1. Course Title

Cyber Defence - NATO Cyber Defence Advisor Course

2. Identification Number (ID)

730

3. Purpose of the Course

The purpose of this course is to provide students with the high-level knowledge, skills and experience required for describing and evaluating the risks and threats of cyber space, improving cyber defence measures and providing advice to decision makers.

The student will be able to re-assess the risks and opportunities during the planning, preparation and execution of operations, elaborating operational risk and opportunities.

This course will provide the required knowledge and training for staff from NATO Headquarters, NATO Commands, NATO MoDs, and NATO Agencies appointed to ...

4. Learning Objectives

Upon completion of the course, the qualified student will be able to successfully describe, and provide advice on:

- CIS & Vulnerabilities (inside and outside NATO)
- Critical Infrastructure & Vulnerabilities (outside NATO but impacting NATO Mission)
- Cyber Threats and Mission Risks from CIS & Critical Infrastructure
- NATO CD & Policy
- NATO (Cyber) Intelligence and Mission Risks
- NATO Cyber Defence Legal issues and Risks
- NATO Cyber Defence Capabilities and Measures
- NATO Cyber Defence in Operations (Situational awareness, Assess, Advise)
NATO Cyber Defence Advice (case study 1, case study 2)

5. Qualification

NATO Cyber Defence Advisor

6. Student Criteria

The student will be accepted on the course if he/she meets all of the following criteria:

1. The student has been assigned or selected for assignment to a NATO HQ, or a NATO Agency, or a NATO Unit or earmarked for assignment to a NATO post.

2. The student has been assigned to a post fulfilling the roles and responsibilities of Security Manager Staff or CIS Security (INFOSEC/COMPUSEC) Staff.

3. The Student requires to meet the Background Knowledge Prerequisites for this course (see point 16).

7. Rank

The student has to hold a rank between OF-2 and OF-5 or Civilian equivalent.

This restriction is to ensure that the course correctly targets a suitable audience in order to achieve its aim.

8. Language Proficiency

According to STANAG 6001: English SLP 3232

9. Security Clearance

NATO SECRET (Minimum).

The student has to hand-carry a duly filled in and signed original of the NATO Security Clearance Certificate (see AD 70-1, Part IV, Chapter 1, Annex D). This is primarily for facility access.
10. Course Length

7 working days (first 2 days will be delivered via e-learning)

11. Special Instructions

None

12. Class Size (Maximum/Recommended/Minimum)

20 / 15 / 12

13. Nomination Procedure

www.nciss.nato.int

14. Pre Course Study Material

Students should be aware of the contents of the following policy documents:

  This is a good reference for non-ACO personnel.

15. Location

The course is conducted at the NATO Communications and Information Systems School (NCISS), Latina, Italy.
16. Background Knowledge Prerequisites

The student must have successfully completed either:

- CIS Officers (NCISS ID 101 or 103) or
- FULFILL all the Essential Prerequisites

**Essential Prerequisites:**

- Basic knowledge of CIS networks within a NATO/National environment.
- Familiarity with NATO/National security publications

**Desirable Prerequisites:**

- [ ]