ORGANIZACIÓN MARÍTIMA INTERNACIONAL

S

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

Circular nº 4739
13 julio 2023

A: Estados Miembros de la OMI y otros Gobiernos
Naciones Unidas y organismos especializados
Organizaciones intergubernamentales
Organizaciones no gubernamentales con carácter consultivo

Asunto: **Simposio OMI/Universidad de Plymouth (Cyber-SHIP Lab) sobre "Ciberseguridad y resiliencia en el sector marítimo" (1 y 2 de noviembre de 2023)**

1 El Secretario General de la Organización Marítima Internacional y el Laboratorio Cyber-SHIP de la Universidad de Plymouth, tienen el honor de invitar a participar en su próximo Simposio conjunto sobre "Ciberseguridad y resiliencia en el sector marítimo", que está previsto que tenga lugar los días 1 y 2 de noviembre de 2023 en la sede de la OMI, 4 Albert Embankment, Londres SE1 7SR.

2 En el Simposio se compartirán los últimos estudios internacionales sobre evaluación y mitigación de riesgos cibernéticos en el sector marítimo y se estudiará cómo pueden colaborar los gobiernos, el sector, los investigadores y las ONG para crear resiliencia cibernética en la cadena de suministro marítima internacional. Expertos del sector y del mundo académico abordarán temas relacionados con la ciberseguridad de los buques, los puertos y la cadena de suministro marítima, incluida la ciberseguridad y la seguridad de los bienes y las personas, las nuevas tecnologías, la elaboración de políticas y la formación de los marinos.

3 El laboratorio Cyber-SHIP es el banco de pruebas ciberfísicas del sector marítimo, basado en soporte físico, exclusivo del Grupo de investigación sobre amenazas cibernéticas del sector marítimo de la Universidad de Plymouth. Se trata del tercer simposio anual del Cyber-SHIP Lab y del segundo año que se celebra en la OMI. Se basará en el éxito de los simposios de 2021 y 2022, que atrajeron a una gama excepcionalmente amplia de ponentes y delegados internacionales expertos en la cuestión.

4 El Simposio está abierto a todos los Gobiernos Miembros, organismos de las Naciones Unidas, organizaciones intergubernamentales, organizaciones no gubernamentales y otros participantes. Se invita a los Estados Miembros y organizaciones internacionales a que difundan ampliamente esta invitación entre todas las partes interesadas.

5 El Simposio se celebrará presencialmente y se llevará a cabo en inglés únicamente. También se retransmitirá en el canal de YouTube de la OMI (IMO YouTube channel) tras el evento. El orden del día provisional del Simposio figura en el anexo 1.

6 Es obligatorio inscribirse para participar. Los procedimientos relativos a la inscripción figuran en el anexo 2. Los participantes organizarán por sí mismos el viaje y el alojamiento. Se proporcionarán cartas de apoyo para el visado si se solicitan una vez que se haya ultimado la inscripción.

7 Para toda información adicional y preguntas, se ruega dirigirse por correo electrónico a la Secretaría de la OMI, a: 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 roadmap 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	[Title TBC] • **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 multi-system 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

***

ANEXO 2

PROCEDIMIENTOS DE INSCRIPCIÓN

La inscripción en el Simposio se podrá efectuar de la siguiente manera:

.1 a través del sistema de inscripción en línea para las reuniones (OMRS) para los participantes que se inscriban a través de su coordinador nacional de delegación del OMRS; o

.2 para los participantes no inscritos en el OMRS, tal como se indica a continuación.

Sistema de inscripción en línea para las reuniones (OMRS)

Los Gobiernos Miembros, los organismos de las Naciones Unidas, las organizaciones intergubernamentales y las organizaciones no gubernamentales deberán remitir, con antelación a la fecha de la reunión, los nombres de todos los miembros de sus delegaciones que asistan al simposio, a través del sistema de inscripción en línea para las reuniones (OMRS), tal como se informa en la circular nº 4336, de 5 de noviembre de 2020. Esto facilita su entrada en el edificio y la elaboración de la lista de participantes por parte de la Secretaría.

A los delegados que asistan al Simposio y que hayan completado el proceso de inscripción se les expedirá en la OMI una tarjeta electrónica de acceso para que puedan pasar por la barrera de seguridad en el edificio de la Organización.

A fin de que se les expida dicha tarjeta de acceso tendrán que presentar una prueba de identidad que contenga una fotografía, como, por ejemplo, el pasaporte, el documento de identidad o el permiso de conducir. Asimismo, cabe la posibilidad de que el personal de seguridad de la OMI solicite a los participantes que muestren una prueba de su identidad en cualquier momento mientras se encuentren en el edificio de la sede. Habida cuenta de los considerables costos que supone la expedición de las tarjetas de acceso, se ruega a los delegados que ya dispongan de una tarjeta expedida en reuniones anteriores que la traigan consigo para su reactivación.

Cualquier asunto relacionado con el uso del OMRS y la participación próximamente en el Simposio "Ciberseguridad y resiliencia en el sector marítimo" de la OMI y la Universidad de Plymouth deberá comunicarse a:

Dependencia de Inscripción
Sección de Servicios de Reuniones e Interpretación
Correo electrónico: onlineregistration@imo.org

Participantes no inscritos en el OMRS

Se ruega a los participantes que deseen asistir al Simposio compartiendo la invitación de los Estados Miembros u organizaciones internacionales, pero que no estén afiliados a una delegación de la OMI, que se pongan en contacto con cyber-ship-lab@plymouth.ac.uk para conocer los procedimientos específicos de inscripción.
