IAPH Cyber Resilience Guidelines

Webinar: Port- Maritime Cybersecurity: Protection Against Digital Threats

Gadi Benmoshe

Managing Director, Marinnovators Consulting
Vice Chair, IAPH Data Collaboration Committee

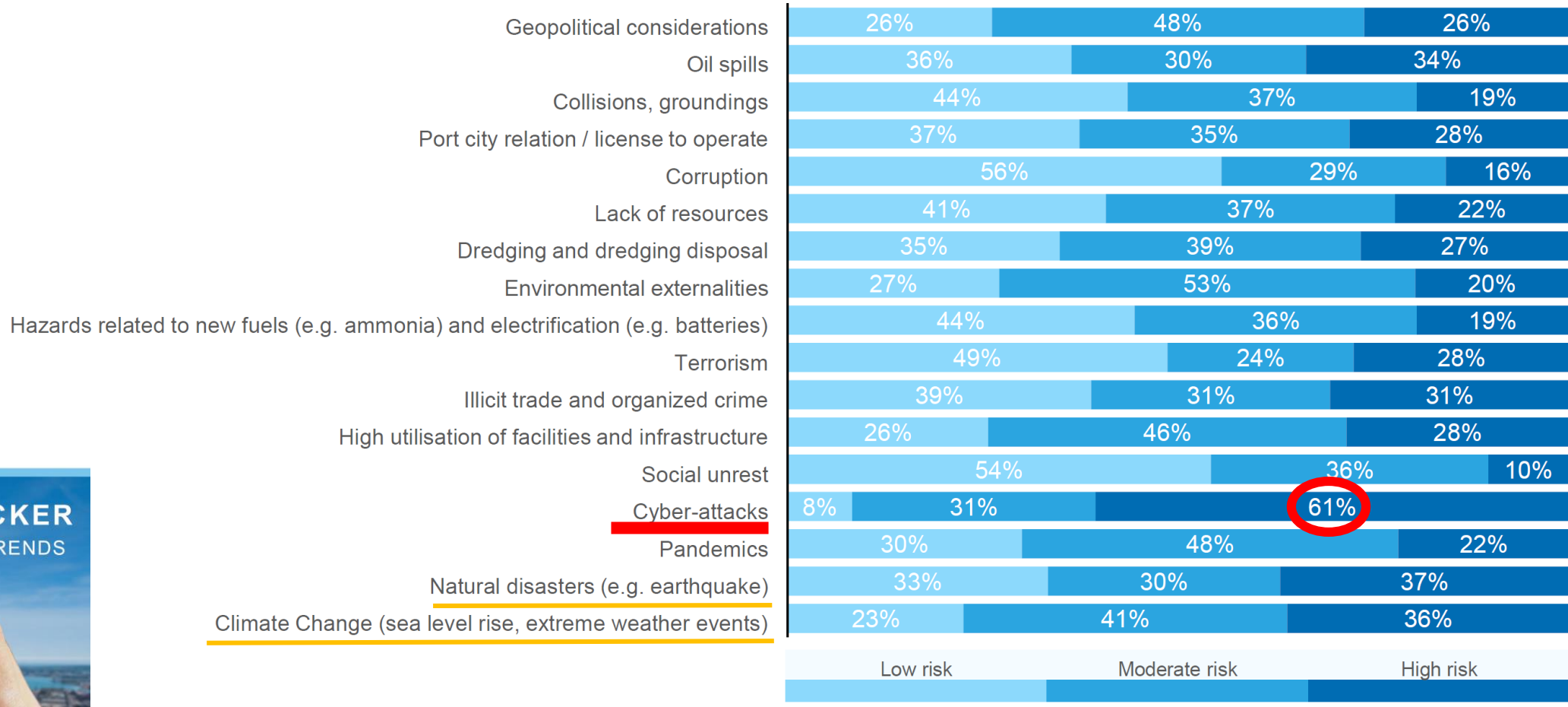
18/5/26

International Association of Ports and Harbors

- *Founded in 1955*
- *More than 380 members*
  205 ports and 177 port-related businesses across 89 countries
- *Technical committees are the backbone of the IAPH activity*
  - *Climate & Energy*
  - *Risk & Resilience*
  - *Data Collaboration:*
    - *Digital Transformation,*
    - *Innovation,*
    - *Cybersecurity*

https://www.worldportsconference.com/event/WPC/home

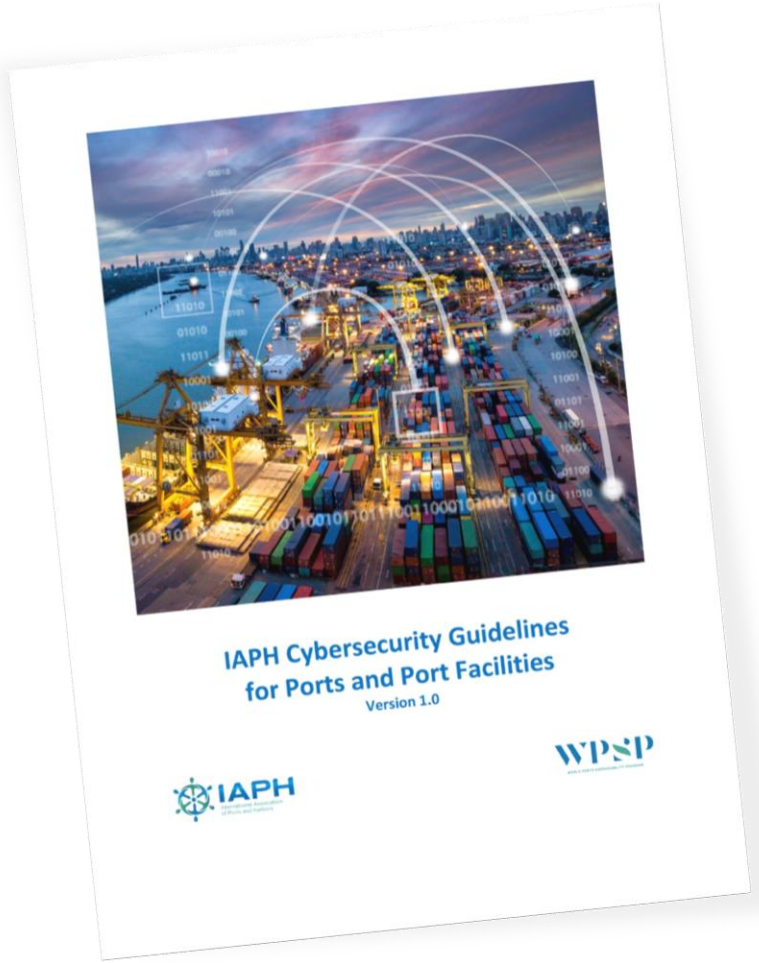
Cybersecurity threats are the most important risk factor perceived by port authorities



https://iaphworldports.us17.list-manage.com/track/click?u=dafe5935f04bdeefcfff28f98&id=359a49b41d&e=1ebabfec1f

IAPH Cybersecurity Guidelines for ports

- Developed with 22 experts, IAPH members from around the world and contributors from the World Bank
- Endorsed at IMO FAL 46 and added to IMO's Cybersecurity Guidelines on Maritime Cyber Risk Management.



https://sustainableworldports.org/iaph-launches-cybersecurity-guidelines-for-ports-and-port-facilities-as-part-of-industry-call-to-action-to-digitalize-the-maritime-transport-chain/

iaph

The five essential steps towards cyber resilience

1

Port leaders should acknowledge cyber risk management as a top-level responsibility recognizing it as a competitive and operational imperative

2

Successful cyber risk management begins with and depends on a common understanding of terms, financial grounding, and recognition of shared responsibility

3

You cannot minimize the threat until you understand the risk

4

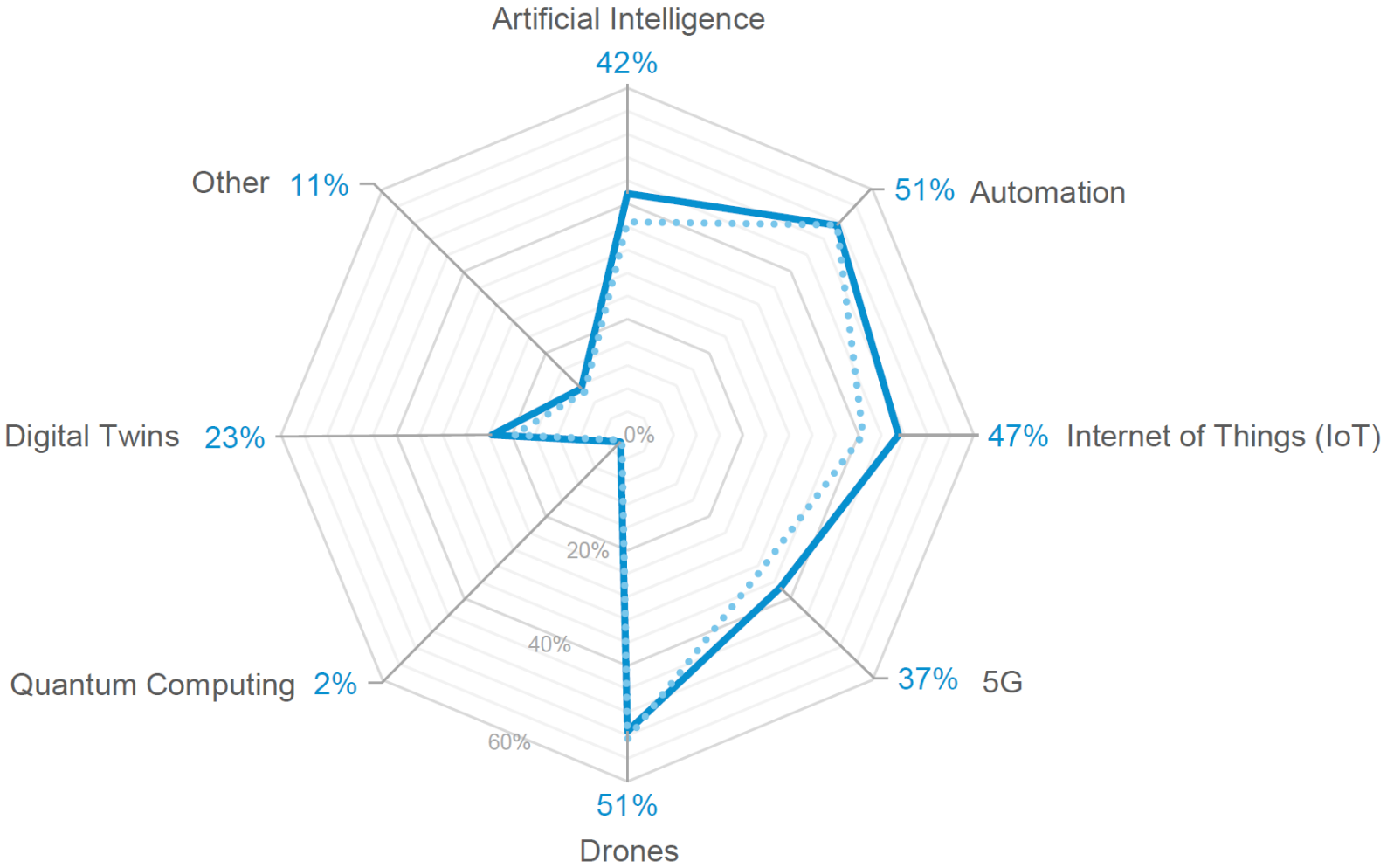
Protect, detect and mitigate

5

Work towards effective organizational cyber awareness

iaph

The adoption of emerging technologies



https://iaphworldports.us17.list-manage.com/track/click?u=dafe5935f04bdeefcfff28f98&id=359a49b41d&e=1ebabfec1f

IAPH Cyber Resilience Guidelines for Emerging Technologies In the Marine Supply Chain


Quantum


Artificial Intelligence (AI)


Drones


Internet of Things (IoT)


5G

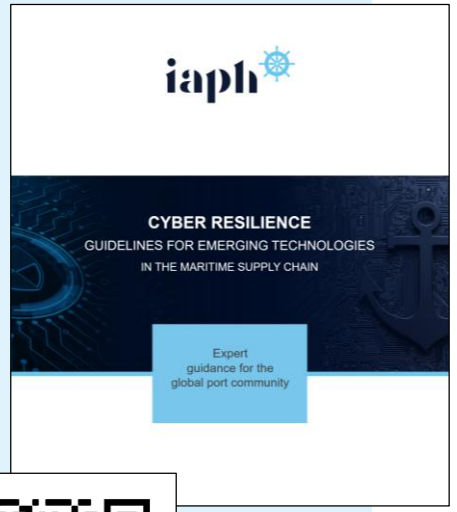

Automation


Green Energy


Training and Education


Legislation

- Developed with 28 experts, IAPH members from all 6 IAPH regions and contributors from the World Bank and WEF
- Endorsed at IMO FAL 50 and will be added to IMO's Cybersecurity Guidelines on Maritime Cyber Risk Management



English

Spanish

iaph

The main principles for achieving a cyber-secure implementation of emerging technologies in the maritime supply chain

1. **Integrate** cybersecurity aspects in the early stages of emerging technologies planning, implementing “cybersecurity by design”.
2. **Assess** cybersecurity risks and vulnerabilities introduced by emerging technologies, even if those technologies are not planned to be implemented within the organization.
3. **Avoid** the misconception that non-IT systems do not require cybersecurity assessments.
4. **Conduct** a holistic cybersecurity assessment when integrating multiple technologies.
5. **Look** for new cybersecurity solutions that are enabled by emerging technologies.

Let’s continue implementing innovation in Ports in a resilient way

Gadi Benmoshe

Managing Director, Marinnovators Consulting
Vice Chair, IAPH Data Collaboration Committee

gadib@marinnovators.com
+972506460980
LinkedIn

https://www.worldportsconference.com/event/WPC/home