release: ☒

DEVELOPMENT OF CYBERSECURITY STANDARDS FOR SHIPS AND PORT FACILITIES

Proposal for of cybersecurity standards for satcom in shipping

Submitted by
Aashi Mittal
Rashpal Singh

Executive Summary

Maritime industry fully depends on the digital aspects for navigation, communication and various operations. Therefore, it is vulnerable to cyber threats. In this paper, we put light on the guidelines on SATCOM protection and proposed the methods to strengthen the SATCOM systems on board.

Maritime Autonomous Surface Ships (MASS) are ships with different methods and levels of autonomy that can be achieved through monitoring and remote control from a nearby manned ship or an onshore control centre using Artificial Intelligence and Machine Learning. Hence Cyber security becomes even more relevant. This paper endeavours to highlight the cyber security concerns taking the future also into consideration.

PROPOSALS

1. MACRA TOOLKIT

MACRA Toolkit (University of Plymouth Maritime Cyber Risk Assessment Toolkit) developed by Tam and Jones in 2019 is a practical, maritime-specific tool designed to help ship operators assess and manage cyber risks. It guides users through identifying critical assets, evaluating threats and vulnerabilities, and prioritizing risks.

1.1. The first component is Asset Identification, where all critical systems onboard a ship such as ECDIS, AIS, GMDSS and SATCOM are listed and analysed. For example- identifying that the ECDIS is essential for navigation means any cyber compromise could directly impact vessel safety.
1.2. Threat and Vulnerability Assessment where potential cyber threats such as malware infections, phishing, spoofing of GPS signals, or unauthorized access are evaluated against system to identify its weakness. For example- if the SATCOM system has outdated firmware, it becomes a vulnerability that hackers could exploit. (Hackers could send fake GPS signals called spoofing or use viruses to break into the ship's computer systems.

1.3. If the ship's software is old or not updated, it's more at risk.) Impact Assessment which evaluates the consequences of a cyber incident on safety, operations, the environment, finances. For example- a ransomware attack locking access to engine control systems could delay cargo delivery and cause financial loss.

1.4. Likelihood Rating means where the probability of each threat is judged based on past events, current exposure, and threat future probability. For example- phishing emails targeting ship crew may be rated as highly likely due to increasing cases in the industry.

2. **QUANTUM TECHNOLOGY FOR CYBER SECURITY**

2.1 Quantum Technology in Satellite Communication in the Maritime Sector. The maritime industry increasingly relies on satellite communication (SATCOM) for navigation, logistics, safety, and crew connectivity. As cyber threats evolve, traditional cryptographic methods are becoming vulnerable, especially with the advent of quantum computing. To counter this, quantum technologies, especially Quantum Key Distribution (QKD) via satellite, offer a new frontier in secure maritime communication and should be adopted.

2.2 Quantum technology uses the principles of quantum mechanics to enhance communication and computation.

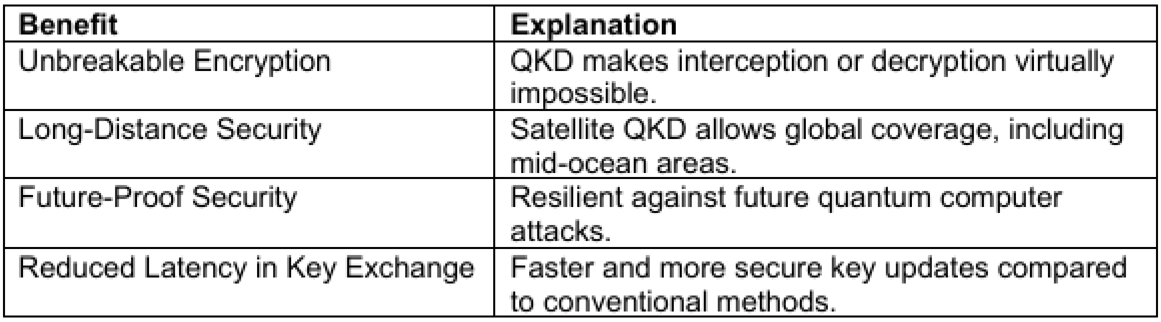
In SATCOM, it primarily involves:

2.2.1 Quantum Key Distribution (QKD**)**: Secure exchange of cryptographic keys using quantum particles (photons).

2.2.2 Quantum Entanglement: Enables theoretically unbreakable encryption.

2.2.3 Quantum Random Number Generation (QRNG): Produces truly random keys for encryption. Satellites provide global coverage, making them ideal for delivering quantum secured communication to ships in remote seas.

Advantages of Quantum technology in shipping: -



Benefit	**Explanation**
Unbreakable Encryption	QKD makes interception or decryption virtually impossible.
Long-Distance Security	Satellite QKD allows global coverage, including mid-ocean areas.
Future-Proof Security	Resilient against future quantum computer attacks.
Reduced Latency in Key Exchange	Faster and more secure key updates compared to conventional methods.

2.3. Global Developments and Projects related to Quantum Technology in SATCOM

2.3.1 Micius Satellite (China): World's first quantum communication satellite; demonstrated satellite-to-ground QKD.

2.3.2 EU Quantum Flagship Program: Funding research into QKD networks including maritime and aerospace sectors.

2.4 **UPGRADATION OF SATCOM**

SATCOM uses encrypted keys to secure the data stored within it. These encryptions can be protected using quantum random number generator (QRNGs). Classic PRNGs (Pseudo Random Number Generator) uses mathematical algorithm to encrypt keys known as seeds, which if predicted can give access to data.

TRNGs (Traditional Random Number Generators) uses physical source such as electrical, noise or thermal to create random numbers which get affected by environmental interference (temperature, EM- interference), whereas QRNGs offers a high speed of protection against external source.

QRNGs can enhance cyber security in satellite communications in several ways, mostly because they produce truly random numbers to seed high quality encryption keys. Theses keys can be used to:

- Use QRNG to generate truly random keys by photon detection which are fundamentally unpredictable.
- Use QRNG to create digital signatures that can authenticate satellite communications.
- Use QRNG in combination with QKD to establish secure keys for satellite communication.

2.5 **WORKING: -**

2.5.1 A satellite transmits entangled photons or uses quantum channels to distribute keys known as ciphertext. Both the ship and headquarters independently receive identical keys via quantum-secure channels.

2.5.2 The system itself decodes them automatically and the user views the final output only. Anyone trying to interfere with the pads, the system will either destroy the pad or give alarm because they are generated by QRNG and securely send keys between ship and headquarters by QKD.

3.Central COS (Security Operation Centre): - is a technical and operational facility, and not a governing body. These centralized cyber security units are operated by a shipping company or port authority.

As SATCOM is the most crucial link between the port and ship while navigation, it becomes important to monitor any cyber-attack in the system.

Therefore, COS offers 24/7 monitoring of shipboard and shore-side systems, ensuring that any abnormal activity or cyber threat is detected in real time.

4.CIERT (Cyber Incident Emergency Response Team):- is a specialized team responsible for detecting, responding and managing cyber incidents within an organization or sector. CIERT plays a crucial role in protecting shipboard and shore-based systems like SATCOM by coordinating rapid response, containment, and recovery efforts during cyberattacks. such committees can also be nationally formed to look after the SATCOM protection. Therefore, every nation must have such committee working for the cyber-attacks and each committee must have sub-committee working on individual aspects.

5. Improving Bandwidth Efficiency: -To further advance satellite communication in the maritime sector, targeted innovation must focus on enhancing bandwidth efficiency and spectrum utilization. SATCOM must be made affordable by providing Government subsidy to small owners and operators.

6. The committee is requested to consider our proposal in this document as mentioned in paragraphs 1, 2.1,2.4, 3,4 & 5.