Contribution ID: **242** Type: **ORAL**

# Cybersecurity as an essential aspect of transport and maritime nuclear systems

Data-driven decision-making is a key aspect of the nuclear industry. Yet this data does not exist within a vacuum. Instead, digital systems are utilised at every stage of the nuclear lifecycle, from conceptual design to transport to daily operation and ultimately decommissioning, with accurate and reliable data an essential aspect of nuclear operations.

Due to the vast amount of data collected on a daily basis, the sensitivity of some of the data transmitted, and increased reliance on digital systems, it is critical that these systems are built to include cybersecurity. This is essential to ensure appropriate safety, security, and safeguards for both operational technology and information technology.

The increase in cyber incidents affecting energy infrastructure, including operational technology attacks and ransomware attacks regarding company information, underline the importance of strong cybersecurity/defence. It is crucial for actors across the sector to understand and establish systems which counter the risks posed by weak cybersecurity.

The IAEA has long been involved in establishing cybersecurity guidelines for industry, offering guidance for operators as well as providers across the supply chain. This is supported by efforts by the International Electrotechnical Commission (IEC) to establish international standards on cybersecurity for operational technology and fixed installations. Yet domestic regulations on cybersecurity and transportable systems vary by jurisdiction, creating a patchwork assessment structure for firms looking to ensure international compliance. This is further complicated by non-uniform data protection regulations, limited worker expertise in cybersecurity for nuclear, and differences in design basis threats.

Amidst this complex regulatory landscape, nuclear innovation continues. Floating Nuclear Power Plants (FNPPs) and future maritime civil nuclear propulsion applications pose distinct cybersecurity dilemmas. The modular nature of the reactors, advanced technology which relies on increasingly digital operating systems including remote control, and options for international operation all present challenges. Building upon existing standards for terrestrial applications, as well as adapting existing best practices from other sectors, will be necessary to guarantee cybersecurity for maritime nuclear applications.

It is essential that these practical solutions are supported internationally through collaboration on cybersecurity standards and assessments. This should include incorporating cyber into baseline security assessments as well as cybersecurity incident reporting. Any approach should ensure a technology-agnostic approach which allows for future-proofing as technology advances. These measures are necessary to establish the groundwork necessary for integration of advanced technology, including artificial intelligence (AI).

The establishment of standards and regulations are only as effective as those who implement them. There is a distinct need for upskilling and increasing knowledge and understanding within the sector when it comes to cybersecurity. Creating a cybersecurity culture across the sector which is built upon systems prioritising safety, security, and safeguards by design will be indispensable to ensuring lasting impact and effectiveness of any regulation.

As technology advances to include advanced digital solutions, international standards and baseline operating approaches are needed to ensure safe, stable, and reliable nuclear systems.

## Country or International Organization

N

## Instructions

**Author:** Ms MILLS, Alex (NEMO)

**Co-author:** Mr EDWARDS, William (NEMO)

**Presenters:** Ms MILLS, Alex (NEMO); Mr EDWARDS, William (NEMO)

**Track Classification:** Track 4 Computer Security and Emerging Technologies