CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

NATO CCDCOE TRAINING CATALOGUE, 2025

training@ccdcoe.org

www.ccdcoe.org

Foreword

It is my pleasure to present the 2025 Training Catalogue for the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). With these education and training offerings, the NATO CCDCOE continues its tradition of quality and advances its mission to enhance the capability, cooperation, and information sharing between NATO, its Member Nations, and its partners in cyber defence.

In this 2025 Training Catalogue, you will find relevant, engaging and state-of-the-art training solutions that will enhance the cyber defence capability within NATO and the NATO CCDCOE's Sponsoring Nations and Contributing Participants. A core belief at the NATO CCCOE is that education and training are the foundation for a robust and agile cyber defence community.

Our meticulously curated training activities have been developed by subject-matter experts from the NATO CCDCOE, international organisations, and industry to provide the knowledge, methods, techniques, and best practices that empower our training audience to *face cyber threat as a coalition*.

To best meet the training needs of the North Atlantic Treaty Organisation as well as the Centre's Sponsoring Nations and Contributing Participants, we provide courses in a variety of formats and locations, covering a broad range of topics within the technical, legal, strategic, and operational cyber defence domains. In addition, we complement our education and training by organising a variety of workshops, conferences, and exercises.

With all of the developments and activities at the NATO CCDCOE, please be aware that some details of the training program, in particular the dates, may be subject to change. Therefore, it is advisable to check the latest information on our website: https://ccdcoe.org/training/.

I would like to express my sincere gratitude to all those involved in the preparation of these training activities and exciting developments for the NATO CCDCOE. Training and education can often be complex endeavour and I could not be prouder of the Centre's staff and partners.

Dr. Mart Noorma

Director of NATO Cooperative Cyber Defence Centre of Excellence

Tallinn, Estonia

Contents

Introduction

The 2025 training portfolio is composed of:

- 10 face-to-face courses, including two NATO-approved, which can be delivered in Tallinn (residential) or at a location requested by a nation (mobile). They cover technical, legal and operational areas within cyberspace;
- 16 e-learning courses, including one NATO-approved, hosted on the NATO JADL platform;
- 1 seminar aimed at executive level (non cyber experts);
- 2 cyber exercises (Locked shields and Crossed Swords);
- 1 technical workshop that is directly linked to our exercises; and
- the Cyber Conflict annual conference (CyCon).

What is new in 2025:

About the portfolio:

- CCDCOE will deliver in June 2025 the pilot course of the Cyber Threat Intelligence that is aimed at Intelligence practitioners. We plan to have the first iteration, opened for all students, at the end of the second semester (see details in the catalogue). Please note that the course lasts 2 weeks.

- We are also revising our Critical Information Infrastructure Protection course (CIIP) tat will be more cyber-focused and will take more insights from our Europeans partners. The new course will be delivered in May 2025 (see details in the catalogue).

- Unfortunately our Cyber Defence Monitoring Course in not available in 2025.

About the registration process:

- All courses are already open for registration. As previously done, registration will close 2 months before the course and priorization will be made.

- Our priorization is based on different factors such as :

  * fair distribution of seats among the CCDCOE member nations (one free seat is always offered to each CCDCOE member nation)

  * Statistics of previous attendance;

  * Adherence to the target audience. If the student is not in the target audience, his/her participation can be denied. Indeed, under skilled students can hamper the achievement of the learning objectives of the rest of the audience.

Please, pay attention to the target audience and the prerequisites.

Our training solutions are a resource for Sponsoring Nations (SNs) and Contributing Participants (CPs) of the Centre as well as for NATO entities.

Students from other nations can attend the courses upon CCDCOE Steering Committee approval. Requests can be submitted to training@ccdcoe.org .

This catalogue provides an overview of all scheduled activities for 2025 as well as the intended target audience, objectives, prerequisites and basic administrative information (joining instructions).

Please be aware that some part of the training programme, in particular the dates, may be subject to change. Therefore, it is advised that you check the latest information on our website: https://ccdcoe.org/training/.

What we offer

Residential (In-house) training

We create an interactive learning experience. Our instructors deliver knowledge, innovative techniques and useful tips by combining expertly-designed lectures with software demonstrations and hands-on sessions.

In 2025, 10 courses (16 iterations), an executive seminar and a technical workshop are planned to be held in Tallinn (new CCDCOE premises, located at Filtri tee 5).

As part of our business continuity plan, we keep the possibility to deliver some courses be held online but only in exceptional circumstances (ex: COVID).

Technical Trainings

1. Malware and Exploits Essentials Course (2 iterations).
2. Exploit Advanced Course (1 iteration);
3. IT Systems Attacks and Defence Course (1 iteration).
4. Reverse Engineering Malware Course (2 iterations);
5. Introductory Digital Forensics Course (1 iterations);
6. Industrial Control Systems Security Introductory Course (1 iteration)

Operational Level Training

7. Integrating Cyberspace Considerations into Operational Planning Course[1] (2 iterations).
8. Critical Information Infrastructure Protection Course (1 iteration).
9. Cyber Threat Intelligence Course (pilot + 1 iteration)

Legal Training

10. International Law of Cyber Operations Course1 (3 iterations).

Strategic Level Training

11. Executive Cyber Seminar (2 iterations)

Technical workshop

12. Locked Shield Forensics workshop (hybrid: residential/online)

[1] NATO-approved course

Mobile training

The same quality content and instruction as our in-house training can also be delivered as mobile training. This is a convenient option, offering Sponsoring Nations and Contributing Participants an efficient way to train a group of personnel in a short time. In 2025, 4 courses (6 iterations) are planned to be held at the Centre's member or NATO locations:

1. Integrating Cyberspace Considerations into Operational Planning (Spain, Chechia, Slovenia);
2. IT Systems Attack and Defence Course (Latvia);
3. Reverse Engineering Malware Course (Latvia)
4. Industrial Control System Security Introductory Course (Latvia)

The possibility to deliver a mobile iteration of the new version of the Critical Information Infrastructure Protection Course is pending.

e-Learning courses

All CCDCOE e-Learning courses are hosted on the NATO ACT Joint Advanced Distributed Learning Portal (JADL, https://jadl.act.nato.int). As of 1st November 2024, there is no possibility for non-NATO members to access the JADL platform.

Registration

As per NATO ACT regulations, a NATO-Military, Governmental or NATO official email is required for registration.

For Non-NATO members, the access to JADL is no longer available as of October 2024. A new solution, approved by NATO authorities, is pending. CCDCOE is trying to mitigate this situation.

e-learning Portfolio

The 2025 e-Learning portfolio is:

1. ADL 076 Cyber Defence Awareness (NATO-approved)
2. ADL 230 Operational Cyber Threat Intelligence Course[2];
3. ADL 335 Cyber Awareness course for System Administrators;
4. ADL 343 Information Security Management System (pre-learning module for the Critical Information Infrastructure Protection Course);
5. ADL 344 Digital Forensics and Digital Evidence (pre-learning module for the Introductory Digital Forensics Course);
6. ADL 345 Network and Log Monitoring (pre-learning module for the Cyber Defence Monitoring Course);
7. ADL 346 Web Application Security Course;
8. ADL 347 Critical Infrastructure and Industrial Control Systems (pre-learning module for the Industrial Control Systems Security Course);
9. ADL 348 Fighting a Botnet Attack: a Case Study Course;
10. ADL 349 Systematic Approaches to the Mitigation of Cyber Threats ;
11. ADL 365 Cyber Awareness Course Tallinn Manual Module (pre-learning module for the International Law of Cyber Operations Course);
12. ADL 375 pre-learning module for Integration of Cyber into Operational Planning Course;
13. ADL 383 pre-learning module for the Malware and Exploits Essentials Course;
14. ADL 394 pre-learning module for the IT Systems Attacks and Defence Course;
15. ADL 420 pre-learning module for the International Law of Cyber Operations Course; and
16. ADL 430 pre-learning module for the Cyber Defence Monitoring Course.

[2] Even though the residential OCTIC is no longer active, this e-learning module is still relevant

Administrative considerations

Entry to Estonia

Citizens of Member States of the European Union and the European Economic Area and of the Swiss Confederation must have with them:

1. Passport or identity card;
2. If you are a member of the Armed Forces (military or civilian component), individual or collective movement order in English, issued by an appropriate agency of the sending state or of NATO, certifying the status of the individual or group as a member or members of the Armed Forces and the movement ordered (NATO Travel Order for NATO nations)

Citizens of other nations:

1. Passport or Armed Forces identity card;
2. If you are a member of the Armed Forces (military or civilian component), individual or collective movement order in English, issued by an appropriate agency of the sending state or of NATO, certifying the status of the individual or group as a member or members of the Armed Forces and the movement ordered (NATO Travel Order for NATO nations)
3. If you are NOT a member of the Armed Forces, a visa could be required in addition to the identification document. Link to the visa requirements

Accommodation

Students will receive the negotiated fixed hotel room rates and booking instructions for each of these hotels along with the course confirmation email. Please note that fixed room rates are subject to limited availability and prices may vary throughout the year (depending whether it is high or low season).

The following hotels are located close to our training venue (new CCDCOE building) located at Filtri tee 5.

1. **Hestia Hotel Kentmanni 4**

   https://www.hestiahotels.com/kentmanni/en/

   Address: Kentmanni 13, 10116 Tallinn

2. **Ibis Tallinn Center Hotel**

   https://www.ibistallinncenter.ee/

   Address: Juhkentali 28, 10132 Tallinn

3. **Radisson Blu Hotel Olümpia**

   https://www.radissonhotels.com/en-us/hotels/radisson-blu-tallinn-olumpia

   Address: Liivalaia 33, 10118, Tallinn

4. **Hilton Tallinn Park Hotel**

   https://www.hilton.com/en/hotels/tllhihi-hilton-tallinn-park/rooms/

   Address : F. R. Kreutzwaldi 23, 10147 Tallinn

Transportation

There is no transportation provided by the NATO CCDCOE. Course participant is responsible for its own transportation between the airport, hotel and course venues.

Information about the public transport in Tallinn can found here.

Lennart Meri Tallinn Airport is located 4 km from the city centre.

By taxi: a taxi stand can be found just outside the airport´s arrivals hall. The fare from the airport to the hotels is between €5 to €10. Read more about Tallinn's taxis here.

By tram: Tram no 4 from the airport to the city centre operates on a frequent schedule, the tram stop is located next to the airport terminal towards the city. More detailed information in this link.

Lunch

CCDCOE offers the possibility to use the Estonian Defence Forces military canteen **only if booked during the registration process**. The canteen is located at Filtri tee 12 Tallinn (5-min walk from CCDCOE building).
Please be aware that we cannot guarantee the availability of specific dietary options.

Additionally, there is a limited choice of restaurants and food points close to the CCDCOE and there is no designated eating area in the CCDCOE premises.

CCDCOE doesn't use disposable cups anymore. Therefore, in order to use the water machine in the course venue, course participants must bring their own water bottle. Otherwise, they have the opportunity to buy a water bottle onsite (5 Euros).

Both coffee/water cups can be paid either via bank transfer when ordered during registration or paid by card during the in-processing (8h30-9h on Mondays).

Dress code

Smart casual and uniform are acceptable.

General course schedule

Day 1 - Day 4 (Monday – Thursday)

08:30-09:00 In processing (only on Monday)
09:00 1st Session
10:30 Break
10:45 2nd Session
12:00 Lunch Break
13:00 3rd Session
14:30 Break
14:45 4th Session
16:30 End of course day

Day 5 (Friday)

09:00 1st Session
10:30 Break
10:45 2nd Session
12:00 Lunch Break
13:00 3rd Session
15:15 End of course

Registration

Before registering, please check the up-to-date information on the NATO CCDCOE website.

General procedure:

1. The potential applicants need a Registration Code. These codes are shared with the official Education & Training POCs of each nation. Please note that each Registration Code change after each course iteration.
2. Each nation is entitled to one free seat for each iteration of a course. The applicant needs to insert the Discount Code at the end of the registration process. The Discount Code is only shared with the official Education & Training POCs (see list in Annex B).

Registration for all 2025 courses are opened as of 1st November 2024. They close 9 weeks before the course.

8 weeks before the course, when the priorization process is over, CCDCOE will approve the participation of the registrants. They will received a confirmation email including all admistrative details.

Getting around in Tallinn

Please find below links to websites providing information you might need:

- Tallinn map
- Public transportation timetable
- Tallinn comprehensive overview
- What to do
- Weather

Contact

For more detailed information please contact:

- training@ccdcoe.org
- events@ccdcoe.org

Training costs

Residential courses

Residential courses costs are composed of:

1. Course fee[3]: **500 €** (Sponsoring Nations, Contributing Participants and NATO bodies are offered 1 free seat per iteration); and
2. Lunch service (optional) : **30 €**
3. Coffee service (optional) :
    - **15 €** (includes the CCDCOE reusable coffee cup);
    - **10 €** (if the students use their own coffee cup).

The payment of course fee is required before the course. It can be paid either via bank transfer (invoice and bank details are provided in the confirmation email) and exceptionally by card during the in-processing (8h30-9h on Mondays).

The seat allocation will be approved when the course fee is paid.

E-Learning

E-learning (https://jadl.act.nato.int/) is free of charge.

Mobile courses

The Centre does not charge any course fee for mobile trainings. However, the requesting entity must cover all expenses associated with the planning and conduct of the mobile iteration itself, including (but not limited to): travel, accommodation and per-diem.

[3] Under exceptional circumstances, some of residential courses can be performed online. In that case, the course fee still applies.

Cancellation regulation

In order to cancel their participation, the students must send an email to: events@ccdcoe.org or training@ccdcoe.org

In that case :

- the course fee will be refunded;
- the lunch service fee will be refunded unless the cancellation occurs 2 weeks prior to the course.

Note: if the lunch fee had not been paid during the registration, it is still due. Student are then requested to pay it via bank transfer.

Residential (In-house) trainings

Cyber Threat Intelligence Course (CTI)

First iteration: 27 October - 07 November 2025

Registration deadline: 5th September 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

The aim of the course is to provide national intelligence practitioners with the skills and knowledge required to contribute to the development of an collection plan, collect the relevant information, analyse the collected information and then disseminate the information using the proper products.

Learning Objectives

1. Develop a Plan using the Intelligence Planning Process
2. Maintain an information data base IAW the collection plan
3. Analyse information using one or more analytical model
4. Disseminate Cyber Threat Intelligence products

Target Audience

Intelligence practitioners filling primarily intelligence roles in national military organization and civilian authorities or institutions who has been designated to work in a Cyber Operations Centre or civilian equivalent

Outline

1. Refresher on the Intelligence Cycle
2. Introduction to Cyberspace Intelligence
3. Integration of Cyber Intelligence into Cyber Operation
4. Legal Considerations in Cyber
5. Internal sources of information in Cyber Threat Intelligence
6. External sources of information in Cyber Threat Intelligence
7. Cyberspace Intelligence Tools
8. Credibility and Reliability in Cyberspace
9. Introduction to Analytical Methods
10. Application of Analytical Methods
11. Information Sharing
12. Cyber Intelligence Products

Prerequisites

Under revision The course has a mandatory e-learning module (ADL 230 “Operational Cyber Threat Intelligence Course”, see the details in the “e-Learning courses” chapter).

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 230 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Malware and Exploit Essentials Course (MExEC)

First iteration: Date: 17 - 21 February 2025

Registration deadline: 13rd December 2024

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Second iteration: 01-05 September 2025

Registration deadline: 4th July 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

The Malware and Exploit Essentials course will provide deep technical insights for cyber defenders into techniques that malware uses to exploit vulnerabilities and to intrude into systems. Based on an introduction to OS features and analysis techniques, the use of debuggers as the most important tools for exploit research and methods for vulnerability detection like fuzzing will be discussed and then trained in hands-on exercises.

Learning Objectives

1. Use a debuggers (GDB, Immunity Debugger, WinDBG);
2. Basic exploitation techniques on Linux and Windows systems;
3. Introduction to fuzzing;
4. Operate system mechanisms such as ASLR, SEH and DEP and how they get bypassed;
5. Basic static (IDA Pro), dynamic (OllyDbg) and behaviour analysis on different malware samples; and
6. IOC's writing (Yara).

Target Audience

Technical staff of CERTs, IT departments or other governmental or military entities being involved in technical IT security or cyber defence.

NB! Please be aware of the strong technical nature of this course: **this is not a course for beginners**. The presence of unskilled attendees is likely to hinder the overall progress of the course.
Therefore, the CCDCOE will not accept students with the inappropriate background.

Outline

1. Introduction:
    a. Course Introduction.
    b. Malware and Exploits – basics and definitions.
2. Modern OS environment:
    a. Creating a program.
    b. Compilation, linking, shared libraries, sections of program.
    c. Assembly introduction, AT&T vs. Intel syntax, endianness.
3. Debuggers:
    a. Static and dynamic program analysis.
    b. Getting info about binaries.
4. Buffer overflows:
    a. Concept of stack frame and local variables of function.
    b. Buffer overflows without ASLR and NX/XD techniques.
    c. Return-to-system and chaining.
5. Protective mechanisms and common exploitation ideas:
    a. Canaries, non-executable stack.
    b. Structured Exception Handler (SEH).
    c. Address space layout randomization (ASLR).
    d. Data Execution Prevention (DEP)
    e. Return-Oriented-Programming (ROP)
6. Examining static properties of suspicious programs
    a. Static analysis (IDA Pro)
7. Performing behavioural analysis of malicious Windows executables
    a. INetSim, FakeDNS, Wireshark
8. Performing dynamic code analysis of malicious Windows executables
    a. Dynamic analysis (OllyDbg, WinDgb)
9. Determining the network and host-based indicators (IOC)
    a. IOC's writing (Yara)

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 383 "Malware and Exploit Essentials Course", see the details in the "e-Learning courses" chapter).
2. Good work/administration experience in the Linux and Windows environments, especially command line.
3. Basic understanding of assembler and higher programming languages.

4. Programming experience in assembler, C (++) or PYTHON.
5. English language skill comparable to STANAG 6001, 3.2.3.2.

ISACA CPEs

With the completion of this course the students can earn **35** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 383 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Exploit Advanced Course (ExAC)

Date: 02-06 June 2025

Registration deadline: 28th March 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

This 5-day course will provide a very practical training for skills needed in exploitation research and malware analysis. We will start by developing the knowledge of techniques learned in the "Malware and Exploit Essentials Course" further and strengthen the practical experience with them. Advanced topics (like Heap memory or Kernel) will then be introduced and trained in hands-on tasks to understand how these techniques work and help to better defend against them.

Learning Objectives

1. Introduction to advanced exploitation techniques on Linux and Windows systems;
2. Exploitation in Heap memory;
3. Introduction for Kernel exploitation;
4. Advanced static and dynamic analysis of binaries.

Target Audience

Technical staff of CERTs, IT departments or other governmental or military entities being involved in technical IT security or cyber defence.

NB! Please be aware of the strong technical nature of this course: **this is not a course for beginners**. The presence of unskilled attendees is likely to hinder the overall progress of the course.
Therefore, the CCDCOE will not accept students with the inappropriate background.

Outline

1. Refresh and extend basic skills
    a. Buffer overflows
    b. ASLR bypass
    c. ROP Chain

   d. Static and dynamic analysis
2. Advanced exploitation techniques
   a. Windows
   b. Linux
3. Introduction to exploitation in heap memory
4. Kernel exploitation
5. Mitigation mechanisms against Exploitation in operating systems
6. Advanced static and dynamic analysis

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 383 "Malware and Exploit Essentials Course", see the details in the "e-Learning courses" chapter).
2. "Malware and Exploit Essentials Course" or good and practical knowledge about the basic techniques in Exploit Research.
3. Good work experience in Linux and Windows environments, especially command line.
4. Understanding of assembly and higher programming languages.
5. Programming experience in assembly, C(++) and/or PYTHON.
6. English language skill comparable to STANAG 6001, 3.2.3.2.

ISACA CPEs

With the completion of this course the students can earn **35** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 383 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Reverse Engineering Malware Course (REMC)

Date: 17-21 March 2025

Registration deadline: 10th January 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

The content of this course has been transforming over time constantly as the current hot topics related to malicious code is constantly changing. This iteration will be focused on reverse engineering skills, information exchange and building skills for improving existing response infrastructure with real-time event processing technology.

Learning Objectives

1. Understanding malware: life-cycle and motivation of their creators;
2. Identifying malware related activity in endpoints and networks;
3. Autonomously collect information and analyse samples from multiple stages of malware;
4. Producing and using indicators of malware related activity; and
5. Identify and search for IoC's.

Topics

1. Malware Lab Setup;
2. Static Properties Analysis;
3. Emulators;
4. Behavioural Analysis;
5. Malware Network Interactions;
6. Core Assembly Concepts;
7. Static Code Analysis;
8. Dynamic Code Analysis;
9. IDA;
10. Packers;
11. Loaders;
12. Shellcodes; and
13. Dynamic API Resolution.

Target Audience

Cyber security technical staff (CERT, IT departments, etc.) seeking to become familiar with malware analysis and related topics.

NB! Please be aware of the strong technical nature of this course: **this is not a course for beginners**. The presence of unskilled attendees is likely to hinder the overall progress of the course.
Therefore, the CCDCOE will not accept students with the inappropriate background.

Prerequisites

1. Knowledge of Windows internals and how operating systems functions;
2. Familiarity with programming language like C or Python;
3. Basic understanding of assembly language;
4. Basic knowledge of networking concepts; and
5. Understanding of general cybersecurity principles.

Pre-study e-Learning material

1. Malware Reverse Engineering Handbook from the CCDCOE website
2. Recommended: ADL 348 (Fighting a Botnet Attack: a Case Study) and ADL 349 (Systematic Approaches to the Mitigation of Cyber Threats) on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

ISACA CPEs

With the completion of this course the students can earn **35** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

IT Systems Attack and Defence Course (ITSAD)

Date: 20 - 24 October 2025

Registration deadline: 22nd August 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

IT Systems Attack and Defence is a practical 5-day course, intended for system administrators, developers and other technical personnel. The course introduces tools and methods used by attackers to gain access to IT systems and discusses potential countermeasures and ways of detection. A large part of the course is based on hands-on exercises. Practical tasks focus mainly on the offensive side of IT security, the participants can try out for themselves how various real-world attacks can be conducted. In addition, participants can take part in a Capture the Flag competition, where points are awarded for successfully completing the hands-on tasks, with bonus points awarded for the fastest students.

Students will be provided with virtual machines based on Kali Linux. The majority of the tools used in the class are free or open-source. The vulnerable web applications are built using mostly PHP and MySQL. The course does not focus on specific technologies, but rather uses them as an example for certain classes of attacks.

The course introduces students to the way penetration testers and hackers think. Practical work is used to further develop this kind of thinking and also to figure out ways how to defend against these kinds of attacks. The course does not go in-depth into specific vulnerabilities, rather it serves as a broad introduction into IT systems attacks and points the students towards material where to learn further.

Learning Objectives

1. Conduct reconnaissance;
2. Identify vulnerabilities; and
3. Exploit vulnerabilities in custom-built web applications.

Outline

1. Introduction of the lab environment. The basics of Kali Linux and Metasploit;
2. Phases of a cyber-attack:
    a. Reconnaissance.
    b. Scanning and Enumeration.
    c. Gaining Access.

d. Privilege Escalation.
e. Lateral Movement.

3. Reconnaissance: sources and tools for gathering information about target networks;
4. Network scanning: host discovery, TCP and UDP port scanning, operating system detection, vulnerability scanning, scanning in IPv6 networks, honeypots and tarpits;
5. Enumeration: using DNS, SNMP and other protocols to identify potential vulnerabilities;
6. Credential attacks: password guessing and cracking, how passwords are stored in IT systems, hashing functions and identified vulnerabilities in them, Rainbow Tables, best practices for password security;
7. Network infrastructure attacks and defence: MAC flooding, ARP spoofing, ICMP redirection, IP spoofing and fragmentation, VLAN hopping, leaking data over CDP, BGP hijacking; port security, DHCP snooping and dynamic ARP inspection, private VLANs, 802.1x;
8. DNS security: DNS overview, DNS tunnelling, DNS rebinding, DNS snooping, cache poisoning attacks, DNSSec;
9. Windows Security: Pass-the Hash, Pass-the-Ticket, Kerberos 'Silver and Golden Ticket Attack', Authentication methods, Security mechanisms, Privilege escalation, Process injection;
10. Web Application Security:
    a. Main building blocks of web applications;
    b. Session management and authentication attacks;
    c. Injection attacks:
        (1) SQL injection;
        (2) OS command injection;
        (3) File inclusion; and
        (4) Insecure file upload functionality.
    d. Cross-site scripting; and
    e. Cross-site request forgery.

Theoretical lectures are supported by sets of practical exercises. These allow the students to conduct different tasks such as:

1. Using various open-source or freely available tools for information gathering from public sources.

2. Scanning small networks to finding alive hosts or machines with specific vulnerabilities.
3. Using DNS enumeration to find interesting hosts, exploiting unprotected SNMP service for enumeration of information.
4. Tunnelling arbitrary IP traffic over DNS protocol in restrictive environment.
5. Guessing and cracking passwords.
6. Stealing credentials from Windows systems and using them to conduct Pass-the-Hash/Pass-the-Ticket attacks.
7. Conducting man-in-the-middle attacks (e.g. dissecting and sniffing SSL encrypted traffic) by using ARP spoofing in IPv4 networks and falsified Neighbour Advertisements in IPv6 networks.
8. Using Metasploit Framework and existing exploit code against different targets. This includes client-side attacks.
9. Exploiting vulnerabilities in custom-built web applications.

Target Audience

The course has been designed for network and system administrators and security specialists. In general, the expected audience should consist of people who have a good background in information technology, whether gained from studies at university or by practical experience, or both.

We do not expect these individuals to have knowledge or good practical know-how about security problems of computer networks and applications.

NB! Professional security practitioners or penetration testers with years of experience are **NOT** the target audience for this course.

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 394 "IT Systems Attack and Defence", see the details in the "e-Learning courses" chapter) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and will be available to all users of the portal.
2. Ideally, the students would have at least junior administrator level experience with Windows and Linux based systems. They should understand the main networking protocols (e.g. ARP, IP, ICMP, TCP, UDP, DNS, HTTP, SNMP, SMTP), have some experience with web technologies (like HTML, PHP, JavaScript) and knowledge about relational database management systems (MySQL).

3. Programming skills are helpful.
4. English language skill comparable to STANAG 6001, 3.2.3.2. is required.
5. Student's workstation will be based on Kali Linux; therefore at least user-level knowledge of working with Linux systems on the command line is expected (opening ssh connections, working with the filesystem, configuring network settings, etc).

ISACA CPEs

With the completion of this course the students can earn **35** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 394 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Introductory Digital Forensics Course (IDFC)

First iteration: 16-20 June 2025

Registration deadline: 11th April 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Second iteration: 13-17 October 2025

Registration deadline: 8th August 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

Learning Objectives

1. Provide an overview about prospective digital evidence (assuming exclusively Windows hosts),
2. Understand technical and procedural limitations while conducting digital forensic investigation,
3. Conduct digital forensic investigation, focusing primarily on open source/free forensic software (no commercial solutions),
4. Prepare course students for more in-depth forensics/reverse engineering training.

Outline

1. Introduction to Digital Forensics.
2. Forensic process and workflow (Terminology, Methodology, Principles, Chain of Custody.
3. Evidence Acquisition block (theory and hands-on):
    a. System description and verification.
    b. Different types of evidence and locations.
    c. Forensic software/hardware for evidence acquisition.
    d. Acquisition process.
    e. Evidence handling.
4. Analysis (theory and hands-on):
    a. File system analysis,
    b. Media analysis,
    c. Windows OS analysis
        (1) Registries,

(2) Event logs,
(3) Prefetch,

5. Other Windows OS artefacts.
6. Data carving and application fingerprinting (theory and hands-on).
7. Internet activities focus (theory and hands-on):

a. Browser, Email, Instant Messaging Forensics.

8. Memory analysis (theory and hands-on):
9. Terminology, tools, acquisition, analysis.
10. Timeline analysis (theory and hands-on):
11. Timeline creation, filtering, analysis.
12. Network analysis (theory and hands-on):
13. Capturing network traffic, tools, analysis.

Target Audience

The course is targeted at technical IT staff who are used to working with IT in roles such as administrator, auditor and whose normal duties do not include forensic analysis. It is in introductory training solution.

The course is also open to forensics trainers such as lecturers and tutors whose duties include forensics training.

NB! Experienced digital forensic staff performing forensics on a regular basis are NOT the target group and will receive only limited benefit from attending.

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 344) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and will be available to all users of the portal.
2. Good work/administration experience in the Linux and Windows environments, especially command line,
3. Comfortable with using virtual machines for training environment,
4. English language skill comparable to STANAG 6001, 2.2.2.2.
5. For non-technical personnel (but others are welcome as well), we strongly advise to get familiar with:

6. Linux command line: https://ubuntu.com/tutorials/command-line-for-beginners#1-overview
    a. Introduction to Windows PowerShell can be useful reading as well: https://www.tutorialspoint.com/powershell/index.htm
    b. Basics of how virtualization and related tools work
        (1) Virtual Box: https://www.youtube.com/watch?v=VZJ6KZUc25M
        (2) VMWare: https://www.youtube.com/watch?v=7m3f-P-WWbg
    c. Overview how Linux environment looks in general, since SIFT workstation is built upon Ubuntu: https://www.youtube.com/watch?v=D4WyNjt_hbQ
    d. Autopsy tool is presented throughout the course as well: https://www.youtube.com/watch?v=fEqx0MeCCHg

ISACA CPEs

With the completion of this course the students can earn **35** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 344 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Industrial Control Systems Security Introductory Course (ICSSIC)

Date: 08-12 September 2025

Registration deadline: 11th July 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

The aim of this course is to explain security issues of ICS/SCADA environments, and to provide students with the knowledge necessary to protect Programmable Logic Controllers (PLC) and industrial field devices. It offers hands-on exercises for training as well as taught content.

Learning Objectives

1. Understand the PLC programming methods.
2. Manipulate Industrial Control Systems by exploiting their vulnerability.
3. Discover known and unknown industrial protocols.

Target Audience

Technical IT-staff fulfilling roles such as administrator and auditor whose daily duties do not necessarily include IC/SCADA-security.

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 347) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and will be available to all users of the portal.
2. Basic knowledge Windows and Linux based systems
3. Basic knowledge and experience with network traffic analysis (Wireshark or similar).
4. Basic knowledge and experience in programming.
5. Comfortable with using virtual machines for training environment (Virtual Box or similar).
6. English language skill comparable to STANAG 6001, 2.2.2.2

ISACA CPEs

With the completion of this course the students can earn **28** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 347 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Integrating Cyberspace Considerations into Operational Planning Course (ICCOP) – NATO-Approved

First iteration: 10-14 February 2025

Registration deadline: 13rd December 2024

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Second iteration: 15 – 19 September 2025

Registration deadline: 18th July 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

This NATO-approved course provides a comprehensive knowledge of cyberspace as a military operational domain, to guide operational planners in the integration of cyber considerations in the comprehensive operations planning process.

Learning Objectives

1. Characterize cyberspace as a domain of operations
2. Prepare cyberspace recommendation in support of the comprehensive operational planning process
3. Explain NATO and national organization capabilities and limitation in cyberspace operations

Target Audience

This course is designed for operational planners – non-experts in cyber.

Outline

1. Cyberspace overview and taxonomy
2. Cyberspace as domain of operations
3. Integration of Cyber in the operations planning process
4. Cyber incidents handling in the execution of military operations.
5. Cyber intelligence
6. Risk assessment/risk management
7. NATO perspective on Cyber Operations

8. National perspective on Cyber Operations.
9. Cyber organization in NATO
10. NATO technical capabilities
11. Legal considerations and Rules of Engagement in Cyber Operations
12. Host Nation critical infrastructure: coordination with national authorities during cyber crisis situations.

Prerequisites

1. **The course has a mandatory e-learning module** (ADL 375, see the details in the "Online training" chapter) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and it's available to all users of the portal.
2. Basic knowledge of cyber security. It is highly recommended to have completed, previously, the "ADL 076 Cyber Defence Awareness Course", available online in the NATO ACT Joint Advanced Distributed Learning Portal (JADL, https://jadl.act.nato.int).
3. Knowledge of the NATO ACO Comprehensive Operations Planning Directive (COPD). It is highly recommended to have completed, previously, the "ADL 131 Introduction to Comprehensive Operations Planning Directive Course", available online in the NATO ACT Joint Advanced Distributed Learning Portal (JADL, https://jadl.act.nato.int).
4. English language skill comparable to STANAG 6001, 3.3.3.2.

ISACA CPEs

With the completion of this course the students can earn **34** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 375 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Critical Information Infrastructure Protection Course (CIIP)

Date: 10-14 Nov 2025

Registration deadline: 12th Sept 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

This course is currently under review

Course Aim

This 5-day (4-day if online) unclassified course is intended for mid-level managers responsible for the protection of Critical Information Infrastructure. The purpose of the course is to provide students with the knowledge necessary to analyse, assess and make decisions relative to Critical Information Infrastructure Protection (CIIP).

Learning Objectives

At the end of the course, students will:

1. Prioritize critical information infrastructure assets;
2. assess the vulnerabilities and the threat profiles relative to Critical Information Instructure;
3. Select risk response options; and
4. Oversee and critique a comprehensive Risk Assessment of both cyber and physical vulnerabilities for select Critical Information Infrastructure.

Target Audience

Students should be from NATO countries, Sponsoring Nations, Contributing Participants and NATO bodies and be military officers at the OF-3 to OF-5 level or civilians of equivalent rank.

Prerequisites

The course has a mandatory e-learning module (ADL 343) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and will be available to all users of the portal.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 343 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

International Law of Cyber Operations Course (ILoCOC) - *NATO-Approved*

First iteration: 19-23 May 2025

Registration deadline: 21st March 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Second iteration: 22-26 September 2025

Registration deadline: 25th July 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Third iteration: 8-12 December 2025

Registration deadline: 10th October 2025

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Course Aim

The aim of the course is to provide personnel working within the legal framework of NATO cyberspace operations with the skills and knowledge required to successfully incorporate legal considerations into the cyberspace domain of operations.

Learning Objectives

1. Conduct Cyber incident legal assessment;
2. Provide cyberspace operational legal advice; and
3. Provide legal advice on NATO's approach to cyberspace operations.

Outline

1. Introduction to the Cyber Domain:
2. Introduction to technical aspect of the cyber domain;
3. Incident analysis characteristics;
4. Context of a cyber-incident;
5. Introduction to the cyber law toolkit;
6. Rules of state responsibilities;
7. Breach of sovereignty;
8. Breach of prohibited intervention;
9. Use of force;
10. International Law of justifications;
11. Conflict classifications;
12. Advising on lawful response options;

13. Assessing the impact of specialized regimes;
14. Introduction to the Operational Planning Process;
15. Identifying Applicable Legal Frameworks;
16. Rules of Engagement;
17. Legal Implications for Cyber COAs; and
18. Advising on the Conduct of Cyberspace Operations.

The course includes a complex exercise that allows participants to apply the law addressed during lectures and discussion. The lectures will be given by noted scholars and practitioners, some of them involved in the Tallinn Manual 2.0 process. During the course registration process, participants can request for purchase the Tallinn Manual 2.0 handbook on the International Law Applicable to Cyber Operations.

Target Audience

This training solution is intended for personnel who have some experience operating within the framework of international law but who are not necessarily legal advisors. It is also simultaneously designed for legal advisors filling roles in NATO and national military and civilian positions where it is expected that they provide legal advice on cyberspace operations and planning.

Prerequisites

The course has a mandatory e-learning module (ADL 420) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and will be available to all users of the portal.

Pre-study e-Learning material

1. International Law of Cyber Operations (ADL 420) on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)
2. Cyber Awareness Course Tallinn Manual Module (ADL 365) on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

ISACA CPEs

With the completion of this course the students can earn **34** ISACA CPE hours.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

Module certificate of the ADL 420 must be send to training@ccdcoe.org when registering for the residential part of the course. You can download it once you have successfully finished the final test of the e-Learning module.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved when the payment of the course fee is confirmed.

Should you have any questions, please contact: training@ccdcoe.org

Executive Cyber Seminar (ECS)

First iteration: 09 – 11 June 2025

Registration deadline: 09th May 2025

This iteration will be held in Brussels, more details will be provided later

Second iteration: 03-05 November 2025

Registration deadline: 10th October 2025

Aim of the seminar

This seminar has been designed for senior level staff, primarily in NATO and defence, who are new into post and/or for whom cyberspace is a new area of responsibility or consideration. Over the course of a day and a half, participants will be led through a series of themed discussions that will introduce this domain and explore its impact on decision makers of today.

Learning Objectives

1. An introduction to and basic, but comprehensive, grounding in cyberspace; what it is, and what it is not
2. Why cyberspace is important and relevant to decision makers and those who write policy and strategy
3. Introduction to the legal aspects of Cyberspace Operations
4. A perspective of the threat landscape

Target Audience

1. This seminar has been designed to target senior level individuals new into post where cyber is part of their responsibility, but not their primary or only responsibility
2. The seminar is designed to cater for both senior level military and civilian staff, primarily those in NATO and defence, and government officials with policy or decision making responsibility

Outline

As a response to the exponential growth of cyberspace and increasing demand for cyber defence expertise NATO CCDCOE has designed a high-level Executive Cyber Seminar for senior staff, principally OF-6 and higher, or civilian equivalent, primarily in NATO and defence, for whom cyberspace is a new area of responsibility or consideration.

Over the course of a day and a half, participants will be led through a series of themed discussions that will introduce this domain and explore its impact on societies and decision makers.

There will be specific sessions on NATO and EU developments, threats in and through cyberspace, legal aspects including a review on how International Law applies to cyber operations, critical information infrastructure protection, the role of social media etc.

Lecturers include both CCDCOE researchers and external experts, recognised for their expertise in their focus area. Each iteration is tailored to suit the attendees and allows for open Q+A to address any specific areas of interest from the group or individual. In addition, previous participants have valued the mix of expertise represented by other seminar attendees – every seminar is unique due to the discussions, networking and feedback generated by the particular group.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

An email confirming the participation will be sent only after the registration has closed. Should you have any questions, please contact: training@ccdcoe.org

Locked Shields Forensics Workshop (LSFW)

Date: 25 – 27 June 2025

Registration deadline: 9th May 2025

Aim of the workshop

Locked Shields Forensic Workshop (LSFW) is a hands-on analysis of the Locked Shields DFIR challenge. Participants will receive guidance on how to reach possible solutions to all the cases given during the execution. The instructors are CCDCOE Digital Forensics experts and external developers.

Execution

LSFW is planned as a hybrid format. It will be an online event but we can offer a limited number of seats for participants who prefer and are able to travel to Tallinn.

We encourage participants to use their own devices and environment and also to be prepared to share their own solutions, as it might be beneficial for others including the challenge developers.

Target Audience

The workshop is ONLY intended for the Locked Shields 2025 training audience (Blue Team) who were engaged in solving the DFIR Capture the Flag challenge.

Registration

Please register for the course by visiting the NATO CCDCOE website and completing the provided registration form before the deadline. Applicants from CCDCOE member nations should use the registration code provided by their national Point of Contact.

An email confirming the participation will be sent only after the registration has closed. Seat allocation will only be approved if the applicant was part of a LS25 Blue Team.

Should you have any questions, please contact: training@ccdcoe.org

Mobile training

In 2025, the Centre will deploy its trainers and training devices at the Centre's member location(s) to provide **4** courses (**5** iterations):

1. Integrating Cyberspace Considerations into Operational Planning (3 iterations)
2. IT Systems Attack and Defence Course (1 iteration)
3. Reverse Engineering Malware Course (1 iteration)
4. Industrial Control Systems Security Introductory Course (1 iteration)

The possibility to deliver a mobile iteration of the new version of the Critical Information Infrastructure Protection Course is pending.

The objectives, target audience, and outline of courses; and the prerequisites to join them are the same as those for in-house courses listed in the previous chapter.

The Centre does not charge any course fee for mobile trainings. However, the requesting entity must cover all expenses associated with the planning and conduct of the mobile iteration itself, including (but not limited to): travel, accommodation and per-diem.

Sponsoring Nations (SNs), Contributing Participants (CPs) and NATO bodies can request mobile course(s) delivered in national/NATO locations. The selection process will be conducted according with criteria established by the NATO CCDCOE Steering Committee.

Registration will be managed by the course host nation, which can share slots with other SNs or CPs.

e-Learning courses

ADL 076 – Cyber Defence Awareness e-Course (NATO-approved)

Course Aim

To complement the courses offering, the Centre provides an online web-based course on Cyber Defence Awareness, the last update of the course was published in June, 2019.

This NATO-approved course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

The Cyber Defence Awareness e-Learning course aims to enhance the general user's awareness of cyber security risks and measures to mitigate those risks.

Learning Objectives

This course provides an introduction to general cyber security in order to aid familiarisation with attacks, terminology and defensive techniques. It gives an overview of the recent threat landscape.

Target Audience

The Cyber Defence Awareness e-course was developed with the goal of raising the awareness of the average user within the NATO community, covering the most relevant topics in the area. The training audience includes all users of NATO networks.

Outline

1. General Cyber security terminology and categorisation.
2. Malware, viruses and spyware.
3. Anti-virus software.
4. Unauthorised system access and characteristics of a strong password.
5. Identity theft and compromise of classified data.
6. Risks regarding removable media.
7. Phishing.
8. Risks associated with emails (dangerous attachments, hoaxes, etc.).

9. Threats to and from mobile devices.
10. Backing up systems and files.
11. File sharing and copyright issues.
12. The dangers of unsecured wireless networks.
13. Desktop security.
14. Social engineering and other human aspects.
15. Disposal of information.
16. The risks of social networking.

Prerequisites

Basic computer user skills.

Registration

The course is available to all users of the NATO e-Learning Joint Advanced Distributed Learning portal. Once registered, users may access the course by navigating to the 'CENTRES OF EXCELLENCE (COE's)' -> 'Cooperative Cyber Defence Centre of Excellence' -> 'ADL 076 Cyber Defence Awareness (new)' course listing.

ADL 230 – Operational Cyber Threat Intelligence

Course Aim

The aim of this course to provide knowledge to fill the gap between the technical level and the operational level that is responsible for planning cyber activities.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Cyber Threat Intelligence Cycle
2. Cyber Threat Intelligence Sources
3. Cyber Threat Intelligence Tools
4. Actionable Intelligence and Threat Hunting
5. Operational Security
6. Sharing Threat Information
7. Cyber Threat Intelligence Program

Target Audience

The course has been designed for J2, J3, J5, J6 staff members, branch heads, RRT/CERT members, Cyber Threat Analysts, mediators between Tech Level and Operational level.

Prerequisites

a. The Integration of Cyber Considerations into Operational Planning e-Learning course (ADL 375) is recommended for the students of the course.
b. English language skill comparable to STANAG 6001, 3.3.3.2.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 230 Operational Cyber Threat Intelligence Course' course listing.

ADL 335 – Cyber Awareness Course for System Administrators

Course Aim

The Cyber Awareness Course for System Administrators e-Learning course aims to enhance the network and system administrators' skills regarding the different aspects of awareness regarding the current cyber security risks and measures to mitigate those risks, to improve and maintain the general awareness of the network users.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

This course provides an introduction to general cyber security in order to aid familiarisation with attacks, terminology and defensive techniques. It gives an overview of the recent threat landscape, concentrating on the network and system administrators specific tasks.

Target Audience

The Cyber Awareness Course for System Administrators e-course was developed with the goal of improving the awareness attitude of the network and system administrators within the NATO and National networks (systems), covering the most relevant topics in the area.

Outline

1. Information Security Management System
2. Digital Forensics and Digital Evidence
    a. Digital Forensics and Digital Evidence (in general)
    b. Digital Forensic Process
    c. Acquisition of Digital Evidence
    d. Examination and Analysis of Digital Evidence
3. Network and Log Monitoring
    a. Network Monitoring
    b. Log Monitoring

4. Web Application Security
5. Critical Infrastructure and Industrial Control Systems
6. Fighting a Botnet Attack: a Case Study
7. Systematic Approaches to the Mitigation of Cyber Threats

Prerequisites

Basic network and system administrator skills.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Cyber Awareness Course for System Administrators' course listing.

ADL 343 – Information Security Management System Course

Course Aim

This course covers the theory of Information Security Management Systems.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Define an ISMS.
2. List the reasons why an organization should implement an ISMS.
3. Describe the methodologies that could be used to evaluate risks and to select security controls for information systems.
4. Describe examples well-known international and national ISMS standards and frameworks.
5. Describe the process of implementation of an ISMS.

Target Audience

Personnel involved in implementing an Information Security Management System (technical or not)

Outline

1. Introduction of a formal system that is used to manage risks to information systems – an information security management system (ISMS).
2. Discussion of the implementation of an ISMS.
3. Methodologies of the evaluation of risks and the selection of security controls, which an ISMS should include.
4. Some well-known ISMS standards and frameworks.
5. Circular process of implementation of an ISMS.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Information Security Management System' course listing.

ADL 344 – Digital Forensics and Digital Evidence Course

Course Aim

This course is a **mandatory** e-learning module of the **Introductory Digital Forensics Course** (residential).

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Define the scope of the science of digital forensics.
2. Define digital evidence and give examples of it.
3. Describe the legal status of digital evidence.
4. Define the concepts of integrity and authenticity that laws about digital evidence deal with.
5. Describe the difference between digital forensics and incident response.
6. List the areas of digital forensics.
7. Will be able to describe the phases of the digital forensic process and give examples of the requirements that investigators should follow when working on each.
8. Differentiate between dead and live acquisition of digital evidence and explain in what situations which mode of acquisition should be preferred.
9. Define memory and disk imaging.
10. Describe the possible methods of acquisition of memory images and specify which of them are safe to use in digital forensics and which not.
11. Describe the functionalities of different formats of disk images.
12. List the types of evidence that can be found from the system's memory.
13. List the types of evidence that can be found when examining Windows OS.
14. Give examples of the information that an investigator can find and deduce when examining web browser artefacts.
15. Describe the limits of the recovery of instant messages.
16. Describe the elements of an e-mail that an investigator should examine.

Target Audience

Students who applied for the Introductory Digital Forensics Course (residential) :

1. Technical IT Staff, working in the IT area in roles like administrator, auditor, etc., whose normal duties do NOT include forensic analysis, but who might be asked to support a forensic investigation. This course is introductory. Experienced digital forensic staff doing forensics on regular basis are not the target group and will receive only limited benefit from attending.
2. Administrators or IT Security staff who might be first responders to security incidents and want to secure evidence for later analysis, when no forensic staff is available.
3. IT staff who will acquire an initial skill set of how to conduct forensic investigation.
4. Non-technical Staff who operate on the level between the Technical personnel and Management, in the need to understand and support the Technical personnel and properly communicate their findings to the Management.

Outline

1. Digital Forensics and Digital Evidence
2. Digital Forensic Process
3. Acquisition of Digital Evidence
4. Examination and Analysis of Digital Evidence

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Digital Forensics and Digital Evidence' course listing.

ADL 345 – Network and Log Monitoring Course

Course Aim

This course covers network and log monitoring to support the preparation of the participants of the Cyber Defence Monitoring Course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. List the ways of physically connecting a sensor to a monitored network.
2. Describe the differences between an NIDS and an NIPS.
3. Deploy an NIDS and NIPS sensor on a network.
4. List the pros and cons of well-known network monitoring solutions such as Snort, Suricata, Bro and Moloch.
5. Describe the BSD syslog protocol, its shortcomings and recommended solutions for log collection.
6. List the event logging formats and log collection tools of Windows.
7. Describe the purpose of log correlation and the functionalities of the Simple Event Correlator (SEC), which can be used for that.
8. List various log analysis and data visualization tools.
9. Describe the purpose and the pros and cons of security information and event management (SIEM) systems.

Target Audience

Cyber defence monitoring operators.

Outline

1. Network Monitoring - Sensor placement in a Network Intrusion Detection and Prevention Systems (NIDS/NIPS) are provided. Common network monitoring solutions are introduced as well.
2. Log Monitoring:
    a. The BSD syslog protocol, used for event logging;
    b. Tools and solutions for log collection, log correlation and log analysis are introduced.

Prerequisites

1. Good understanding of TCP/IP networking and network and system administration.
2. Recent everyday network/system administrator's work experience for at least **2 years** in UNIX environments.
3. Previous detailed knowledge on the following topics:
   a. work principles of UNIX operating systems and UNIX file system layout;
   b. common UNIX shells (e.g., sh, bash);
   c. common UNIX user tools (e.g., ls, ps, kill); and
   d. common UNIX system administration utilities.
4. Scripting experience is required.
5. Basic Python skills are required: ability to write a function, for loop, invoke standard library and use core data.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Network and Log Monitoring' course listing.

ADL 346 – Web Application Security Course

Course Aim

This course covers web application security.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. List the ways of physically connecting a sensor to a monitored network.
2. Install and configure a web server in a secure way.
3. Secure HTTPS and SSL/TLS by configuring cipher suites and cookies and using HTTP Strict Transport Security (HSTS) and Content Security Policy (CSP).
4. Manage the logs, backups and remote logins of a web application.
5. Describe the purpose and the strengths and weaknesses of a web application firewall (WAF).
6. Test web server security by using vulnerability scanning and pentesting.
7. Describe other elements of web application security that should be taken care of (operating system security, network security and database hardening).

Target Audience

Military and civilian IT specialists. Students do not need to be web developers or have prior experience as web app pen-testers. However, a basic understanding of web technologies (basic html, javascript, SQL) and some server side coding experience will be beneficial.

Outline

1. Practical guidelines about web application security and web server security
2. Following these guidelines by a system administrator helps to make a website more secure.

Prerequisites

1. Network basics (IP's, TCP, ports, client - server protocols, SSL).
2. General understanding of web technologies (basic html, javascript, SQL).

3. Basic shell commands (Linux and/or Windows).
4. Some server side coding experience will be highly beneficial, although not essential.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Web Application Security' course listing.

ADL 347 – Critical Infrastructure and Industrial Control Systems Course

Course Aim

This course is to support the preparation of the participants of the Industrial Control Systems Security Course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Explain the meaning of critical infrastructure and give examples of critical infrastructure sectors.
2. Define an industrial control system.
3. Describe the differences between SCADA and DCS.
4. Describe the functionality of PLC.
5. List the programming languages allowed to use in PLC.
6. List the most common methods of attack against an ICS.

Target Audience

Technical IT-staff fulfilling roles such as administrator and auditor whose daily duties do not necessarily include IC/SCADA-security.

Outline

1. Critical infrastructure and industrial control systems.
2. Meaning of critical infrastructure in the United States and the European Union
3. Three types of industrial control systems (ICSs) that critical infrastructure operators use
4. The supervisory control and data acquisition (SCADA)
5. The distributed control system (DCS) and the programmable logic controller (PLC)
6. The most widespread methods of attack against an ICS

Prerequisites

1. Basic knowledge Windows and Linux based systems
2. Basic knowledge and experience with network traffic analysis (Wireshark or similar).
3. Basic knowledge and experience in programming.
4. Comfortable with using virtual machines for training environment (Virtual Box or similar).

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Critical Infrastructure and Industrial Control Systems' course listing.

ADL 348 – Fighting a Botnet Attack: a Case Study Course

Course Aim

This course is a case study on fighting a botnet attack.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Give examples of the goals behind botnet attacks and describe the botnet attack chain step by step.
2. Give examples of the ways of making the planning of a botnet attack harder for attackers.
3. Describe the methods of delivery of a malicious code and the measures that an organization can take to prevent, discover and block malware delivery attempts.
4. Explain why it is important to look for indicators of persistence of a malicious payload.
5. List the methods to use to protect an infrastructure against the execution of a botnet attack.

Target Audience

Cyber security technical staff (CERT, IT departments, etc.) seeking to become familiar with malware analysis and related topics.

Outline

1. A case study of a botnet attack is presented.
2. Measures to be taken to detect and counteract a botnet attack in each of its phases are described as well.

Prerequisites

1. Good work/administration experience in Linux (as the work environment) and Windows (as the malware environment).
2. Basic understanding of network traffic and malware.
3. Ability to use virtual machine technology (Virtual box or similar).
4. Experience with firewalls and network traffic analysis (Wireshark and similar).
5. Basic understanding of assembler and higher programming languages.
6. Scripting language skill (Python, Visual Basic, Bash).

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Fighting a Botnet Attack: A Case Study' course listing.

ADL 349 – Systematic Approaches to the Mitigation of Cyber Threats Course

Course Aim

This course covers systematic approaches to the mitigation of cyber threats.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Describe the operation of a cyber security incident response team (CSIRT).
2. Use the cyber kill chain to take steps against a cyber attack in its various phases.
3. Describe the purpose of information and cyber security frameworks and give examples of them.

Target Audience

Cyber security technical staff (CERT, IT departments, etc.) seeking to become familiar with malware analysis and related topics.

Outline

Guidelines are provided about the mitigation of cyber threats in a systematic way.

Prerequisites

1. Good work/administration experience in Linux (as the work environment) and Windows (as the malware environment).
2. Basic understanding of network traffic and malware.
3. Ability to use virtual machine technology (Virtual box or similar).
4. Experience with firewalls and network traffic analysis (Wireshark and similar).
5. Basic understanding of assembler and higher programming languages.
6. Scripting language skill (Python, Visual Basic, Bash).

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Systematic Approaches to the Mitigation of Cyber Threats' course listing.

ADL 365 – Cyber Awareness Course, Tallinn Manual Module

Course Aim

This course is a pre-study material for the International Law of Cyber Operations Course (residential).

The "Cyber Awareness Course Tallinn Manual Module" e-Learning course aims to prepare the participants of the International Law of Cyber Operations Course, providing an overview of the topics covered by the Tallinn Manual and provide an introduction on how existing international law could be applied to cyber operations.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Understand the nature and context of cyber operations and cyber attacks
2. Identify and apply the international legal framework that regulates the "Use of Force" under the UN Charter in the cyber context
3. Recognize the role of the Tallinn Manual in the articulation of the legal framework applying to cyber warfare
4. Apply principles of International Humanitarian Law to cyber warfare

Target Audience

This training solution is intended for personnel who have some experience operating within the framework of international law but who are not necessarily legal advisors.

It is also simultaneously designed for legal advisors filling roles in NATO and national military and civilian positions where it is expected that they provide legal advice on cyberspace operations and planning.

Outline

1. Nature and context of cyber operations and cyber attacks
2. International legal framework that regulates the "Use of Force" under the UN Charter in the cyber context

3. Role of the Tallinn Manual in the articulation of the legal framework applying to cyber warfare
4. Principles of International Humanitarian Law to cyber warfare

Prerequisites

Prior knowledge of relevant international law is recommended.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'Cyber Defence Awareness' -> 'Cyber Awareness Course Tallinn Manual Module' course listing.

ADL 375 – Integrating Cyber Considerations into Operational Planning

Course Aim

This course is a **mandatory** e-learning module of the **Integrating Cyber Considerations into Operational Planning** course (residential).

The aim of this course to provide knowledge of cyberspace as a military operational domain, to guide operational planners in the integration of cyber considerations in the comprehensive operations planning process and this way establish a common basis of knowledge for the students attending the residential part of the course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

1. Facilitate the understanding of the cyberspace as a special domain of operations
2. Explain how the intelligence and risk management cycles work
3. Identify cyber aspects of the comprehensive operations planning process

Target Audience

This course is designed for operational planners – non-experts in cyber.

Outline

1. Integrating cyber operations into operational planning
    a. Characterizing cyberspace
    b. Recognising distinguishing aspects of the domain
    c. Identifying the applicable aspects of the existing international law
2. Cyber intelligence and risk cycles
    a. Describing the specifics of the intelligence cycle in relation to cyberspace
    b. Describing the specifics of the risk management cycle in relation to cyberspace
3. Cyber during the Comprehensive Operations Planning Process (COPP)
    d. Identifying the four types of cyberspace operations

e. Listing cyberspace-related issues that should be addressed during the Comprehensive Operations Planning Process
f. Explaining the role of the cyber cell role in an operational headquarters during the execution of operations

Prerequisites

c. Basic knowledge of cyber security. It is highly recommended to have completed, previously, the "ADL 076 Cyber Defence Awareness Course", available online in the NATO ACT Joint Advanced Distributed Learning Portal (JADL, https://jadl.act.nato.int).
d. Knowledge of the NATO ACO Comprehensive Operations Planning Directive (COPD). It is highly recommended to have completed, previously, the "ADL 131 Introduction to Comprehensive Operations Planning Directive Course", available online in the NATO ACT Joint Advanced Distributed Learning Portal (JADL, https://jadl.act.nato.int).
e. English language skill comparable to STANAG 6001, 3.3.3.2.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 375 - Integrating Cyber Considerations into Operational Planning' course listing.

ADL 383 – Malware and Exploit Essentials

Course Aim

This course is a **mandatory** e-learning module of the **Malware and Exploit Essentials** course (residential).

The aim of this course to provide knowledge about technical insights for cyber defenders into techniques that malware uses to exploit vulnerabilities and to intrude into systems. Based on an introduction to OS features and analysis techniques, the use of debuggers as the most important tools for exploit research and methods for vulnerability detection like fuzzing will be discussed and this way establish a common basis of knowledge for the students attending the residential part of the course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

Malware module:

a. Define malware and identify it's different types
b. Identify the symptoms of malware infection as well as the most common attack vectors
c. Explain the structure of the Portable Executable file format
d. Differentiate between static and dynamic malware analysis
e. Describe the most common open-source programs used by investigators when performing malware analysis
f. Differentiate between obfuscated and packed malware and identify packed executables

Exploit module:

a. Describe the meaning of an exploit
b. Describe the basic concept of memory in a modern operating system
c. Compile executable files in Linux
d. Follow the basic instructions in assembly language
e. Explain the basic functionalities of a debugger for exploit development

Target Audience

Technical staff of CERTs, IT departments or other governmental or military entities being involved in technical IT security or cyber defence.

Prerequisites

a. Good work/administration experience in the Linux and Windows environments, especially command line.
b. Basic understanding of assembler and higher programming languages (optional).
c. Programming experience in assembler, C(++) or PYTHON (optional).
d. English language skill comparable to STANAG 6001, 3.2.3.2.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 383 – Malware and Exploit Essentials' course listing.

ADL 391 – IT Systems Attacks and Defence

Course Aim

This course is a **mandatory** e-learning module of the **IT Systems Attacks and Defence** course (residential). The aim of this course to provide knowledge about tools and methods used by attackers to gain access to IT systems and discusses potential countermeasures and ways of detection and this way establish a common basis of knowledge for the students attending the residential part of the course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

The course introduces students to the way penetration testers and hackers think. Practical work is used to further develop this kind of thinking and also to figure out ways how to defend against these kinds of attacks. The course does not go in-depth into specific vulnerabilities, rather it serves as a broad introduction into IT systems attacks and points the students towards material where to learn further.

The following topics will be covered during the course:

a. Networks and threat models
b. Attacks and attackers
c. Reconnaissance
d. Scanning and Enumeration
e. Local network attacks
f. Internet Infrastructure attacks
g. Attacks against Windows domain and workstations

Target Audience

The course has been designed for network and system administrators and security specialists. In general, the expected audience should consist of people who have a good background in information technology, whether gained from studies at university or by practical experience, or both.

We do not expect students to have knowledge or good practical know-how about security problems of computer networks and applications. Professional security practitioners or penetration testers with years of experience are not the target audience for this course.

Prerequisites

a. Ideally, the students would have at least junior administrator level experience with Windows and Linux based systems. They should understand the main networking protocols (e.g. ARP, IP, ICMP, TCP, UDP, DNS, HTTP, SNMP, SMTP), have some experience with web technologies (like HTML, PHP, JavaScript) and knowledge about relational database management systems (MySQL).
b. Programming skills are helpful.
c. English language skill comparable to STANAG 6001, 3.2.3.2. is required.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 394 – IT Systems Attack and Defence' course listing.

ADL 420 – International Law of Cyber Operations

Course Aim

This e-Learning course is a **mandatory** e-learning module of the **International Law of Cyber Operations Course** (residential). The aim of this course to examine the key aspects of the public international law governing 'cyber operations' conducted by States during peacetime. The module addresses the jus ad bellum, which regulates the use of force by States and the jus in bello, the law that governs how States may conduct their military operations during an armed conflict and with this knowledge, the students can attend the residential part of the course.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Learning Objectives

The following topics will be covered during the course:

1. Understanding the nature and context of Cyber Operations (CO);
2. Recognizing the role of the Tallinn Manual in the articulation of the legal framework applicable to CO conducted by States;
3. Identifying the international legal framework applicable to CO conducted in peace time;
4. Identifying the rules that regulate the 'use of force' under the UN Charter as applicable in cyberspace;
5. Identifying the basic principles of IHL applicable to CO conducted in the context of an armed conflict;

Outline of the course

1. Defining the Context
2. Defining the Applicable Legal Framework
3. Peacetime Cyber Activities
4. International Peace and Security and Cyber Operations
5. The Law of Cyber Armed Conflict

Target Audience

1. Military and civilian legal advisors to the armed forces.
2. Intelligence community lawyers.
3. Other civilian attorneys in governmental security posts.
4. Policy specialists who advise on cyber issues and wish to acquire a basic understanding of the applicable legal regimes.
5. Legal scholars and graduate students.

Prerequisites

Prior knowledge of relevant international law is recommended, but not a prerequisite.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 420 International Law of Cyber Operations' course listing.

ADL 430 – Cyber Defence Monitoring

Course Aim

This e-Learning course is a **mandatory** e-learning module of the **Cyber Defence Monitoring** course (residential) and can be used as a standalone introduction to network security monitoring.

While this e-learning module introduces the basics of NSM that everyone should know before attending the classroom training, it **does not** provide the necessary technical prerequisites and experience necessary to follow the classroom training. Make sure you have the necessary experience before joining (see the details below).

With the completion of this course the students can earn **1** ISACA CPE hours.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

Outline of the course

1. Introduction
    a. Basic introduction to network security monitoring (NSM)
    b. Relevance of NSM and network security policies
    c. Overview of different network monitoring tool types
2. Setting up an NSM solution
    d. Placement of sensors on the network
    e. Connecting sensors to the monitored network
    f. Architecture of the NSM solution
    g. Customizing according to the needs of the organization
3. Logging and analysis
    h. Collecting logs from the NSM tools
    i. Analyzing NSM logs
    j. Analyzing PCAP files
    k. Basic dashboarding

Target Audience

1. Technical IT security staff in charge of network security monitoring.
2. Security and IT managers who want to get a real-life understanding of Suricata.
3. Locked Shields Blue Team members and/or national representatives.

Prerequisites

1. Good understanding of TCP/IP networking and network and system administration.
2. Recent everyday network/system administrator work experience for at least 2 years in UNIX environments.
3. Previous detailed knowledge on the following topics:
4. work principles of UNIX operating systems and UNIX file system layout;
5. common UNIX shells (e.g., sh, bash);
6. common UNIX user tools (e.g., ls, ps, kill); and
7. common UNIX system administration utilities.
8. Scripting experience is required.
9. Basic Python skills are required
10. write a function and for loop;
11. invoke standard libraries;
12. use core data structures.
13. English language skill comparable to STANAG 6001, 3.2.3.2.

Registration

The course can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal and is available to all users of the portal. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> 'ADL 430 Cyber Defence Monitoring' course listing.

About NATO CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) is a NATO-accredited cyber defence hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. NATO CCDCOE based in Tallinn, Estonia, embodies and fosters the cooperation of like-minded nations in cyber defence. Its member nations are NATO Allies and like-minded partners beyond the Alliance.

The mission of NATO CCDCOE is to support NATO, its member nations, and the international community with wide-ranging cyber defence expertise. This military organisation conducts research, trainings and exercises in four core areas: technology, strategy, operations and law.

The heart of the Centre is a diverse group of experts from our member nations, bringing together researchers, analysts and trainers from the military, government, academia and industry. Almost half as many more nations are aspiring to become members in the years to come.

To date, 39 nations are contributing to the NATO CCDCOE :

- 31 Sponsoring Nations (SNs): Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Republic of North Macedonia, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Türkiye, the United Kingdom, and the United States.
- 8 Contributing Participants (CPs) : Australia, Austria, Ireland, Japan, Republic of Korea, Sweden, Switzerland and Ukraine.

CCDCOE Flagships

Locked Shields is a unique international cyber defense exercise run by CCDCOE since 2010 and is the biggest and most complex live-fire challenge in the world.

It helps cyber security experts enhance their skills in defending national IT systems and critical infrastructure under real-time attacks, using realistic scenarios, cutting-edge technologies, and simulation of the entire complexity of a massive cyber incident, including strategic decision-making, legal, and STRATCOM aspects.

More than 4000 cyber experts from more than 30 nations took part in Locked Shields in 2024. Locked Shields 2024 - YouTube

Crossed Swords is an annual technical red teaming cyber exercise initiated in 2016 by CCDCOE.

It provides a rigorous training platform for penetration testers, digital forensics experts, and cyber command elements.

Through immersive simulations and scenarios, Crossed Swords participants hone their skills in identifying vulnerabilities, exploiting systems, and orchestrating offensive cyber operations.

This hands-on experience empowers them to stay abreast of evolving threats and bolster their expertise in safeguarding natinal infrastructure against cyberattacks. Crossed Swords - YouTube.

CyCon

The annual International Conference on Cyber Conflict (Cycon), is the annual meeting place for the transatlantic cyber defence community.

The most recent editions of CyCon have attracted more than 600 in person participants. CyCon's agenda includes high-level political, military, academic, and private sector speakers, academic sessions and workshops.

The interdisciplinary nature of the conference encourages research and discussion on the most topical technical, policy, legal and military issues related to cyberspace and its impact to our societies.

Academic contributions are peer reviewed according to IEEE standards and published in the conference proceedings. Conference recordings can be found on the Cycon website.

The 17th International Conference on Cyber Conflict (CyCon 2025) will be held 27-30 May 2025 in Tallinn, Estonia, with the theme "The Next Step".

The Tallinn Manual

The Tallinn Manual is a non-legally-binding scholarly work by distinguished international law academics and practitioners intended to provide an objective restatement of international law as applied in the cyber context.

CCDCOE has initiated the Tallinn Manual 3.0 project, which will review and update the Tallinn Manual 2.0 (published in 2027) in light of the advancing practice of cyber operations and the evolving normative environment.

It will consider major cyber operations occurred since the publication of TM 2.0, such as WannaCry, NotPetya, election meddling, and cyberattacks against medical services during COVID-19, as well as the evolving normative architecture of cyberspace expressed through State practice (including expressed official positions), activities of international fora such as the UN, and the work of non-governmental actors.

International Cyber Law in Practice: Interactive Toolkit

The Cyber Law Toolkit is a dynamic interactive web-based resource for legal professionals who work with matters at the intersection of international law and cyber operations.

The Toolkit consists of hypothetical scenarios, each of which contains a description of cyber incidents inspired by real-world examples, accompanied by a detailed legal analysis.

The activity is run in collaboration with the Czech NCISA, ICRC, and academic partners. The Toolkit provides a thorough examination of the applicability of international law to diverse cyber scenarios and related legal issues, helping legal advisers and other professionals understand the legal issues raised by cyber operations. https://cyberlaw.ccdcoe.org/wiki/Main_Page

Full Spectrum Cyber Security Training

NATO CCDCOE promotes continuous learning in cyber security. Our training courses are based on the latest research and cyber defence exercises. NATO CCDCOE is committed to improving our training offerings to address the changing needs of the ever-developing cyber security field.

As of January 2018, NATO CCDCOE is responsible for identifying and coordinating education and training solutions in cyber defence for all NATO bodies across the Alliance (Department Head function). The same year, NATO Allied Command Transformation has provided NATO CCDCOE with an unconditional Quality Assurance accreditation for its contribution to high-quality NATO Education and Training. In 2024, the Centre was reaccreditated.

To best meet the training requirements of Allies, Partners and NATO as a whole, the Centre provides courses in different formats and locations, covering a broad range of topics in the technical, legal, strategic and operational cyber security domains.

Recent news, publications and upcoming courses of NATO CCDCOE are available at https://ccdcoe.org/ and you can connect with NATO CCDCOE on Twitter @ccdcoe.

Annex A. CCDCOE Training Calendar 2025

MEXEC	Malware and Exploit Essentials Course
EXAC	Exploit Advanced Course
REMC	Reverse Engineering Malware Course
ITSAD	IT Systems Attack and Defence Course
IDFC	Introductory Digital Forensics Course
LSFW	Locked Shields Forensics Workshop
ICSSIC	ICS Security Introductory Course + 1 day workshop
CTIC	Cyber Threat Intelligence Course

ICCOP	Integration Cyber Considerations into Operational Planning Course
ILoCOC	International Law of Cyber Operations Course
CIIP	Critical Information Infrastructure Protection Course
ECS	Executive Cyber Seminar

LS	Locked Shields
XS	Crossed Swords
CyCON	CyCON Conference

Annex B. Official Education & Training Contacts

Nation/Organization	Name	E-mail address
Albania	Denis Dvorani Renaldo Agolli	aimforeignrelation@mod.gov.al renaldo.agolli@aaf.mil.al
Austria	Peter Schlossern	peter.schlossern@bmlv.gv.at
Australia	Ms Simone Neich Andrew Page	simone.neich@defence.gov.au Andrew.Page4@defence.gov.au
Belgium	Kris Boogaerts	Kris.Boogaerts@mil.be
Bulgaria	Petya Yaneva Sibina Mitova	p.yaneva@mod.bg s.mitova@mod.bg
Canada	Candace Smigelski	candace.smigelski@forces.gc.ca
Czech Republic	Tereza Kaňová	tereza.kanova@nukib.gov.cz
Croatia	Damir Sacher	damir.sacher@morh.hr
Denmark	Mr Thomas Thrane John William Dall	thothr@cfcs.dk john.dall@ccdcoe.org
Estonia	Käroli Kullamaa	karoli.kullamaa@kra.ee
Finland	MAJ Markus Riihonen	markus.riihonen@mil.fi
France	Ronan Riou	ronan.riou@intradef.gouv.fr
Germany	Christian Dreyer Major Arne Harmsen	zcsbwfues3ausb@bundeswehr.org zcsbwbetriebsysteme@bundeswehr.org ArneHarmsen@bundeswehr.org
Greece	Cdr. (Navy) Fragkiskos Korkodeilos	f.korkodeilos@cd.mil.gr mcirc@cd.mil.gr
Hungary	Gabor Knapp	knapp.gabor@knbsz.gov.hu hakib@knbsz.gov.hu
	Bence Krizsan	krizsan.bence@knbsz.gov.hu
Iceland	Tómas Orri Ragnarsson	tomas.ragnarsson@utn.is
Ireland	Kerri-Ann Woods NCSC Admin Team	kerriann.woods@decc.gov.ie NCSCadmin@ncsc.gov.ie
Italy	CWO Nicola Damian	primo.form2s@smd.difesa.it
Japan	Mr. Aoyama Takahiko	takahiko.aoyama@ccdcoe.org
Latvia	Pauls Pencis	Pauls.Pencis@mod.gov.lv
	Ieva Krekovska	Ieva.Krekovska@mod.gov.lv
Lithuania	National Cyber Security Centre of The Republic of Lithuania	mokymai@nksc.lt
Luxembourg	Armée luxembourgeoise - Bureau Formation	Bureau.Formation@armee.etat.lu
	AdjMaj Carlo Michels	carlo.michels@armee.etat.lu
	OR-8 Stéphanie Stein	stephanie.stein@armee.etat.lu
Republic North Macedonia	Slavjanka Petrovska	slavjanka.petrovska@mod.gov.mk talin@mfa.gov.mk
Montenegro	Blazo Popovic	blazo.popovic@mod.gov.me
Netherlands	Cyber Warfare & Training Center	dcc.cwtc@mindef.nl
Norway	Erik Kursetgjerde	erik.kursetgjerde@ccdcoe.org
Poland	Lieutenant Colonel Janusz Kurek	janu.kurek@ron.mil.pl
Portugal	Captain (Navy/OF5) Vasco Miguel Ramos Marques Prates	prates.vmrm@emgfa.pt
Romania	Mihaela Marandiș	international_dmru@mapn.ro
Slovakia	Cyber Defence Center of the Slovak Republic	cyber@mosr.sk
Slovenia	COL Samo Flisek	samo.flisek@mors.si
South Korea	Sungyeon Park	cooperation@ncsc.go.kr

Spain	Joint Cyberspace Command (MCCE)	mccd-formacion@mde.es
Sweden	Christofer Flygare	christofer.flygare@ccdcoe.org
Switzerland	Eglin Maurice GS-VBS	maurice.eglin@gs-vbs.admin.ch
	Stefan Varonier	stefan.varonier@vtg.admin.ch
Turkiye	Mr. Hakan Aydoğan	haydogan2@tsk.tr
	Lt Erdi Donmez	erdi.donmez@ccdcoe.org
United Kingdom	Lily Edmonds	Lily.Edmonds102@mod.gov.uk
Ukraine	Oleksiy Tkachenko	top@rnbo.gov.ua
USA	Mr. Mark Wilson	mark.s.wilson18.ctr@mail.mil
NATO Command Structure	NATO Requirement Authority	cyocra@shape.nato.int