NORTH ATLANTIC TREATY ORGANISATION
NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE
NMIOTC
SOUDA BAY
73200 CHANIA
GREECE

5000 NSC-74/Ser.: NU: 81

TO: See Distribution List

SUBJECT: **INVITATION LETTER FOR CYBER DEFENCE TRAINING FOR BLUE TEAMS "GUARDIAN BLUE 2023 (GB23) - EMPOWERING THE DEFENDERS OF CYBERSPACE", 16 - 19 Oct 2023, 20 - 23 Nov 2023.**

DATE: 12 Aug 2023

REFERENCE: A. OCIO (2001) 0021 – NATO Cyber Adaptation, 9 December 2021
B. PO (2022) 0252 – Political-Military Advice for a Framework on the Implementation of Defensive Cyberspace on NATO Networks, 10 June 2022
C. OCIO (2022) 0133 – Cyber Adaptation Roadmap Annex 7 – Defensive Cyberspace Operations (DCO), 25 December 2022
D. NMIOTC Program of Work 2023 (NPOW 2023)
E. MC 0458/4, NATO Education, Training, Exercise and Evaluation (ETEE) Policy (Final), dated 3 January 2023
F. Bi-SC 075-007, Education and Individual Training Directive

1. NMIOTC in coordination with SHAPE Cyberspace Directorate and in support of NATO Cyber Adaptation Roadmap as Ref C, is organizing a cyber security training for NATO Blue Teams (BTs) that will take place virtually, in two identical iterations during October and November 2023 for eight (8) BTs in each iteration.

2. The aim of the training is to provide a **unique** training opportunity to Cyber Security BTs where they can get acquainted with the latest cyber-attacks, advanced cyber defence tactics, techniques, and best cyber defence practices. Main training objective is to incrementally build and improve the cyber defence skills of the participant BTs' members at scale using a hands-on and distributed online virtual training model.

3. Training participants will be able to apply their newly acquired skills immediately after the training at the tactical, operational, and/or strategic levels. Training participants will be trained, in a highly interactive manner, on how to recognize a cyber-attack, and develop Cyberspace Situational Awareness. They will receive recommendations on responses and advice on how to evaluate strategies, tools, procedures, and how to effectively collaborate with other team members

4. The training audience is **Cyber Security BTs'** personnel from NATO member countries**.** Due to the limit in the number of BTs per iteration, the selection of the BTs

attending each training iteration will be under the responsibility of SHAPE's Cyberspace Directorate based on the BTs timely registration order.

5. **Training Schedule:** The duration of each training iteration will be four (4) days:

a. Three (3) days of hands-on, virtually guided technical BTs' training.
b. One (1) day of simulated live-fire exercise-type cyber-attack scenarios and BTs' evaluation and assessments.
c. The training will take place from 09:00 - 16:00 CET (GMT+2) every day including time for a lunch/coffee break.
d. Iterations:
   (1) 16-19 October 2023
   (2) 20-23 November 2023
e. A detailed daily Schedule of Events (SoE), administrative details, training specifications, guidelines for the training environment, and further directions will be promulgated promptly before training dates in a Joining Instructions document, for better preparation and familiarization of the participant BTs' members.

6. **Training Description:** For the preparation and conduct of the aforementioned training the following team structure will be followed:

a. **Blue Teams (BTs)**

BTs are the main training audience. Trainees (BT members) – are required to learn how to defend a pre-built network consisting of virtual machines (cyber range) resembling an HQ network against the Red Team (RT - simulated hackers/adversaries). The BTs' role is to preserve the integrity, confidentiality, and availability of their organization's IT services, CIS infrastructure, and cyberspace in general. BTs are expected to participate in the training **from their own facilities. No traveling will be required**. The maximum number of participant BTs per training iteration is eight (8), consisting preferably of 6-10 members per BT.

b. **White Team (WT)**

The WT has a key role in designing and preparing the training and controlling the exercise's scenarios during 4th day's exercise execution. The WT defines the training objectives, and the scenario develops the attack campaign together with the RT and defines the rules of 4th day live-fire exercise. During the execution phase, the WT acts as the exercise controllers' cell. They decide when to start different phases, control the execution of the RT's attack campaigns, and make scoring/assessment decisions.

c. **Red Team (RT)**

The RT's mission is to compromise or degrade the performance of the systems that are protected by BTs and to teach the training participants how to detect cyber-attacks and respond. Members of the RT are basically the instructors/trainers

throughout the whole training iteration. RT members are also mainly considered as the 'work-force' to challenge the BTs during 4th day exercise scenarios.

d. **Green Team (GT)**

The GT is responsible for preparing and configuring the cyber range technical infrastructure which will be used in the training. The main tasks for the GT include:

(1) Designing and setting up the core training infrastructure/environment: computing nodes, virtualization platform, storage, and networking.
(2) Setting up routing and remote access to the training environment.
(3) Designing and building BT networks.
(4) Programming the automatic scoring/assessment bot and agents.
(5) Setting up solutions that are required for monitoring the general training infrastructure.

7. **Training Learning Objectives:**

a. To train BTs' members in monitoring CIS and identify cyber-attacks using the right tools and well-recognized frameworks like MITRE ATT@CK Framework.
b. To train and exercise:
(1) the cyber defence skills of the participating BTs.
(2) the collaboration and synergy among the members of a BT.
(3) on different cyber-attack use case scenarios and assess the effectiveness of participant BT's responses.
c. To introduce and advice participating teams on the latest cyber-attacks and best cyber defence practices.

8. The training will be conducted in English. Translation to/from other languages will not be provided. The following proficiency standards in English (as described/ coded in STANAG 6001) are required to follow the training content: Listening – Professional (3), Speaking – Functional (2), Reading – Professional (3) and Writing – Functional (2) (STANAG 6001).

9**.** **Registration:**

Participant BTs are kindly requested to register by filling out the Registration Form below and sending it by email directly to the Training Director with Cc the SHAPE J6 POC and Registration POC in paragraph 11, **NLT 11th of Sep 2023. The registration is FREE of charge.** A BT Leader must be identified for coordination and effective collaboration with the training organizers before and during the training conduct.

Registration Form	
Cyber Security Blue Teams Training 2023 (16-19 Oct 23, 20-23 Nov 23)	
NATO Member Country	BT's Country
Organization	BT's Organization
Blue Team Leader	Rank/ Title, First-Last Name, email: Tel.:
Estimated number of BT members	The estimated number of BT members will be engaged in training (Preferably between 6 - 10)
Preferred Training Iteration	16-19 Oct 2023 or 20-23 Nov 2023

10. **Training Classification:** The training content is marked as "NATO Unclassified''

11. **Point of Contacts (POCs)**:

a. **Training Director** : Captain (OF-5) Periklis Pantoleon GRC (N)
Phone : (+30) 2821085716, NCN: 498-5716, Fax: (+30) 28210 85702
Mobile : (+30) 6943482491
e-mail: pantoleonp@nmiotc.nato.int (NU)
pantoleonp@nmiotc.grc.nato.int (NS)

b. **SHAPE J6 POC** : Mr Emmanouil Christofis
Phone : +32 6544 3287 (Office) NCN: 254 3287 ,
e-mail: emmanouil.christofis@shape.nato.int (NS/NU)

c. **Registration POC** : Cdr (OF-4) Konstantinos Papanastasis GRC(N)
Phone : +30 28210 85710 (Office), NCN : 498-5710,
e-mail : papanastasisk@nmiotc.nato.int; studenadmin@nmiotc.nato.int

Themistoklis Papadimitriou
Commodore GRC(N)
Commandant NMIOTC

DISTRIBUTION LIST
EXTERNAL:

ACTION:

LIST III A. IV, V, VI, VII, VIII, IX, X, XII, XIII, XV, XVI, XVII, XIX
LIST XI N

HQ NATO HEL MILREP

INFORMATION

HNDGS/B2
HNDGS/D4
HNDGS/E5
HNGS/B2
HNGS/A4

INTERNAL:

Action:
DIR E&T
SAA
DIR S (FOR B&F)

Information:
DCOM
COS
DIR TS
DOSO