HELLENIC ARMY ACADEMY
SUPERINTENDENT

Subject: Formal Invitation to Participate in Common Module: Cybersecurity

Dear Partners,

On behalf of the Hellenic Army Academy, I extend a formal invitation to your esteemed institution to participate in our upcoming Common Module: ***Cybersecurity***, scheduled to take place from ***May 27 to May 31, 2024***.

The goal of this module is to familiarize participants with the evolving threats and challenges in the information society, with a specific focus on cyber attacks, encompassing the fundamentals of malwares and information-based attacks, along with their methods. Our aim is to present a comprehensive understanding of cyber security, ensuring participants acquire knowledge on international and national cyber security strategies.

The learning outcomes of the module include developing basic knowledge of emerging cyber threats, understanding complex cyber security principles, and gaining insight into the foundational aspects of international and national cyber security strategies. Participants will acquire skills such as identifying cyber threats, describing the fundamentals of malwares and information-based attacks, and recognizing tools to enhance personal and organizational cyber security. Competencies attained involve the capacity to recognize and address cyber threats effectively, establish fundamental cyber security defenses, and consider avenues for the ongoing development of cyber security capabilities.

We believe that your institution's participation will significantly contribute to the depth and diversity of discussions, enhancing the overall success of the module. Kindly confirm your institution's participation at your earliest convenience. Should you have any questions or require further information, please do not hesitate to contact us.

Looking forward to your positive response.

Sincerely,

Anastasios Polychronos
Major General

ANNEX "A"

Course Agenda

Main Topic	Details
Day 1: Cyber Security Organizations and standards	National and international cyber security organizations and standards in practice
Day 2: Cyber attacks	Attacking methods: DoS, DDoS, APT, Social Engineering, EW attacks (directed energy)
	Identifying of malwares and other attacks
Day 3: Cyber Security tools	Basics of personal cyber security tools on individual workstations
	Personal firewalls, anti malwares, secure use of workstation
	Ensuring cyber security on networks
	Firewalls, network tools
	Cyber security and social media
Day 4: Case studies	Analysing known cyber incidents, identifying attack vectors and the possible steps to prevent similar cases