Summary of IAPH Cyber Resilience Guidelines for Emerging Technologies in the Maritime Supply Chain

Introduction

The IAPH **Cyber Resilience Guidelines for Emerging Technologies in the Maritime Supply Chain** aim to provide a framework for mitigating cyber threats associated with new and evolving technologies in the maritime industry. As digital transformation accelerates, ports and maritime stakeholders face increasing cybersecurity risks. This summary document outlines key considerations, best practices, and regulatory recommendations to ensure the secure implementation of emerging technologies and is intended as an Information Document under item 7 "Revision of the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity". The full Guidelines will be published mid-2025 and will be available on the IAPH website.

1. Main principles for a cyber-secure implementation of emerging technologies

The main principles described in these guidelines, for achieving a cyber-secure implementation of emerging technologies in the maritime supply chain are:

1. **Integrate cybersecurity aspects in the early stages of emerging technologies planning, implementing "cybersecurity by design".**
   Cybersecurity should be embedded in the early stages of technology planning. Delaying implementation, or addressing vulnerabilities only after a cyberattack, can result in significantly higher costs and a higher impact on the organization operation continuity.
2. **Assess cybersecurity risks and vulnerabilities introduced by emerging technologies, even if those technologies are not planned to be implemented within the organization.**
   Even if an organization does not intend to adopt a particular emerging technology, it is crucial to evaluate potential risks it may introduce to existing infrastructure within the organization. For example, quantum computing will affect current encryption methods.

International Association of Ports and Harbors (IAPH)
The Global Ports' Forum for Industry Collaboration and Excellence

Finance and Administration Unit
South Tower New Pier Takeshiba (7th Floor)
1-16-1 Kaigan, Minato-ku
Tokyo 105-0022 – Japan

Contact us
info@iaphworldports.org
www.iaphworldports.org

3. **Avoid the misconception that non-IT systems do not require cybersecurity assessments.**
   Even seemingly 'non-cyber' initiatives such as Green Energy might introduce new cyber security vulnerabilities, which may have a disastrous impact on maritime supply chain operation.
4. **Recognize the potential physical impact of cyberattacks.**
   For example, drone hijacking: an attacker could take full control of the drone, redirecting it to unauthorized targets or using it for sabotage.
5. **Conduct a holistic cybersecurity assessment when integrating multiple technologies.**
   Some emerging technologies, such as Automation, rely on a combination of other technologies. Cybersecurity assessments should consider the overall system, not just individual components.
6. **Implement technology-specific protection, detection, and mitigation measures, in addition to general cybersecurity measures outlined in the "IAPH Cybersecurity Guidelines for Ports and Port Facilities".**
   Emerging technologies have specific characteristics and it is important to implement protection, detection, and mitigation measures that are tailored to the technology and not only the general ones. For example, dedicated authentication methods used in 5G networks.
7. **Look for new cybersecurity solutions that are enabled by emerging technologies.**
   Some emerging technologies may introduce new cybersecurity solutions that should be leveraged to enhance organizational cybersecurity.
   For example, AI excels at monitoring information systems. Using behavioral analysis, it identifies anomalies in network traffic and user behavior.
   Even IoT introduces new cybersecurity solutions, such as decentralized IoT-based honeypot solutions: IoT devices, which can serve as honeypots to lure attackers, allowing organizations to gather intelligence on their attack methods.
8. **Training and education is an important tool to ensure "cybersecurity by design" implementation of emerging technologies in the maritime supply chain.**

When teaching emerging technologies in maritime related courses, cybersecurity related content should be included. This is relevant to internal training in maritime supply chain organizations and in maritime supply chain related education institutions, including universities.

9. **Engage in the efforts to update the national and international legislation to adapt the existing requirements, for a cyber-secure implementation of emerging technologies in the maritime supply chain.**
   A cyber-secure implementation of emerging technologies is essential to ensure their contribution to a resilient, efficient and sustainable maritime supply chain.

2. Chapters

The new guidelines contain chapters on the following emerging technologies:

- Quantum
- Artificial Intelligence (AI)
- Drones
- Internet of Things (IoT)
- 5G
- Automation
- Green Energy

For each technology, the following aspects are described:

- **Technology overview**: An introduction to the technology, including its current and potential applications in maritime operations.
- **Cybersecurity risks and vulnerabilities**: An analysis of the specific threats posed by each technology, such as encryption-breaking quantum computing risks, AI-generated cyberattacks, drone hacking threats, IoT device vulnerabilities, 5G network slicing exploitation, automation system breaches, and cyber risks associated with green energy infrastructure.
- **Protection, detection, and mitigation measures**: A set of actionable recommendations for the cyber-secured implementation of emerging technologies in ports. Some of these are already described in the "IAPH Cybersecurity Guidelines for Ports and Port Facilities" and some are repeated

within each chapter to ensure a comprehensive, standalone reference for each technology. This is in addition to technology specific measures, which are described in these guidelines such as encryption strategies, network segmentation, multi-factor authentication, AI-driven anomaly detection, and post-quantum cryptography adoption.

- **New cybersecurity solutions enabled by the technology**: An exploration of how these technologies can also enhance cybersecurity, such as AI-driven threat detection, automation-based cyber resilience, and the role of quantum cryptography in securing communications.

There are also chapters covering **training and education** to support emerging technologies cybersecurity and the relevant **legislation**, for completeness.

3. Future Outlook and Recommendations The rapid evolution of emerging technologies necessitates a dynamic approach to cybersecurity. Key recommendations include:

- **Investment in Cybersecurity Training**: Enhance workforce awareness and technical capabilities. Harnessing the full potential of the emerging technologies in maritime supply chain organizations depends largely on human interaction rather than simply the technology itself. While the curriculum and training in cyber security have both advanced in the past few years, there is still a lack of maritime supply chain -specific programs that can address the risks pertaining to maritime operations in cyberspace.
- **Collaboration and Information Sharing**: Strengthen partnerships among maritime stakeholders, cybersecurity firms, and regulatory bodies.
- **Adoption of Advanced Security Technologies**: Leverage AI-driven threat detection, blockchain for secure transactions, and quantum encryption.
- **Regulatory Adaptation**: Policymakers should update and refine cybersecurity regulations to address the challenges posed by emerging technologies. While emerging technologies are revolutionizing maritime operations, the absence of strong legislative frameworks could introduce severe cybersecurity risks to the maritime supply chain.

4. Conclusion As ports and maritime industries embrace digital transformation, cybersecurity must remain a top priority. By implementing robust security measures, fostering collaboration, and staying ahead of emerging threats, the sector can enhance its resilience against cyber risks while harnessing the benefits of new technologies. These guidelines serve as a foundational reference for ensuring secure and efficient port operations in an increasingly interconnected world.

[Ends]

International Association of Ports and Harbors (IAPH)

The Global Ports' Forum for Industry Collaboration and Excellence

Finance and Administration Unit

South Tower New Pier Takeshiba (7th Floor)
1-16-1 Kaigan, Minato-ku
Tokyo 105-0022 – Japan

Contact us

info@iaphworldports.org
www.iaphworldports.org