INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

Circular Letter No.4739
13 July 2023

To: IMO Member States and other Governments
United Nations and specialized agencies
Intergovernmental organizations
Non-governmental organizations in consultative status

Subject: **IMO/University of Plymouth (Cyber-SHIP Lab) Symposium on "Maritime cyber security and resilience" (1 and 2 November 2023)**

1 The Secretary-General of the International Maritime Organization and the Universityof Plymouth's Cyber-SHIP Lab have the honour to invite participation in their forthcoming joint Symposium on "Maritime cyber security and resilience", scheduled to take place on 1 and 2 November 2023 at IMO Headquarters, 4 Albert Embankment, London SE1 7SR.

2 The Symposium will share the latest international maritime cyber risk evaluation and mitigation research and explore how Governments, industry, researchers and NGOs can collaborate to build international maritime supply chain cyber resilience. Industry and academic expert speakers will address topics across ship, port and maritime supply chain cyber security, including cyber security and safety of assets and people, new technologies, policy development and mariner training.

3 The Cyber-SHIP Lab is the University of Plymouth Maritime Cyber Threats Research Group's unique hardware-based maritime cyber-physical testbed facility. The Symposium is the third Cyber-SHIP Lab annual symposium and its second year hosted by IMO. It will build on the success of the 2021 and 2022 symposia that attracted an exceptionally wide range of expert international speakers and delegates.

4 The Symposium is open to all Member Governments, UN Agencies, IGOs, NGOs and other participants. Member States and international organizations are invited to disseminate this invitation widely to interested parties and stakeholders.

5 The Symposium will be held in person and in English only. It can also be streamed on the IMO YouTube channel after the event. The provisional programme for the Symposium is set out in annex 1.

6 Registration is mandatory for participation and registration procedures are set out in annex 2. Participants are responsible for their own travel and accommodation. Visa support letters can be provided upon request once registration has been completed.

7 For any additional information and queries, please contact the IMO Secretariat by email at: marsec@imo.org

***

ANNEX 1

**IMO/UNIVERSITY OF PLYMOUTH (Cyber-SHIP Lab) SYMPOSIUM
"MARITIME CYBER SECURITY AND RESILIENCE"**

PROVISIONAL PROGRAMME

Day 1, Actional research outputs	
Session 1: Opening session	
09.00-09.20	**Opening remarks** • **Kitack Lim,** Secretary-General, IMO • **Kevin Jones**, Principal Investigator, Cyber-SHIP Lab; Executive Dean, Faculty of Science and Engineering, University of Plymouth
09.20-10.00	**"Was that really the worst that could happen?"** • **Kevin Jones,** University of Plymouth
10.00-10.30	**Discussion**
10.30-11.00	**Refreshment break**
Session 2: **What is and isn't being reported? And what are/should we be doing about it?**	
11.00-11.30	**Analysis of publicly reported cyber incidents in the maritime sector 2002-2023** • **Stephen McCombie,** Professor of Maritime IT Security, NHL Stenden University of Applied Sciences • **Jeroen Pijpker,** Senior Lecturer/Researcher in Cyber Security, NHL Stenden University of Applied Sciences
11.30-12.30	**Panel and audience discussion** **- Current and future directions in maritime cyber security** • **Marie Haugli-Sandvik,** Project Manager and PhD Candidate, Norwegian University of Science and Technology • **Adam Sobey**, Professor of Data-Centric Engineering, University of Southampton; Group Lead for Marine and Maritime in the Data-Centric Engineering Programme, The Alan Turing Institute • **Gary Kessler**, independent academic, consultant, and maritime cyber security practitioner; Professor of Cyber Security (retired) • **Kimberly Tam**, Cyber-SHIP Lab Academic Lead and Lecturer in Cyber Security, University of Plymouth
12.30-13.30	**Lunch**

Session 3: **Mapping, modelling, mitigating and - somehow - insuring against maritime cyber risk**	
13.30-14.10	**Development of a comprehensive cyber security road map through a Concept of Operations (ConOps), including a review of initiatives to meet IACS newbuild ships' cyber resilience requirements** • **Jungo Shibata**, Manager, Maritime and Logistics IoT Team, Maritime Technology Group, Monohakobi Technology Institute, a Research & Development subsidiary company of NYK Line
14.10-14.50	**Threat modelling of the autonomous ship's OT systems** • **Muhammed Erbas**, Maritime Transportation, Management Engineering and Cybersecurity Researcher, Tallinn University of Technology
14.50-15.30	**The complex relationship between the marine insurance market and cyber risks - further tested by the emergence of cyber-enabled ships** • **Eva Szewczyk**, PhD candidate researching legal and insurance implications of autonomous shipping, Northumbria University
15.30-16.00	**Refreshment break**
Session 4: **Cyber-physical research platforms and current maritime security ops capabilities**	
16.00-16.25	**Our next generation maritime cyber security / cyber-physical research platform** • **Avanthika Vineetha Harish**, Industrial Researcher, Pentesting • **Wesley Andrews**, Project Engineer, Cyber-SHIP Lab, Uni. of Plymouth
16.25-16.50	**When your asset doesn't stay still - the state of play in maritime security operation centers** • **Allan Nganga**, PhD candidate in Maritime Cybersecurity, Western Norway University of Applied Sciences
16.50-17.00	**Q&A / discussion and Day-1 wrap-up**

Day 2, Industry-focused knowledge sharing	
Session 5: Opening session	
09.00-09.20	**Day 2 opening remarks** • **Baroness Vere**, Minister for Aviation, Maritime and Security, United Kingdom Department for Transport • **James Parkin**, Rear Admiral, Director Develop - Navy Command Headquarters, Royal Navy
09.20-09.45	**A tale of two very real-world maritime cyber threats: software supply chain and port security** • **Andy Howell**, Principal Cyber Security Consultant, BMT • **Thomas Scriven**, Principal Consultant, Mandiant
09.45-10.05	**The UK's strategic approach – a cyber security framework to support the global maritime community** • **Matthew Parker**, Head of Maritime Security Strategy, Threat & Risk, United Kingdom Department for Transport
10.05-10.30	**United States Coast Guard perspective on maritime cyber security** • **Adam B. Morrison**, Captain, Deputy Coast Guard Cyber Commander, United States Coast Guard
10.30-11.00	**Refreshment break**
Session 6: **Boosting resilience through intelligence, coordination and prioritization**	
11.00-11.35	**Cyber resilience through industrywide intelligence and SOC capabilities** • **Makiko Tani**, Deputy Manager of Cyber Security Team, ClassNK
11.35-12.10	**The Maritime Cyber Priority: findings from DNV's 2023 maritime cyber security research report** • **Svante Einarsson**, Head of Cyber Security Maritime, DNV
12.10-12.50	**Panel and audience discussion - Our maritime cyber security concerns** • **James Parkin**, Royal Navy • **Matthew Parker**, United Kingdom Department for Transport • **Tim Acland**, Chief Technology Officer, HENSOLDT • **Svante Einarsson**, DNV
12.50-14.00	**Lunch**

Session 7: **Industry and international maritime cyber guidance, regulation and review**	
14.00-14.25	**Maritime industry guidelines for cybersecurity on board ships, a comprehensive review** • **Jakob Larsen**, Head of Maritime Safety & Security, BIMCO
14.25-14.50	**Cyber security considerations for the maritime single window (MSW, mandatory from 2024)** • [IMO nominated expert]
14.50-15.15	**Maritime cyber attack activity and trends, and public/private sector efforts towards information-sharing** • **Scott Dickerson**, Executive Director, MTS-ISAC; Founder and Principal, CISO
15.15-15.45	**Refreshment break**
Session 8: Bolstering against battles against breaches	
15.45-16.10	**Cyber battle damage repair. Towards an improvement of cyber resilience of navy ships** • **William van der Geest**, Commander, Royal Netherlands Navy
16.10-16.35	**Our vessel breach: What's technically plausible in real-world multisystem vessel testing?** • **Kelly Malynn**, Product Lead and Underwriter for Cyber Physical Damage, Beazley
16.35-16.45	**Closing remarks** • **Heike Deggim**, Director, Maritime Safety Division, IMO
16.45-17.00	**Symposium wrap-up** • **Kevin Jones,** University of Plymouth

***

ANNEX 2

REGISTRATION PROCEDURES

Registration for the Symposium will be available as follows:

.1 via the IMO Online Meeting Registration System (OMRS) for participants registering through their national OMRS Delegation Coordinator; or

.2 for non-OMRS registered participants as set out below.

Online Meeting Registration System (OMRS)

Member Governments, UN Agencies, IGOs and NGOs are required to provide, prior to the meeting date, the names of all members of their delegations attending the Symposium via OMRS, as advised in Circular Letter No.4336 of 5 November 2020. This facilitates both their entry into the building and the production of the list of participants by the Secretariat.

For those delegates attending the Symposium who have completed the registration procedure, an electronic access card will be issued at IMO to pass through the security barrier in the IMO building.

Issue of the access card will require photographic proof of identity, e.g. passport, identity card or driving licence. Participants may also be required to show proof of identity at any time while they are in the Headquarters building if requested by IMO Security. In view of the significant costs incurred in producing access cards, delegates who have previously been issued with one are kindly requested to bring it with them for reactivation.

Any matters relating to the use of the OMRS and participation in the forthcoming IMO/University of Plymouth Symposium "Maritime cyber security and resilience" should be communicated to:

Registration Unit
Meeting Services and Interpretation Section
Email: onlineregistration@imo.org

Non-OMRS registered participants

Participants wishing to attend the Symposium by sharing the invitation from Member States or international organizations but who are not affiliated with an IMO delegation are requested to contact cyber-ship-lab@plymouth.ac.uk for specific registration procedures.