NORTH ATLANTIC TREATY ORGANISATION
NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE
NMIOTC
SOUDA BAY
GREECE

3000 NSC - 74/ser.: NU:34

SUBJECT: **10th NMIOTC CONFERENCE ON CYBER SECURITY IN MARITIME DOMAIN – CALLING LETTER**

DATE: 10 March 2026

REFERENCE: 10th NMIOTC CONFERENCE ON CYBER SECURITY IN MARITIME DOMAIN – SAVE THE DATE LETTER

1. **Introduction:** NMIOTC has the pleasure to announce its 10th NMIOTC Conference on Cyber Security in Maritime Domain, which will take place at its premises, in Souda Bay Crete, Greece, from Wednesday **23 to** Thursday **24 of September 2026**.

2. **Aim:** The Conference aims to promote structured collaboration among scientific, industrial, naval, maritime, and academic stakeholders in the field of Cyber Security and Cyber Defence Operations within the Maritime Domain. This collaboration will foster a coordinated and comprehensive approach to Maritime Cyber Security challenges, enhance collective awareness, and strengthen the overall resilience of the Maritime community. As in the past iterations of the Conference, the event is expected to attract researchers, practitioners, Naval personnel, academic institutions, shipping companies, standardization bodies, governmental authorities, international organizations, and representatives of both the public and private sectors.

3. The key objectives of the Conference are as follows:

a. Examine and assess the impact of emerging cyber threats and vulnerabilities on Maritime Operations, with particular emphasis on the effectiveness of current Cyber Defence strategies and respective policy frameworks.

b. Review and evaluate advancements in future Maritime Cyber Security technologies, systems, and industrial solutions, including their operational applicability and integration potential.

c. Provide insights into methodologies, standards, and frameworks for the assessment, certification, and assurance of Maritime Security.

d. Present and analyze ongoing initiatives and cooperative mechanisms in Cyber Security between NATO and the European Union, with attention to policy alignment and operational interoperability.

e. Identify and evaluate strategic and technical measures for the protection of Maritime value and supply chains, critical infrastructures, and essential services.

f. Foster and advance innovative, interdisciplinary research in the fields of Maritime Cyber Security and Cyber Defence.

4. An indicative, though non-exhaustive, list of potential thematic areas includes:

- The conceptualization and operational characteristics of Cyberspace within the Maritime Environment.
- The evolving nature of current and emerging cyber-attacks affecting Maritime Operations.
- Doctrinal and operational planning for Cyberspace defensive military operations in the Maritime Domain.
- Emerging attack vectors and corresponding defence strategies.
- Security considerations in advanced technologies, including Artificial Intelligence (AI), 5G networks, Big Data analytics, and Machine Learning applications.
- Cyber Security challenges in autonomous ships and unmanned maritime systems.
- Protection of industrial maritime components and control systems (e.g., SCADA systems, navigation systems, PLCs, and related operational technologies).
- Broader Cyber Security dimensions and risk factors within the maritime sector.
- NATO–EU information exchange mechanisms and cooperative frameworks in Maritime Cyber Security.
- Analysis of cyber threats, incidents, and operational events within the Maritime Environment.
- Development and enhancement of Cyberspace Situational Awareness capabilities in maritime contexts.
- Cyber capabilities, forces, and the integration of cyber effects in maritime operations.
- Cross-border Cyber Security information sharing, coordination, and analytical processes.
- Innovative methodologies for dynamic Cyber Risk Assessment, modelling, and forecasting.
- Advanced Cyber Defence and Cyber Security technologies and enabling tools.
- Practical training frameworks, certification schemes, and professional standards in Maritime Cyber Security.
- Maritime cyber ranges, simulation environments, and exercise design.
- Code auditing, assurance, and vulnerability assessment of maritime Information and Communications Technology (ICT) systems.
- The intersection of Artificial Intelligence and Maritime Cyber Security.
- Incident response methodologies, technologies, and resilience mechanisms.
- Cyber-attacks targeting maritime supply chains and their propagation dynamics.
- Predictive modelling of cyber threats, attacks, and operational impacts.
- NATO–EU implementation roadmaps concerning the Cyberspace operational environment.
- Geopolitical and strategic implications arising from Cyberspace operations.
- Cyber Security considerations in Maritime Logistics.
- Regulatory and operational implications of EU security and data protection legislation for the Merchant Navy.
- International legal frameworks governing Cyberspace, including reference to the Tallinn Manual.

This thematic structure is intended to encourage rigorous academic inquiry, operational relevance, and interdisciplinary dialogue across the full spectrum of Maritime Cyber Security and Cyber Defence.

5. **Call for papers.** Papers are hereby invited on the thematic areas of the Conference. Interested speakers are requested to submit an abstract of their proposed paper or presentation no later than 10 July 2026. Submissions should be accompanied by a short Curriculum Vitae and a concise description of the organization, institution, or company represented by the author(s).

Following the Conference, selected papers may be considered for publication in the Journal of the NATO Maritime Interdiction Operational Training Centre (NMIOTC). Authors of selected contributions will be afforded the opportunity to revise and update their manuscripts prior to publication.

The abstracts should not exceed 250 words and must clearly state the provisional title, the author(s), and a concise synthesis of the paper's scope, methodology, and principal arguments or findings.

The full papers should not exceed 8 pages or 5,000 words, inclusive of figures, tables, and references. Provisional acceptance will be based upon evaluation of the submitted abstract. Final acceptance will be granted following review and approval of the complete draft paper.

6. **Specific details:** First Announcement - Call for Papers: 10th of March 2026

Submission of an abstract and a CV by 15 July 2026
Authors advised of acceptance by 20 July 2026
Registration due date 15 September 2026
Papers/Presentations to be submitted by 19 September 2026
Conference: 23 to 24 September 2026

7. **Schedule:** The Conference will be held over two days, **from** Wednesda,y **23 to** Thursday, **24 September 2026**. Tuesday, 22 and Friday, 25 September should be considered as travel days. A provisional overview of the conference is as per Enclosure 1, while a final detailed Agenda will be issued in due course and will be regularly updated on the NMIOTC web page at: https://nmiotc.nato.int/nmiotc-annual-conferences/cyber-security-conference/

8. **Participants-Speakers**

Participation in the Conference is open to all relevant stakeholders and members of the wider Maritime Community. Distinguished speakers drawn from military organizations, academia, and industry will present their perspectives and professional assessments on the Conference themes. Attendance is particularly encouraged from officials and civilian representatives of NATO and NATO Partner Nations. The Conference seeks to ensure a diverse audience, including personnel from the Armed Forces, Law Enforcement Agencies, and staff officers from relevant Ministries (e.g., Foreign Affairs, Interior, Defence), as well as representatives of other governmental and non-governmental organizations engaged or interested in the cyber dimension of Maritime Security. Recipients are kindly requested to disseminate this invitation, as appropriate, to individuals and entities who may have an interest in attending or participating in the Conference.

9. **Classification:** The conference has no classification marking and all contents will be releasable to the public. **The conference will be held under the Chatham House Rules.**

10. **Attire:** The attire for the Conference will be summer service uniform or business casual (jacket & tie) for the military personnel and business casual for the civilians. The attire for the Dinner reception will be smart casual (jacket - no tie)

11. **Registration:** Participants are requested to sign up to our event portal in NMIOTC website https://nmiotc.nato.int or using directly the link https://nmiotc.classter.com/Actions/Registration. A signup confirmation message will be received to the email provided during the sign up process, along with the respective credentials. Login to https://nmiotc.classter.com and register to the 9th NMIOTC Conference on CyberSecurity in Marititme Domain by using the "Application Management" function at the top left corner of the portal main page. **Registration status can be verified within the portal**. If you encounter any problem during registration process, please contact studentadmin@nmiotc.nato.int or NMIOTC PoCs, mentioned in paragraph 18. Registration should be submitted ***NLT Monday 15 September 2026***.

12. **Lodging and Transportation:** Although attendees are responsible for the arrangement of their own accommodation and transportation from/to Chania International Airport, NMIOTC can provide assistance if requested. A list of recommended hotels can be found in Enclosure 2. Transportation to/from the NMIOTC premises and specified pick-up points in the city of Chania will be provided during the conference days. Detailed joining instructions will be issued in due course.

13. **Medical service:** First aid and emergency medical support is offered by NMIOTC paramedic and local Naval Hospital. However, for all other situations, medical expenses must be paid by the individuals or their insurance agencies. All participants are strongly advised to have appropriate medical insurance.

14. **Conference fee:** The Conference fee is **180€** for each attendee to cover Conference and administrative expenses. For the speakers, the fee will be reduced to **70€**.

The possible methods of payment are reported in the following table:

A.BEFORE THE MEETING/EVENT	INFORMATION	REMARKS
1.By Bank Deposit	NATIONAL BANK OF GREECE, NMIOTC BANK ACCOUNT 494/540010-48 SWIFT BIC: ETHN GRAA IBAN: GR3801104940000049454001048	Bank deposits should be completed not later than **2 working days before the start date of the event**, bank charges are not covered by NMIOTC. The receipt should be sent by email to papadakisst@nmiotc.nato.int and Cc mitsoulie@nmiotc.nato.int

2.By Debit/Credit Card	Upon notification from the participant, the direct link for credit/debit card payment will be sent to the designated-by the participant-email address.	The participant should send an email to papadakisst@nmiotc.nato.int and Cc mitsoulie@nmiotc.nato.int for receiving the link for the credit/debit card payment.
B. ON THE FIRST DAY OF THE MEETING/EVENT	**INFORMATION**	**REMARKS**
3. By Debit/Credit card	A valid credit/debit card should be presented on the first day of the event.	The fee is always paid in euros [the credit/debit card may provide the option to pay in another currency (other than euro) and therefore the 'euro' currency option must be chosen].
4. By Cash	-	The fee is always paid in euros.

15. **Social program:** NMIOTC will host a dinner reception on Wednesday, 23 September.

16. **Visa Requirements:** Participants or their supervising authorities are responsible for visa arrangements for their personnel. It is advised that participants should contact their national embassies/consulates in Greece or the Greek Military Attachés at the Greek Embassies in their respective capitals for relevant information.

17. **Remarks:** More detailed and updated information will be always available at the website of the centre: https://nmiotc.nato.int/transformation/conferences/cyber-security-conference/

18. **Points of Contact:** For further information or clarifications please contact:

Lead Conference Planner:
Captain (OF-5) Giuseppe CATAPANO ITA (N)
NMIOTC Director of Training Support
Tel +30 28210 85713(NCN:498-5713)
Email: catapanog@nmiotc.nato.int

Officer of Primary Responsibility (OPR):
Captain (OF-5) Dimitrios MEGAS GRC (N)
Director of Staff Operations / TS/IT Section Head
Tel +30 28210 85706-85711 (NCN:498-5706/11)
Email: megasd@nmiotc.nato.int

Website and registration POC:
Master Sergeant (OR-6) Ioanna STAMATAKI GRC (LG)
Students' Administration Affairs
Tel: +30 28210 85710 (NCN:498-5710)
Email: studentadmin@nmiotc.nato.int

19. Thanking you in advance for your support to the 10th NMIOTC Conference on Cyber Security in Maritime Domain, I look forward to welcoming you to Chania, Greece in September.

Commodore Pavlos Angelopoulos GRC (N)
Commandant NMIOTC

ENCLOSURES:

1. 10th NMIOTC Cyber Security Conference (23-24 Sep 2026) Provisional Agenda
2. List of Recommended Hotels in Chania

ENCLOSURE 1 TO:
NMIOTC NOTE: NU:34
NSC-74/ 10 March 2026

9TH NMIOTC CYBER SECURITY CONFERENCE (23-24 SEP 2026)
PROVISIONAL OVERALL AGENDA

1. The detailed Agenda of the conference is under development.

2. Overall Agenda

a.	Tue, 22 September 26:	Travel Day
b.	Wed, 23 September 26:	In-processing
		Opening Session
		Cyber Security Conference Day 1
		Ice-Breaker Reception
c.	Thu, 24 September 26:	Cyber Security Conference Day 2
d.	Fri, 25 September 26:	Travel Day

ENCLOSURE 2 TO:
NMIOTC NOTE: NU:34
NSC-74/ 10 March 2026

LIST OF RECOMMENDED HOTELS IN CHANIA

Accommodation: Participants are responsible to arrange their own accommodation as there is no accommodation facilities on the Centre's premises. NMIOTC can provide guidance / assistance, if requested. Hotels near Chania city centre are highly recommended for transportation purposes. The list of recommended hotels in Chania offering special prices and including breakfast and internet connection is as follows:

a. THE CHANIA 5* hotel www.thechaniahotel.com (Booking via email: reservations@thechaniahotel.com with reference to NMIOTC). Tel. (+30) 28210 90002.

b. HILTON Garden Inn 5* (Booking via email: reservations@hgichania.com and Dionysis.makastaridis@hilton.com with reference to NMIOTC).

c. AKALI 4* hotel www.akali-hotel.gr (promotional code "NMIOTC" via hotel's online booking platform or booking via email: info@akali-hotel.gr with reference to NMIOTC). Tel. (+30) 28210 92872.

d. KYDON 4* hotel www.kydon-hotel.com (promotional code "NMIOTC" via hotel's online booking platform) E-mail: info@kydon-hotel.gr Tel. (+30) 28210 52280.

e. SAMARIA 4* hotel www.samariahotel.gr (promotional code "NMIOTC" via hotel's online booking platform). E-mail: reservations@samariahotel.gr, tel. (+30) 28210 38600.

f. ARKADI 3* hotel www.arkadi-hotel.gr (promotional code "NMIOTC" via hotel's online booking platform), E-mail: info@arkadi-hotel.gr Tel. (+30) 28210 90181.

g. KRITI 3* hotel www.kriti-hotel.gr (promotional code "NMIOTC26" via hotel's online booking platform or booking via email: info@kriti-hotel.gr with reference to NMIOTC). Tel. (+30) 28210 51881.

h. PORTO VENEZIANO 3* hotel www.portoveneziano.gr. (Booking via email: hotel@portoveneziano.gr with reference to NMIOTC), tel. (+30) 28210 27100.