ORGANISATION MARITIME INTERNATIONALE

F

4 ALBERT EMBANKMENT
LONDRES SE1 7SR
Téléphone : +44 (0)20 7735 7611 Télécopieur : +44 (0)20 7587 3210

Lettre circulaire n° 4739
13 juillet 2023

Destinataires : États Membres de l'OMI et autres gouvernements
Organisation des Nations Unies et institutions spécialisées
Organisations intergouvernementales
Organisations non gouvernementales bénéficiant du statut consultatif

Objet : **Colloque de l'OMI et de l'Université de Plymouth (Cyber-SHIP Lab) sur la "Cybersécurité maritime et la résilience" (1er et 2 novembre 2023)**

1 Le Secrétaire général de l'Organisation maritime internationale et le Cyber-SHIP Lab de l'Université de Plymouth ont l'honneur d'inviter les destinataires susmentionnés à participer à leur prochain colloque commun sur la "Cybersécurité et la résilience maritimes", qui devrait se tenir les 1er et 2 novembre 2023 au Siège de l'OMI, 4 Albert Embankment, Londres SE1 7SR.

2 Le colloque présentera les dernières recherches portant sur l'évaluation et l'atténuation des risques de cybersécurité maritime internationale, et examinera les possibilités de collaboration entre les gouvernements, le secteur, les chercheurs et les ONG aux fins de créer une chaîne d'approvisionnement maritime résiliente à l'international. Des spécialistes issus du milieu académique et du secteur maritime aborderont des sujets relatifs à la cybersécurité des navires, des ports et de la chaîne d'approvisionnement maritime, y compris la cybersécurité et la sécurité des actifs et des personnes, les nouvelles technologies, l'élaboration des politiques et la formation des gens de mer.

3 Le Cyber-SHIP Lab est un système cyberphysique unique du Maritime Cyber Threats Research Group de l'Université de Plymouth, équipé d'un banc d'essai avec infrastructure informatique. Le présent colloque est le troisième colloque annuel du Cyber-SHIP Lab, accueilli par l'OMI pour la deuxième année. Il s'appuiera sur le succès des colloques de 2021 et 2022, qui avaient vu l'intervention de spécialistes les plus divers, et réuni des représentantes et représentants du monde entier.

4 Le colloque est ouvert à tous les Gouvernements Membres, institutions des Nations Unies, OIG, ONG et autres participants. Les États Membres et les organisations internationales sont invités à diffuser ces renseignements auprès de toutes les parties intéressées.

5 Le colloque se tiendra en présentiel et en anglais uniquement. Il est également possible de le visionner sur la chaîne YouTube de l'OMI après l'événement. On trouvera à l'annexe 1 le programme provisoire du colloque*.

* En anglais seulement.

6 L'inscription est obligatoire pour y participer et les modalités d'inscription figurent dans l'annexe 2. Les participants devront prendre leurs propres dispositions de voyage et d'hébergement. Des lettres d'appui pour les demandes de visas peuvent être fournies sur demande, une fois l'inscription effectuée.

7 Pour tout renseignement ou toute question supplémentaire, prière de s'adresser au Secrétariat de l'OMI par courrier électronique à l'adresse suivante : 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

***

ANNEXE 2

PROCÉDURES D'INSCRIPTION

L'inscription au colloque pourra être effectuée :

.1 dans le système d'inscription en ligne aux réunions de l'OMI (OMRS) pour les participantes et participants qui se sont inscrits par l'intermédiaire du coordonnateur national de délégation pour l'inscription dans l'OMRS; ou

.2 pour tous les participantes et participants qui ne sont pas inscrits dans l'OMRS, comme renseigné ci-dessous.

Système d'inscription en ligne aux réunions (OMRS)

Ainsi qu'il est indiqué dans la lettre circulaire n° 4336 du 5 novembre 2020, les Gouvernements Membres, les institutions des Nations Unies, les organisations intergouvernementales et les organisations non gouvernementales doivent fournir à l'avance les noms de tous les membres de leur délégation qui assisteront au colloque, en utilisant l'OMRS. Cela facilitera leur entrée dans le bâtiment et permettra au Secrétariat d'établir la liste des participantes et participants.

Les représentantes et représentants qui assistent au colloque et qui ont suivi la procédure d'inscription se verront délivrer, sur place, un badge électronique qui leur permettra de franchir les portillons de sécurité.

Pour permettre la fabrication de ce laissez-passer, les représentants et représentantes seront tenus de présenter à leur arrivée une pièce d'identité portant leur photographie, par exemple un passeport, une carte d'identité ou un permis de conduire. Les participants pourront également être invités à présenter une pièce d'identité à n'importe quel moment pendant qu'ils se trouveront dans le bâtiment, sur demande du personnel de sécurité de l'OMI. Vu les dépenses importantes qu'occasionne la fabrication des badges, les représentants et représentantes qui en possèdent déjà un sont priés de bien vouloir l'apporter aux fins de sa réactivation.

Pour toute question relative à l'utilisation de l'OMRS et à la participation au prochain colloque de l'OMI et de l'Université de Plymouth intitulé "La cybersécurité et la résilience maritime", prière de s'adresser au :

Service des inscriptions
Section du service des réunions et de l'interprétation
Courriel : onlineregistration@imo.org

Participantes et participants qui ne sont pas inscrits dans l'OMRS

Les participantes et participants qui souhaitent participer au colloque en utilisant l'invitation d'États Membres ou d'organisations internationales mais qui ne font pas partie d'une délégation auprès de l'OMI sont priés d'envoyer un courriel à cyber-ship-lab@plymouth.ac.uk pour prendre connaissance des modalités d'inscription spécifiques.
