UNIVERSITY OF PLYMOUTH
Marine Institute

The Queen's Anniversary Prizes
For Higher and Further Education
2019

POLICY BRIEFING

HOW TO BE cyber secure AT SEA

Protecting maritime infrastructure from digital threats

EXECUTIVE SUMMARY

Professor Kevin Jones and Dr Kimberly Tam

As the maritime sector becomes more technologically advanced there is an increased threat of critical national infrastructure to be compromised, essential services to be stopped, and both lives and livelihoods to be affected. The Maritime Cyber Threats Research Group at the University of Plymouth is looking holistically at the **digital threats that affect the maritime sector,** spanning the technical, social-technical, and cyber-physical, and the implications these will have for technology, people and policy/law. Increased advocacy, aid and incentives to promote **secure-by-design cyber security principles** are essential for moving forward safely.

SOCIAL CONTEXT

Maritime cyber security is a critical area for the UK, which as an island nation relies on shipping for roughly 95% of all inbound and outbound goods. Currently, the **UK imports around 50% of its gas** from the international market. **The UK also imports around 56% of the total food it consumes.** Due to our 'just-in-time' model, we tend to rely on smaller, more frequent deliveries, and have less in storage and reserves. **A cyber-attack on shipping or ports could therefore have significant impact on people and industries.**

Other UK imports and exports affect manufacturing and trade. According to the Office of National Statistics, UK exports in March 2022 grew across every industry. Some of the main exports being precious metals production (~£22.8 Billion), aircraft parts (~£17.3 Billion), motor vehicles (~£14.6 Billion) and pharmaceuticals (~£13.2 Billion). In a competitive, time-sensitive context, an unsecure maritime sector could prevent UK industry from acquiring raw materials, lower interest in UK goods, or increase the risk of goods becoming out-of-date.

The country is also leading offshore renewable energy solutions to reduce dependency on international fuels, and to lower carbon emissions. This will only increase the amount of critical national infrastructure – such as **ocean windfarms** – in UK coastal waters, making maritime cyber security a key consideration for social and economic security.

RESEARCH AIMS AND CONTRIBUTIONS

We wish to approach policymakers and legislators, especially **MPs and Peers,** on several key issues around maritime-cyber security to discuss key objectives for improving maritime cyber security. The overall aim, however, is to improve the **sharing of best practices in the sector and secure-by-design principles.**

- Strengthen the partnerships across marine/maritime organisations in sharing best cyber-defence strategies.
- Detect, investigate and disseminate threat intelligence, from criminal to terrorist activity, to protect the UK.
- Improve cyber-physical risk assessment to protect maritime supply chains.
- Enhance and expand the nation's cyber-skills around all marine/maritime critical national infrastructure.
- Foster the growth of a sustainable, world-leading department of maritime cybersecurity solutions.
- Strengthen cyber-resilience at all levels of marine/maritime organisations, onshore and at sea.
- Secure the next generation of marine autonomy, smart ports and offshore renewable energy.
- Instil secure-by-design mindset into ship builders, ship operators, and device manufacturers.
- Enable law enforcement to track both new and old maritime threats with a cyber element (e.g. smuggling).
- Inform UK and international legislation.

RESEARCH FINDINGS

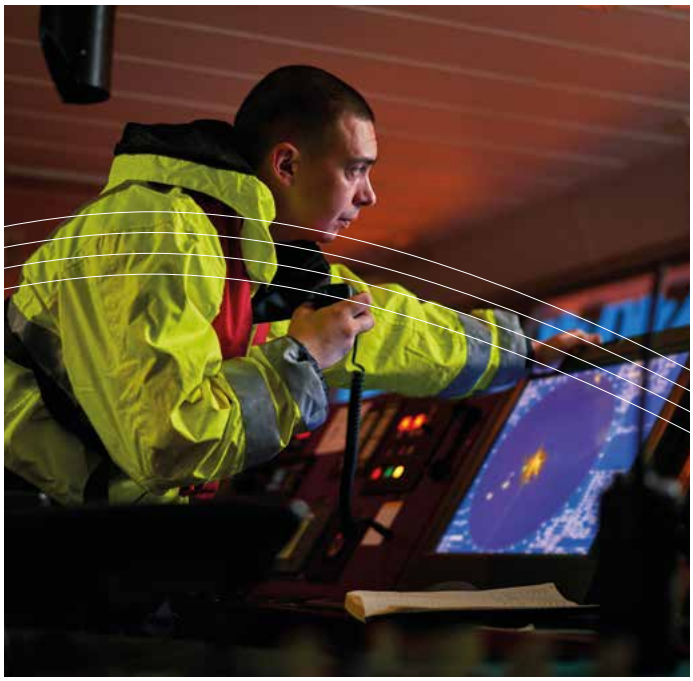
- **Risk assessment for the maritime sector is unique** and would benefit from cyber-physical risk assessment.
- There are **gaps in digital forensic and cyber-incident investigation and response,** and mariner cyber security training, both technically and with standards/regulations.
- With ever-increasing remote-access technology, automation, big-data sensor networks and new infrastructure, **maritime cyber security is critical to safeguard the industry** and those it serves.
- **Maritime organisations and individuals lack awareness of the impact of a maritime cyber incident,** the potential threats, and how to communicate cyber-risks and solutions to on-shore and at-sea assets, the people who operate those systems, and the people/businesses that rely on this infrastructure.

Maritime organisations and individuals lack awareness of the impact of a maritime cyber incident.

KEY POINTS

1. **Lack of cyber security in the maritime sector affects all other UK sectors including energy and manufacturing.**
2. **Cyber-threats are not well understood or communicated, and systems are not built to be secure.**
3. **The sector will be adopting more technology – better monitoring for fuel efficiency, autonomy, new vessels and offshore structures – that will require security.**

Cyber security is a critical area for the UK, which as an island nation relies on shipping for roughly 95% of all inbound and outbound goods.



POLICY IMPLICATIONS

Our work highlights the critical nature of addressing cyber security concerns in the increasingly technology-driven maritime sector. Incentives and aid for new blue technology to promote secure-by-design principles will be key drivers for progress in this area.

Incentives and aid for new blue technology to promote secure-by-design principles will be key drivers for progress.

POLICY RECOMMENDATIONS

- Policy makers to advocate that vessels, ports and structures are 'safe' and 'seaworthy' in terms of cyber security. This can be through DfT support for industry and organisations.
- Facilitate the discussion of threats and solutions between marine/maritime organisations and the public.
- Support new training programmes around the safe and secure use of next-generation marine/maritime technology. This is for workers both on ships and onshore.
- Promote investment in research and development to create solutions that will benefit the UK that address the cyber-security challenges of a highly technical sea space.

UNIVERSITY OF PLYMOUTH
Marine Institute

POLICY QUESTION

How will the UK address the cyber-security issues that threaten our infrastructure, people, and goods at sea?

Professor Kevin Jones
Executive Dean, Faculty of Science and Engineering

Dr Kimberly Tam
Associate Professor in Cyber Security

The University of Plymouth is renowned for internationally leading education, research and innovation; it has a mission to Advance Knowledge and Transform Lives. A three-time winner of the Queen's Anniversary Prize, most recently in respect of pioneering research on microplastic pollution in the ocean, the University continues to drive global action in marine and maritime, sustainability, health technologies and climate.

Find out more about our researchers and their work: plymouth.ac.uk/research/maritime-cyber-threats-research-group