CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

NATO CCDCOE
TRAINING CATALOGUE, 2022

Tallinn 2021

Tallinn, 15th of November 2021

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE)
12 Filtri tee, 10132 Tallinn, ESTONIA

events@ccdcoe.org

www.ccdcoe.org

Foreword

It is my pleasure to present the 2022 NATO CCDCOE Training Catalogue. With these training offerings, the NATO Cooperative Cyber Defence Centre of Excellence continues its tradition of quality and advances its mission to enhance capability, cooperation and information sharing between NATO, its member nations, and its partners in cyber defence.

Our training activities have been developed by subject-matter experts in cooperation with international organisation and industry to provide knowledge, methods, techniques, and best practices that empower the training audience to effectively cope with the current and emerging real-life cyber challenges.

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

The feedback received from participants has been positive and has been used to improve the 2020 programme. Therefore, I hope that those attending our training activities in 2020 will find the content at least as interesting and relevant as did their predecessors, and I encourage you to share your comments, ideas and suggestions.

As an important milestone in 2018, the NATO ACT provided NATO CCDCOE an unconditional quality assurance accreditation. ACT outlined, that NATO CCDCOE core processes were reviewed and identified as elements that are aligned with NATO Quality Standards. The NATO CCDCOE efforts to set the conditions for quality improvements of education and individual training through effective planning and problem solving, and ultimately raising the level of quality progressively, are commendable.

The still ongoing COVID-19 pandemic presents significant challenges to the activities of the Centre, including training courses, exercises and other events. In 2020, to meet our commitments and continue providing high-quality NATO-accredited Education and Training courses in the context of COVID-19, the Centre has looked for new ways to deliver the courses and successfully transferred some residential courses to online during the fall. Based on the feedbacks of the students, this delivery method was well-received by the participants, however based on the different characteristics of the courses in our portfolio, this delivery method is not applicable for all of the trainings unfortunately. In 2021, the Centre delivered many trainings online too and probably we will deliver some courses also online in 2022 (see the details later).

Please be aware that some details of the training programme, in particular the dates, may be subject to change; and due to the COVID-19 pandemic circumstances (taking into account a change in the dynamics of the infection rate), some of the courses might be cancelled on short notice. Therefore, it is advised that you check the latest information on our website: https://ccdcoe.org/training/.

Finally, I would like to express my gratitude to all those involved in the preparation of these training activities. Training can often be a complicated operation and I could not be prouder of the Centre's staff and partners.

Col Jaak Tarien

Director of NATO Cooperative Cyber Defence Centre of Excellence

Tallinn, Estonia

Contents

Introduction

The programme for 2022 consists of 20 in-house/online courses (technical, legal and operational, one of them is tentative), 9 mobile courses (1 more course is under consideration (tentative status)), several e-Learning courses, two technical cyber exercises, a number of hands-on workshops and an annual conference.

These courses are set up as a resource for Sponsoring Nations (SNs) and Contributing Participants (CPs) of the Centre as well as for NATO bodies. In addition to taking part in the training, the participants can test their individual and collective cyber capabilities, share information and knowledge, and network with the international cyber defence community.

This catalogue provides the information needed to join our courses. It provides an overview of all scheduled activities for 2022 as well as the intended target audience, objectives and prerequisites. Administrative information on logistical issues such as venue, hotel booking and meals is also provided.

Please be aware that some details of the training programme, in particular the dates, may be subject to change; and due to the COVID-19 pandemic circumstances (taking into account a change in the dynamics of the infection rate), some of the courses might be cancelled on short notice. Therefore, it is advised that you check the latest information on our website: https://ccdcoe.org/training/.

The NATO Cooperative Cyber Defence Centre of Excellence is committed to improving the training offerings to address a wide range of aspects of the ever-developing cyber domain.

What we offer

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. Classes are held at NATO CCDCOE facilities in Tallinn.

Due to the effects of the COVID-19 pandemic, some of the courses are planned with optional online delivery (see the details later), if it's feasible.

During 2022, 20 courses are planned to be held in Tallinn or online:

Technical Trainings

- Malware and Exploits Essentials Course (1 iteration)
- Exploit Advanced Course (1 iteration)
- Cyber Defence Monitoring Course Suite
    - Cyber Defence Monitoring Course: Rule-based Threat Detection (1 iteration)
    - Cyber Defence Monitoring Course: Large Scale Packet Capture Analysis (1 iteration)
- IT Systems Attacks and Defence Course (1 iteration)
- Reverse Engineering Malware Course (1 iteration)
- Introductory Digital Forensics Course (2 iterations)
- Industrial Control Systems Security Introductory Course (1 iteration)

Operational Level Training

- Integration Cyber Considerations into Operational Planning Course (2 iterations)
- Critical Information Infrastructure Protection Course (2 iterations)
- Operational Cyber Threat Intelligence Course (2 iterations)

Legal Training

- International Law of Cyber Operations Course (3 iterations).

Strategic Level Training

- Executive Cyber Seminar (2 iterations)

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. During 2021, 9 courses are planned to be held at the Centre's member or NATO locations (or online) and 1 more course is under consideration (tentative status):

- Introductory Digital Forensics Course (1 iteration)
- Cyber Defence Monitoring Course: Rule-based Threat Detection (1 iteration)
- Integration Cyber Considerations into Operational Planning (2 iterations, 1 of tentative, for NATO JFCBS)
- International Law of Cyber Operations Course (1 iteration)
- IT Systems Attack and Defence Course (1 iteration)
- Industrial Control Systems Security Introductory Course (1 iteration)
- Operational Cyber Threat Intelligence Course (1 iteration)
- Reverse Engineering Malware Course (1 iteration)
- Exploit Advance Course (1 iteration)

e-Learning courses

Until 2018, the Centre offered only one e-Learning course, the Cyber Defence Awareness e-Course. (This course is aimed at raising cyber defence awareness for a broad audience, such as NATO IT systems users. The e-Learning platform is chosen since it is the most efficient method to reach a large audience, whilst being flexible and convenient for individual participation.)

In 2018, the online course portfolio has grown to 10 courses including new pre-learning modules for technical courses. The last update of the Cyber Awareness course was published in June, 2019 and the development of two courses were finished in 2020:

- pre-learning module for „Integration of Cyber into Operational Planning" residential course (ADL 375)
- pre-learning module for „Malware and Exploits Essentials Course" residential course (ADL 383)

The development of the pre-learning modules continued in 2021 as well and two new courses were published this year:

- pre-learning module for "IT Systems Attacks and Defence Course" residential course (ADL 394)
- pre-learning module for „Operational Cyber Threat Intelligence Course" residential course (ADL 230)

For 2021, one more e-Learning material are planned:

- pre-learning module for „International Law of Cyber Operations Course" residential course"

The last course also will be available in 2022, therefore the e-Learning portfolio of the Centre will be the following in 2022:

1. ADL 076 Cyber Defence Awareness
2. ADL 365 Cyber Awareness Course Tallinn Manual Module (Pre-study material for International Law of Cyber Operations Course)
3. ADL 335 Cyber Awareness course for System Administrators
4. ADL 344 Digital Forensics and Digital Evidence (Pre-study material for Introductory Digital Forensics Course)
5. ADL 345 Network and Log Monitoring (Pre-study material for Cyber Defence Monitoring Course)
6. ADL 346 Web Application Security (Pre-study material for Web Applications Attack and Defence Course)
7. ADL 347 Critical Infrastructure and Industrial Control Systems (Pre-study material for Industrial Control Systems Security Course)
8. ADL 348 Fighting a Botnet Attack: a Case Study (Pre-study material for Botnet Mitigation Course)
9. ADL 349 Systematic Approaches to the Mitigation of Cyber Threats (Pre-study material for Botnet Mitigation Course)
10. ADL 343 Information Security Management System
11. ADL 375 Pre-learning module for „Integration of Cyber into Operational Planning" residential course
12. ADL 383 pre-learning module for „ Malware and Exploits Essentials Course" residential course
13. ADL 230 pre-learning module for „Operational Cyber Threat Intelligence Course" residential course
14. ADL 394 pre-learning module for „ IT Systems Attacks and Defence Course" residential course
15. *pre-learning for „International Law of Cyber Operations Course" residential course (probably from December, 2021)*

Besides of the e-Learning portfolio, in 2021 due to the COVID-19 pandemic, several courses were delivered online and in 2022, probably several courses will be delivered online again with MS Teams platform (see the details for the potential online iterations in the next chapter). Currently the Centre is able to offer the following residential courses online:

- Integration Cyber Considerations into Operational Planning Course
- IT Systems Attacks and Defence Course
- Operational Cyber Threat Intelligence Course
- International Law of Cyber Operations Course
- Critical Information Infrastructure Protection Course
- Malware and Exploits Essentials Course
- Cyber Defence Monitoring Course: Rule-based Threat Detection Course

In-house training

Malware and Exploit Essentials Course (MExEC)

Location: Location: Online or Tallinn

Date: 16-20 May 2022

Registration starts: 01 Feb 2022

Registration deadline: 01 April 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

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

- Introduction into memory, assembly language and compiling
- Usage of debuggers (GDB, Immunity Debugger, WinDBG)
- Basic exploitation techniques on Linux and Windows systems
- Introduction to fuzzing
- Understand operating system mechanisms like ASLR, SEH and DEP and how they get bypassed
- Basic static (IDA Pro), dynamic (OllyDbg) and behavior analysis on different malware samples
- IOC's writing (Yara)
- Hands-on training of all the learned techniques

Target Audience

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

Outline

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

Prerequisites

- Good work/administration experience in the Linux and Windows environments, especially command line.
- Basic understanding of assembler and higher programming languages (optional).
- Programming experience in assembler, C(++) or PYTHON (optional).
- **The course has a mandatory e-learning module** (ADL 383 "Malware and Exploit Essentials Course", 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. 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.
- English language skill comparable to STANAG 6001, 3.2.3.2.

NB! Please be aware of the strong technical nature of this course: this is not a course for beginners. Note that we most strongly discourage the participation of students who do not fulfil the prerequisites, since the course contains advanced lab sessions assuming this knowledge. Therefore, the presence of unskilled attendees is likely to hinder the overall progress of the course.

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

Module certificate of the ADL 383: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the e-Learning module. When you register for the residential part of the course please email it to: events@ccdcoe.org

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

Exploit Advanced Course (ExAC)

Location: Tallinn, Estonia.

Date: 06-10 June 2022

Registration starts: 15 February 2022

Registration deadline: 15 April 2022.

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

Administration fee: 130 €

Course Aim

The Malware and Exploit Advanced Course will provide a very practical training for skills needed in exploitation research and malware analysis. We will start to develop 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

- Very good practical knowledge in fundamental exploitation techniques
- Introduction to advanced exploitation techniques on Linux and Windows systems
- Exploitation in Heap memory
- Introduction for Kernel exploitation
- 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.

Outline

- Refresh and extend basic skills
  - Buffer overflows
  - ASLR bypass
  - ROP Chain
  - Static and dynamic analysis
- Advanced exploitation techniques
  - Windows
  - Linux
- Introduction to exploitation in heap memory
- Kernel exploitation
- Mitigation mechanisms against Exploitation in operating systems
- Advanced static and dynamic analysis

Prerequisites

- Attended “Malware and Exploit Essentials Course” or good and practical knowledge about the basic techniques in Exploit Research.
- **The course has a mandatory e-learning module** (ADL 383 “Malware and Exploit Essentials Course”, 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. 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.
- Good work experience in Linux and Windows environments, especially command line.
- Understanding of assembly and higher programming languages.
- Programming experience in assembly, C(++) and/or PYTHON.
- English language skill comparable to STANAG 6001, 3.2.3.2.

NB! Please be aware of the strong technical nature of this course**: this is not a course for beginners.** Note that we most strongly discourage the participation of students who do not fulfil the prerequisites, since the course contains advanced lab sessions assuming this knowledge. Therefore, the presence of unskilled attendees is likely to hinder the overall progress of the course.

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

Module certificate of the ADL 383 or the certificate of the “Malware and Exploit Essentials” course: One of the certificates is necessary when applying for the residential part of the course. You can download the certificate of the ADL 383, once you successfully finish the final test of the e-Learning module. When you register for the residential part of the course please email one of the certificates (or both) to: events@ccdcoe.org

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

Cyber Defence Monitoring Course Suite

Cyber Defence Monitoring Course: Rule-based Threat Detection

Location: Online or Tallinn

Date: 03 - 07 October 2022 ***(in the case of the online delivery, the course will be a two weeks long course)***

Registration deadline: 19 August 2022.

Registration starts: 04 July 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

This intensive hands-on course concentrates on a single solution from several important Cyber defence monitoring techniques and solutions. We focus only on rule-based threat detection, more widely known as *Intrusion Detection*. We will use Suricata, an open-source free software tool, to build network security monitoring for different scales, from SOHO/SME up to enterprise level.

Because of the required high level standards and skills described in the "Prerequisites" below, we most strongly discourage the participation of students who do not fulfil these prerequisites, since the course contains advanced lab sessions assuming this knowledge. Therefore, the presence of unskilled attendees is likely to hinder the overall progress of the course.

Learning Objectives

The course demonstrates how Suricata is a perfect fit for modern network security monitoring. Attendees gain practical experience on how to build up a scalable system and how challenging the security-engineering process can be. During hands-on exercises, students start from the basic single instance installation and end up implementing a distributed system with centralised command, analysis and visualisation solutions.

Target Audience

- Technical IT security staff in charge of network security monitoring.
- Security and IT managers who want to get a real-life understanding of Suricata.

Non-target audience:

Outline

- Installing a single instance for small office network.
- Building from source to get a custom set of required features.
- Controlling the rule base.
- Tweaking protocols and artefact extraction.
- Tweaking outputs with scripting.
- Controlling a large setup.
- Gathering logs and extractions.
- Visualising for humans.

Prerequisites

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

NB! We most strongly discourage the participation of students who do not fulfil these prerequisites, since the course contains advanced lab sessions assuming this knowledge. Therefore, the presence of unskilled attendees is likely to hinder the overall progress of the course.

Course materials:

The lecture and lab materials for this course are publicly available on the following GitHub page: https://github.com/ccdcoe/CDMCS/tree/master/Suricata

Materials will be updated prior to each course.

Recommended for attendees without prior system or network monitoring experience:

ADL 345 Network and Log Monitoring on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

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: events@ccdcoe.org.

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

Cyber Defence Monitoring Course: Large Scale Packet Capture Analysis

Location: Tallinn

Date: 13 - 17 June 2022

Registration deadline: 02 May 2022

Registration starts: 14 March 2022

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

Administration fee: 130 €

Course Aim

The Locked Shields technical environment is very complex and Blue Teams need a network traffic overview to plan their strategy. It is also essential to have an overview of what happened in the network during execution. This course will make use of the latest Locked Shields execution network traffic capture as a learning material.

This intensive hands-on course concentrates on a single solution out of several important Cyber Defence Monitoring techniques and solutions. We will focus only on packet capture and analysis. It is not meant to replace IDS engines, but instead work alongside them to store and index all the network traffic and providing fast access to the captured data. We use Moloch, an open-source free software tool, to build network security monitoring for different scales, from SOHO/SME up to enterprise level.

Learning Objectives

The course demonstrates how Moloch is a perfect fit into modern network security monitoring. Attendees gain practical experience of how to build up a scalable system and how challenging the security-engineering and analysis process can be.

Target Audience

- Locked Shields Blue Team members and/or national representatives.

Outline

- Methods used to conduct network traffic analysis.
- Installing a single instance for small office network.
- Building from source to get a custom set of required features.
- Controlling a large setup.
- Using APIs for integration.
- Using proxies/aggregators to get data from external sources.
- Scaling up to 10Gb+.

- Scaling up months of history.
- Separation concerns.

On this course, we will work with network traffic from the recent Locked Shields, which means that the traffic will have real intrusions.

Prerequisites

- Good understanding of TCP/IP networking and network and system administration.
- Recent everyday network/system administrator's work experience for at least **2 years** in UNIX environments.
- Previous detailed knowledge on the following topics:
  - work principles of UNIX operating systems and UNIX file system layout;
  - common UNIX shells (e.g., sh, bash);
  - common UNIX user tools (e.g., ls, ps, kill); and
  - common UNIX system administration utilities.
- Scripting experience is required.
- Basic Python skills are required: ability to write a function, for loop, invoke standard library and use core data.
- English language skill comparable to STANAG 6001, 3.2.3.2.

NB! We most strongly discourage the participation of students who do not fulfil these prerequisites, since the course contains advanced lab sessions assuming this knowledge. Therefore, the presence of unskilled attendees is likely to hinder the overall progress of the course.

Course materials:

The lecture and lab materials for this course are publicly available on the following GitHub page: https://github.com/ccdcoe/CDMCS/tree/master/Suricata

Materials will be updated prior to each course.

Recommended for attendees without prior system or network monitoring experience:

ADL 345 Network and Log Monitoring on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

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: events@ccdcoe.org.

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

IT Systems Attack and Defence Course (ITSADC)

Location: Tallinn or online

Date: 19-23 September, 2022

Registration starts: 28 June 2022

Registration deadline: 2 August 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

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.

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:

- Phases of a cyber-attack:
  - Reconnaissance.
  - Scanning and Enumeration.
  - Gaining Access.
  - Privilege Escalation.
  - Lateral Movement.
- Provide an overview of common tools used by penetration testers and attackers.
- Show various ways of doing reconnaissance.

- Understand, see and do different ways of network scanning.
- See and do different ways of network infrastructure attacks.
- See and do different types of DNS attacks.
- Explore Web Application Security:
    - Main building blocks of web applications.
    - Session management and authentication attacks.
    - Injection attacks (SQL injection, OS command injection, File inclusion, Insecure file upload functionality).
    - Cross-site scripting.
    - Cross-site request forgery.
- Get an overview of various protection mechanisms and common misconfigurations in a Windows domain environment.
- See and do stealing credentials from Windows systems and using them to conduct Pass-the-Hash and Pass-the-Ticket attacks.
- Conduct man-in-the-middle attacks.
- Use Metasploit Framework and existing exploit code against different targets, including client-side attacks.
- Exploit 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. Professional security practitioners or penetration testers with years of experience are not the target audience for this course.

Outline

- Introduction of the lab environment. The basics of Kali Linux and Metasploit.
- Reconnaissance: sources and tools for gathering information about target networks.
- Network scanning: host discovery, TCP and UDP port scanning, operating system detection, vulnerability scanning, scanning in IPv6 networks, honeypots and tarpits.
- Enumeration: using DNS, SNMP and other protocols to identify potential vulnerabilities.
- 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.
- 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.

- DNS security: DNS overview, DNS tunnelling, DNS rebinding, DNS snooping, cache poisoning attacks, DNSSec.
- Windows Security: Pass-the Hash, Pass-the-Ticket, Kerberos 'Silver and Golden Ticket Attack', Authentication methods, Security mechanisms, Privilege escalation, Process injection.
- Web Application Security:
    - Main building blocks of web applications.
    - Session management and authentication attacks.
    - Injection attacks:
        - SQL injection.
        - OS command injection.
        - File inclusion.
        - Insecure file upload functionality.
    - Cross-site scripting.
    - Cross-site request forgery.

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

- Using various open-source or freely available tools for information gathering from public sources.
- Scanning small networks to finding alive hosts or machines with specific vulnerabilities.
- Using DNS enumeration to find interesting hosts, exploiting unprotected SNMP service for enumeration of information.
- Tunnelling arbitrary IP traffic over DNS protocol in restrictive environment.
- Guessing and cracking passwords.
- Stealing credentials from Windows systems and using them to conduct Pass-the-Hash/Pass-the-Ticket attacks.
- 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.
- Using Metasploit Framework and existing exploit code against different targets. This includes client-side attacks.
- Exploiting vulnerabilities in custom-built web applications.

Prerequisites

- 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).
- Programming skills are helpful.
- English language skill comparable to STANAG 6001, 3.2.3.2. is required.
- 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).

- **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. 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.
-

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: events@ccdcoe.org.

Module certificate of the ADL 394: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the e-Learning module. When you register for the residential part of the course please email it to: events@ccdcoe.org

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

Reverse Engineering Malware Course (REMC)

Location: Tallinn, Estonia or online

Date: 03 - 07 October 2022

Registration deadline: 19 August 2022.

Registration starts: 04 July 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

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. Year 2021 iterations 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

Goal of this course is to deliver to the participants following skills and knowledge:

- Understanding malware: life-cycle and motivation of their creators.
- Identifying malware related activity in endpoints and networks.
- Autonomously collect information and analyze samples from multiple stages of malware.
- Producing and using indicators of malware related activity.
- Work as team while identify and search for IoC's.

Topics

- Cybersecurity incident life cycle; Lockheed Martin Kill Chain.
- Preparing the lab
  - Tools and skills; safety
- ”Black box” analysis
  - Monitoring host activity
  - Monitoring network activity
  - Collecting and selecting meaningful observable indicators
- Deobfuscating Code in a Word Macro
- Reverse Engineering Basics
  - Introduction into Assembly
- Familiarizing reverse engineering
- Static analysis (IDA Pro)
- Dynamic analysis (OllyDbg, WinDgb)
- Writing IOCs (Yara rules)
- Familiarizing with Ghidra debugger
- Making systems more resilient to the attacks

    - Collecting and sharing IOCs
    - Network architecture
    - Endpoint security
    - Automating mitigation
- Anti-Debugging and Anti-VM Techniques
- Practice: teamwork with parallel tasks for solving malware activity related incident

Target Audience

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

Prerequisites

- Good work/administration experience in Linux (as the work environment) and Windows (as the malware environment).
- Basic understanding of network traffic and malware.
- Ability to use virtual machine technology (Virtualbox or similar).
- Experience with firewalls and network traffic analysis (Wireshark and similar).
- Basic understanding of assembler and higher programming languages.
- Scripting language skill (Python, Visual Basic, Bash).
- English language skill comparable to STANAG 6001, 3.2.3.2.

NB! Please be aware of the strong technical nature of this course. It is not intended for inexperienced IT security specialists. The topics covered in this course are mostly similar to the previously given Botnet Mitigation Course. Therefore, this course is not recommended for previous participants of the BMC.

Pre-study e-Learning material

- Malware Reverse Engineering Handbook from the CCDCOE website (https://ccdcoe.org/library/ publications/)
- 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/)

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: events@ccdcoe.org.

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

Introductory Digital Forensics Course (IDFC)

First iteration:

Location: Tallinn, Estonia or online

Date: 27 June – 01 July 2022

Registration deadline: 13 May 2022

Registration starts: 01 April 2022.

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Second iteration:

Location: Tallinn, Estonia or online

Date: 26-30 September 2022

Registration deadline: 12 August 2022.

Registration starts: 27 June 2022.

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

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. Experienced digital forensic staff doing forensics on a regular basis are not the target group and will receive only limited benefit from attending.

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

Learning Objectives

- Provide an introduction to digital forensics investigation, explain related terminology, methodology, principles and steps to conduct digital forensic investigation,
- Provide an overview about prospective digital evidence (assuming exclusively Windows hosts),
- Understand technical and procedural limitations while conducting digital forensic investigation,
- Learn and practice digital forensic investigation techniques, focusing primarily on open source/free forensic software (no commercial solutions),

- Conducting forensic investigation through a number of hands-on sessions,
- Prepare course students for more in-depth forensics/reverse engineering training.

Target Audience

- 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.
- 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.
- IT staff who will acquire an initial skill set of how to conduct forensic investigation.

Outline

- Introduction to Digital Forensics.
- Forensic process and workflow (theory):
    - Terminology, Methodology, Principles, Chain of Custody.
- Evidence Acquisition block (theory and hands-on):
    - System description and verification.
    - Different types of evidence and locations.
    - Forensic software/hardware for evidence acquisition.
    - Acquisition process.
    - Evidence handling.
- Analysis (theory and hands-on):
    - File system analysis,
    - Media analysis,
    - Windows OS analysis
    - Timeline analysis,
- Data carving and application fingerprinting (theory and hands-on).
- Internet activities focus (theory and hands-on):
    - Browser, Email, Instant Messaging Forensics.

Added Value

- IT staff without forensic knowledge will ‘understand’ digital forensic capabilities, raising awareness and improving possible future support.
- Basic knowledge to ensure that evidence is not spoiled by the acquisition process and all available evidence is collected.
- Security awareness training for staff to understand the traces left behind on a system which can lead to intelligence gathered by others.
- Practising forensic methods on the basis of prepared, exemplary exercises.

Prerequisites

- Good work/administration experience in the Linux and Windows environments, especially command line,
- Comfortable with using virtual machines for training environment,
- English language skill comparable to STANAG 6001, 2.2.2.2.

NB! This course will provide an overview and is not meant to provide an in-depth introduction of forensic methods or tools.

Pre-study e-Learning material

ADL 344 Digital Forensics and Digital Evidence (Pre-study material for Introductory Digital Forensics Course) on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

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: events@ccdcoe.org.

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

Industrial Control Systems Security Introductory Course (ICSSIC)

Location: Tallinn, Estonia.

Date: 05-08 September 2022

Registration deadline: 01 August 2022.

Registration starts: 01 June 2022

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

Administration fee: 130 €

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

- Understand the basics of Industrial Control Systems.
- Understand the PLC programming methods.
- Get to know the basic tools and software.
- Manipulate Industrial Control Systems by exploiting their vulnerability.
- 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

- Basic knowledge Windows and Linux based systems
- Basic knowledge and experience with network traffic analysis (Wireshark or similar).
- Basic knowledge and experience in programming.
- Comfortable with using virtual machines for training environment (Virtual Box or similar).
- English language skill comparable to STANAG 6001, 2.2.2.2

Pre-study e-Learning material

ADL 347 Critical Infrastructure and Industrial Control Systems (Pre-study material for Industrial Control Systems Security Course) on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

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: events@ccdcoe.org.

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

Integration Cyber Considerations into Operational Planning Course (ICCOP)

First iteration:

Location: Tallinn, Estonia or online.

Date: 14-18 March 2022

Registration deadline: 28 January 2022.

Registration starts: 01 December 2021

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Second iteration:

Location: Tallinn, Estonia or online.

Date: 13-17 June 2022

Registration deadline: 02 May 2022

Registration starts: 01 March 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

Provide 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

- Identify the concept and implications of cyberspace as a domain of operations.
- Implement cyberspace considerations into the comprehensive operations planning process.
- Recognize NATO and national organization, capabilities and limitations on cyberspace operations.

Target Audience

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

Outline

- Cyberspace overview and taxonomy
- Cyberspace as domain of operations
- Integration of Cyber in the operations planning process
- Cyber incidents handling in the execution of military operations.
- Cyber intelligence
- Risk assessment/risk management
- NATO perspective on Cyber Operations
- National perspective on Cyber Operations.
- Cyber organization in NATO
- NATO technical capabilities
- Legal considerations and Rules of Engagement in Cyber Operations
- Host Nation critical infrastructure: coordination with national authorities during cyber crisis situations.

Prerequisites

- 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).
- 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).
- **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. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> ADL 375 'Integration of Cyber Considerations into Operational Planning' course listing.
- English language skill comparable to STANAG 6001, 3.3.3.2.

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: events@ccdcoe.org.

Module certificate of the ADL 375: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the e-Learning module. When you register for the residential part of the course please email it to: events@ccdcoe.org

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

Critical Information Infrastructure Protection Course (CIIPC)

First iteration:

Location: Tallinn, Estonia or online.

Date: 23 – 27 May 2022

Registration deadline: 08 April 2022.

Registration starts: 08 February 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Second iteration:

Location: Tallinn, Estonia or online.

Date: 10 – 14 October 2021

Registration deadline: 26 August 2022

Registration starts: 11 July 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

NB! Please note that the ongoing pandemic situation may necessitate that one or both iterations of this course will be done as an online-course. In that case, the course will last only 4 days.

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:

- be able to understand what constitutes Critical Information Infrastructure and the threats to its operations;
- be able to assess the vulnerabilities and the threat profiles relative to Critical Information Instructure;
- be able to make proper decisions regarding protection of Critical Information Infrastructure, including training of personnel, investment in protection, information sharing and risk assessment;

- Be able to oversee and critique a comprehensive Risk Assessment of both cyber and physical vulnerabilities for select Critical Information Infrastructure; and
- Know how to prioritise the protection of the most critical core information infrastructure for a military operation, institution, government or private sector enterprise.

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.

Pre-Course Preparation

Select readings will be identified and made available to registered students before the courses. These are to be read prior to course participation.

Pre-study e-Learning material

- ADL 343 Information Security Management System on the NATO e-Learning website **(JADL - https://jadl.act.nato.int/)**

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: events@ccdcoe.org.

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

International Law of Cyber Operations Course (ILoCOC)

First iteration:

Location: Tallinn, Estonia or online

Date: 14-18 February 2022

Registration deadline: 14 January 2022.

Registration starts: 22 November 2021

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Second iteration:

Location: Tallinn, Estonia or online.

Date: 16-20 May 2021

Registration starts: 01 February 2022

Registration deadline: 01 April 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Third iteration:

Location: Tallinn, Estonia or online.

Date: 28 November – 2 December 2022

Registration deadline: 17 October 2022.

Registration starts: 05 September 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

The course provides an understanding of the legal framework in which cyber operations involving states occur during both peace- and war-time. Participants will learn to apply to real-world situations the legal principles and rules examined.

This 4,5-day residential course includes lectures dedicated to introducing the technology involved in cyber operations, covering internet structure, defensive and offensive tools and techniques, as well as the feasibility of and challenges to technical attribution. Additionally, it examines NATO Cyber Defence Policy and the role of cyber operations in the contemporary geopolitical environment.

The core of the course is divided into two blocks of study:

- Peacetime international law governing cyber operations
- International humanitarian law that applies during armed conflict involving cyber operations

The sessions (on Tuesday, Wednesday and Thursday afternoon) conclude with a complex exercise that allows participants to apply the law addressed during lectures and discussion. The peacetime law session deals with issues like sovereignty, jurisdiction, due diligence, the law of state responsibility, the prohibition of intervention and self-defence, all in the cyberspace operations context. It will answer questions such as which cyber operations outside an armed conflict violate international law, when can states hack back, and when has a cyber armed attack occurred such that states may engage in self-defence. The session dedicated to jus in bellum - covers traditional international humanitarian law topics, such as classification of cyber conflict, the principle of distinction during cyber operations, and targetable and protected persons and objects in the cyber context. This session is taught from an operational legal advisor's perspective, examining all necessary steps in a cyber targeting legal analysis. The lectures will be given by noted scholars and practitioners, some of them members of the group of authors of the Tallinn Manual 2.0. Participants will also receive a complimentary copy of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

Learning Objectives

Provide a practice-oriented survey of the international law applicable to cyber operations involving states that occur both in peacetime (Block 1) and armed conflict (Block 2).

Block 1 answers questions such as which cyber operations outside an armed conflict violate international law, when can states hack back, and when has a cyber armed attack occurred such that states may engage in self-defence

Block 2 covers traditional international humanitarian law topics, and is taught from an operational legal advisor's perspective, examining all necessary steps in a cyber targeting legal analysis

The course begins with one module dedicated to the technology involved in cyber operations

Target Audience

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

Prerequisites

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

Pre-study e-Learning material

ADL 365 Cyber Awareness Course Tallinn Manual Module on the NATO e-Learning website (JADL - https://jadl.act.nato.int/)

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: events@ccdcoe.org.

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

Operational Cyber Threat Intelligence Course (OCTIC)

First iteration:

Location: Tallinn, Estonia or online.

Date: 28 February - 04 March 2022

Registration starts: 29 Nov 2021

Registration deadline: 21 January 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Second iteration:

Location: Tallinn, Estonia or online.

Date: 14-18 November 2022

Registration deadline: 03 October 2022.

Registration starts: 22 August 2022

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

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

To provide knowledge about the cyber threat intelligence at the operational level, that is responsible for planning cyber activity, having also a view on NATO doctrine on Cyber Operations. To provide a clear comprehension of the main data you need to plan cyber operations, having acquired knowledge about the Intel Cycle to the cyber domain. You will identify the gaps you need to fill and drive the collection phase, tasking the correct sources to gather needed information. Having understanding of the Cyber Intel process, you will understand how to transform them into a possible cyber threat situation by using a sharing platform environment (MISP).

Learning Objectives

- To acquire knowledge on NATO doctrine on Cyber operations and future NATO development.
- To acquire knowledge on cyber intelligence, cyber threat intelligence and cyber situational awareness.
- To acquire knowledge on Cyber Kill chain, Diamond model, Mitre ATT&CK platform.

- To acquire the essential elements of understanding the cyber domain for Intelligence purposes, identifying data useful for planning cyber activities and gaining a better understanding of the enemy's cyber capability, taking also into account cyber resilience and cyber deterrence.
- To gain knowledge with the main technical data available through the network, understanding OSINT sources that could be used to collect this information.
- To gain knowledge with the main data available through social networks and social media, understanding which sources could be used to collect this information.
- To gain essential knowledge on MISP.
- To gain essential knowledge on a SOC organization.
- To gain essential knowledge on threat haunting.

Target Audience

J2, J3, J5, J6 staff members, branch heads, RRT/CERT members, Cyber Threat Analysts, mediators between Tech Level and Operational level.

Outline

- Nato Doctrine on Cyber Ops
- Intel cycle applied to the cyber domain
- Cyber kill chain, Diamond model, MITRE Att@ck platform
- Cyber Defence Threat Assessment
- Intelligence Support to Cyber Operations
- Cyber deterrence and cyber resilience
- OSINT and Social media gathering information
- Information sharing (MISP)
- Cyber situational awareness
- Exercises

Prerequisites

- The Integration of Cyber Considerations into Operational Planning e-Learning course (ADL 375, see the details in the "Online training" chapter) that can be accessed through the NATO e-Learning Joint Advanced Distributed Learning portal is recommended for the students of the course. Once registered, users may access the course by navigating to the 'Centres of Excellence' -> 'COE Cyber Defence' -> ADL 375 'Integration of Cyber Considerations into Operational Planning' course listing.
- **The course has a mandatory e-learning module** (ADL 230 "Operational Cyber Threat Intelligence Course", 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. 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.

- English language skill comparable to STANAG 6001, 3.3.3.2.
- Basic knowledge of Windows and Linux, TCP/IP stack, social media, virtualisation product and good understanding of technical cyber vocabulary and means.

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: events@ccdcoe.org.

Module certificate of the ADL 230: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the e-Learning module. When you register for the residential part of the course please email it to: events@ccdcoe.org

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

Executive Cyber Seminar (ECS)

First iteration:

Location: Tallinn, Estonia.

Date: 07 – 09 March 2022

Registration deadline: 28 January 2022

Registration starts: 15 November 2021

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

Second iteration:

Location: Tallinn, Estonia.

Date: 21 – 23 November 2022

Registration deadline: 10 October 2021

Registration starts: 24 August 2021

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

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

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

Target Audience

- 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
- 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.

Prerequisites

NA

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: events@ccdcoe.org.

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

Mobile training

During 2022, the Centre will deploy its trainers and training devices at the Centre's member location(s) to provide 9 courses and 1 more course are under consideration (tentative status):

- Introductory Digital Forensics Course (1 iteration)
- Cyber Defence Monitoring Course: Rule-based Threat Detection (1 iteration)
- Integration Cyber Considerations into Operational Planning (2 iterations, 1 of tentative, for NATO JFCBS)
- International Law of Cyber Operations Course (1 iteration)
- IT Systems Attack and Defence Course (1 iteration)
- Industrial Control Systems Security Introductory Course (1 iteration)
- Operational Cyber Threat Intelligence Course (1 iteration)
- Reverse Engineering Malware Course (1 iteration)
- Exploit Advance Course (1 iteration)

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.

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. Depending on the COVID-19 situation, the mobile trainings might be delivered online as well.

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

e-Learning courses

Cyber Defence Awareness e-Course (ADL 076)

Date: On demand.

Course fee: free.

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 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

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

- Threats to and from mobile devices.
- Backing up systems and files.
- File sharing and copyright issues.
- The dangers of unsecured wireless networks.
- Desktop security.
- Social engineering and other human aspects.
- Disposal of information.
- 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.

Cyber Awareness Course, Tallinn Manual Module (ADL 365)

Date: On demand.

Course fee: free.

Course Aim

To provide a pre-study material for the International Law of Cyber Operations Course (residential course of the Centre).

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

- Understand the nature and context of cyber operations and cyber attacks
- Identify and apply the international legal framework that regulates the “Use of Force” under the UN Charter in the cyber context
- Recognize the role of the Tallinn Manual in the articulation of the legal framework applying to cyber warfare
- Apply principles of International Humanitarian Law to cyber warfare

Target Audience

The TA of this module is the same TA, as the targeted TA of the International Law of Cyber Operations Course.

Outline

- Nature and context of cyber operations and cyber attacks
- International legal framework that regulates the “Use of Force” under the UN Charter in the cyber context
- Role of the Tallinn Manual in the articulation of the legal framework applying to cyber warfare
- Principles of International Humanitarian Law to cyber warfare

Prerequisites

The requirements of the International Law of Cyber Operations Course are also valid here.

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.

Cyber Awareness Course for System Administrators (ADL 335)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on different cyber awareness and technical related topics, targeting network and system administrators.

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.

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.

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

- Information Security Management System
- Digital Forensics and Digital Evidence
    - Digital Forensics and Digital Evidence (in general)
    - Digital Forensic Process
    - Acquisition of Digital Evidence
    - Examination and Analysis of Digital Evidence

- Network and Log Monitoring
    - Network Monitoring
    - Log Monitoring
- Web Application Security
- Critical Infrastructure and Industrial Control Systems
- Fighting a Botnet Attack: a Case Study
- 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.

“Digital Forensics and Digital Evidence” Course (ADL 344)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on digital forensics and digital evidence to support the preparation of the participants of the Introductory Digital Forensics 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

- Define the scope of the science of digital forensics.
- Define digital evidence and give examples of it.
- Describe the legal status of digital evidence.
- Define the concepts of integrity and authenticity that laws about digital evidence deal with.
- Describe the difference between digital forensics and incident response.
- List the areas of digital forensics.
- 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.
- Differentiate between dead and live acquisition of digital evidence and explain in what situations which mode of acquisition should be preferred.
- Define memory and disk imaging.
- Describe the possible methods of acquisition of memory images and specify which of them are safe to use in digital forensics and which not.
- Describe the functionalities of different formats of disk images.
- List the types of evidence that can be found from the system's memory.
- List the types of evidence that can be found when examining Windows OS.
- Give examples of the information that an investigator can find and deduce when examining web browser artifacts.
- Describe the limits of the recovery of instant messages.
- Describe the elements of an e-mail that an investigator should examine.

Target Audience

The TA of this module is the same TA, as the targeted TA of the Introductory Digital Forensics Course.

Outline

- Digital Forensics and Digital Evidence
- Digital Forensic Process
- Acquisition of Digital Evidence
- Examination and Analysis of Digital Evidence

Prerequisites

The requirements of the Introductory Digital Forensics Course are also applicable here.

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.

“Network and Log Monitoring” Course (ADL 345)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on network and log monitoring to support the preparation of the participants of the different modules to the Cyber Defence Monitoring Suite.

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

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

Target Audience

The TA of this module is the same TA, as the targeted TA of the Introductory Digital Forensics Course.

Outline

- Network Monitoring
  - Instructions about the sensor placement in a Network Intrusion Detection and Prevention Systems (NIDS/NIPS) are provided. Common network monitoring solutions are introduced as well.
- Log Monitoring

- First, the BSD syslog protocol, used for event logging, is described. Then, tools and solutions for log collection, log correlation and log analysis are introduced.

Prerequisites

The requirements of the Cyber Defence Monitoring Suite modules are also applicable here.

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.

“Web Application Security” Course (ADL 346)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on web application security to support the preparation of the participants of the Web Applications Attack and Defence 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

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

Target Audience

The TA of this module is the same TA, as the targeted TA of the Web Applications Attack and Defence Course.

Outline

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

Prerequisites

The requirements of the the Web Applications Attack and Defence Course are also applicable here.

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.

“Critical Infrastructure and Industrial Control Systems” Course (ADL 347)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on critical infrastructure and industrial control systems 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

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

Target Audience

The TA of this module is the same TA, as the targeted TA of the Industrial Control Systems Security Course.

Outline

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

Prerequisites

The requirements of the Industrial Control Systems Security Course are also applicable here.

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.

“Fighting a Botnet Attack: a Case Study” Course (ADL 348)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on fighting a botnet attack (as a case study) to support the preparation of the participants of the Botnet Mitigation 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

- Give examples of the goals behind botnet attacks and describe the botnet attack chain step by step.
- Give examples of the ways of making the planning of a botnet attack harder for attackers.
- 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.
- Explain why it is important to look for indicators of persistence of a malicious payload.
- List the methods to use to protect an infrastructure against the execution of a botnet attack.

Target Audience

The TA of this module is the same TA, as the targeted TA of the Botnet Mitigation Course.

Outline

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

Prerequisites

The requirements of the Botnet Mitigation Course are also applicable here.

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.

“Systematic Approaches to the Mitigation of Cyber Threats” Course (ADL 349)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on systematic approaches to the mitigation of cyber threats, to support the preparation of the participants of the Botnet Mitigation 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

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

Target Audience

The TA of this module is the same TA, as the targeted TA of the Botnet Mitigation Course.

Outline

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

Prerequisites

The requirements of the Botnet Mitigation Course are also applicable here.

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.

Information Security Management System Course (ADL 343)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on the theory of Information Security Management Systems, to support the preparation of the participants of the Centre residential technical courses.

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

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

Target Audience

The TA of this module is the same TA, as the targeted TA of most of residential technical courses provided by the Centre.

Outline

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

Prerequisites

The requirements of most of residential technical courses provided by the Centre are also applicable here.

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.

Integrating Cyber Considerations into Operational Planning (ADL 375)

Date: On demand.

Course fee: free.

Course Aim

This course is a **mandatory** e-learning module of the residential **Integrating Cyber Considerations into Operational Planning course**. 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, where the students who earned **the certificate for this module** can continue their studies with practical scenarios and examples.

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

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

Target Audience

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

Outline

- **Integrating cyber operations into operational planning**
    - Characterizing cyberspace
    - Recognising distinguishing aspects of the domain
    - Identifying the applicable aspects of the existing international law
- **Cyber intelligence and risk cycles**
    - Describing the specifics of the intelligence cycle in relation to cyberspace
    - Describing the specifics of the risk management cycle in relation to cyberspace
- **Cyber during the Comprehensive Operations Planning Process (COPP)**
    - Identifying the four types of cyberspace operations
    - Listing cyberspace-related issues that should be addressed during the Comprehensive Operations Planning Process

    - Explaining the role of the cyber cell role in an operational headquarters during the execution of operations

Prerequisites

- 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).
- 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).
- 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.

Module certificate: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the module. When you register for the residential part of the course please email it to: events@ccdcoe.org.

Malware and Exploit Essentials (ADL 383)

Date: On demand.

Course fee: free.

Course Aim

This course is a **mandatory** e-learning module of the residential **Malware and Exploit Essentials** course. 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, where the students who earned **the certificate for this module** can continue their studies with practical scenarios and examples.

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:

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

Exploit module:

- Describe the meaning of an exploit
- Describe the basic concept of memory in a modern operating system
- Compile executable files in Linux

- Follow the basic instructions in assembly language
- 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

- Good work/administration experience in the Linux and Windows environments, especially command line.
- Basic understanding of assembler and higher programming languages (optional).
- Programming experience in assembler, C(++) or PYTHON (optional).
- 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.

Module certificate: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the module. When you register for the residential part of the course please email it to: events@ccdcoe.org.

IT Systems Attacks and Defence (ADL 394)

Date: On demand.

Course fee: free.

Course Aim

This course is a **mandatory** e-learning module of the residential **IT Systems Attacks and Defence** course. 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, where the students who earned **the certificate for this module** can continue their studies with practical scenarios and examples.

The residential 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.

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:

- Networks and threat models
- Attacks and attackers
- Reconnaissance
- Scanning and Enumeration
- Local network attacks
- Internet Infrastructure attacks
- 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 these individuals 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

- 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).
- Programming skills are helpful.
- 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.

Module certificate: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the module. When you register for the residential part of the course please email it to: events@ccdcoe.org.

Operational Cyber Threat Intelligence (ADL 230)

Date: On demand.

Course fee: free.

Course Aim

This course is a **mandatory** e-learning module of the residential **Operational Cyber Threat Intelligence** course. 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, and this way establish a common basis of knowledge for the students attending the residential part of the course, where the students who earned **the certificate for this module** can continue their studies.

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:

- Cyber Threat Intelligence
- Cyber Threat Intelligence Cycle
- Cyber Threat Intelligence Sources
- Cyber Threat Intelligence Tools
- Actionable Intelligence and Threat Hunting
- Operational Security
- Sharing Threat Information
- 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

- The Integration of Cyber Considerations into Operational Planning e-Learning course (ADL 375) is recommended for the students of the course.
- English language skill comparable to STANAG 6001, 3.3.3.2.
- Basic knowledge of Windows and Linux, TCP/IP stack, social media, virtualisation product and good understanding of technical cyber vocabulary and means.

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.

Module certificate: It is necessary when applying for the residential part of the course and you can download it once you successfully finish the final test of the module. When you register for the residential part of the course please email it to: events@ccdcoe.org.

Administrative issues for in-house courses

Registration

To register for a particular training activity in this catalogue, please follow the instructions specified in the paragraph ‘Registration’ in the corresponding course.

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

General procedure:

- For most of the courses, the potential applicants need a Registration Code. These codes are shared with the official Education & Training POCs at the particular nation, and the Registration Code is different for each course iteration.
- For the free seat at a course (only the Administration fee will apply), the applicant needs a Discount Code, this code should be applied at the end of the registration process. The Discount Code is different for each nation and shared only with the official Education & Training POCs at the particular nation.

Regarding the official Education & Training POCs, please look Annex B.

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: Estonian Ministry of Foreign Affairs website.

COVID-19 related assumptions and countermeasures

The ongoing COVID-19 pandemic presents significant challenges to the activities of the NATO CCDCOE, including training courses, exercises and other events.

To meet our commitments and continue providing high-quality NATO-accredited Education and Training courses in the context of COVID-19, the Centre has looked for new ways to deliver courses, e.g. virtual classrooms or other online training facilities. As there will be some residential events and courses, a set of guidelines for participants must be followed.

The NATO CCDCOE will adhere to official rules and safety standards set by Estonian Government, i.e. the Host Nation (EST). Persons signed up for the events organised by the NATO CCDCOE are not allowed to attend in person if they are not able to provide a certificate about the full COVID-19 vaccination (2 doses) or a certificate of their recovery. It means, that the Centre won't accept other students, even if they will provide any kind of test certificate. The potential applicants can check the current Estonian regulations here, and they should send their certificate (full vaccination or recovery) to the events@ccdcoe.org email address before the particular course.

Taking into account a change in the dynamics of the infection rate, NATO CCDCOE may cancel the registration on short notice. The NATO CCDCOE will inform any attendees concerned directly, however, at the same time it is still strongly recommended to check for updates at reasonable time prior to the travelling to Estonia at the website of the Ministry of Foreign Affairs (linked above).

COVID-19 related restrictions in Estonia

- **The participants may only begin their travel to Estonia if they are healthy (they have no symptoms of an infectious disease). They may also only participate in classroom lectures and seminars if they are healthy.**
- The Estonian government calls on individuals to maintain a safe distance from others whenever possible both indoors and outdoors. This applies to all public spaces, including shopping centres, religious institutions, saunas, spas, entertainment venues, schools, sports venues, and museums.
- Wearing a mask is recommended for all in enclosed, crowded places such as shopping malls, individual shops, and on public transit.
- **Self-isolation is mandatory for everyone showing symptoms of an infectious disease.**

- **Please note that NATO CCDCOE´s training facilities (EDF / EST MOD territory) is not suitable for self-isolation.**

Organisational restrictions and guidance during the courses

- The participants always have to use the hand sanitiser, when entering the training facilities, and also wash their hands well and often to avoid the contamination.
- All persons entering the NATO CCDCOE training facilities are required to social distance.
- **Wearing a face mask is compulsory at all times.**
- Lunch will be provided by the NATO CCDCOE at the training facilities for all the course participants throughout the course week. (See the details below in the Lunch breaks section.)
- **Course participants and speakers not adhering to these requirements will not be allowed to the NATO CCDCOE training facilities.**

What to do if a course participant suspects having contracted coronavirus?

Based on recommendations by the Health Board

1. Anyone in Estonia who thinks they have symptoms should contact the family physician advisory line, **1220**. If you have general questions about the virus, you can call the Estonian Alarm Center's COVID-19 Helpline at **1247**, which is in operation 24/7.
2. In case of a more serious health concern (difficulty breathing), call the emergency number **112**. Do not go to the emergency department for help, as you might transmit the virus to other people at the department.
3. When waiting for coronavirus test results or if the test came back positive, stay at hotel room/rental apartment to prevent the spread of the virus. If a case is identified, the infected individual will be put in isolation. The Health Board will reach out to those who were possibly in close contact with an affected individual and advise them to limit their social engagements.
4. **Self-isolation is mandatory for everyone showing symptoms of an infectious disease.**
5. **Please note that NATO CCDCOE´s training facilities (EDF / EST MOD territory) is not suitable for self-isolation.**

Accommodation

There are four hotels which we recommend for the course and workshop participants. Students will receive the fixed 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 closest hotel to training venue (CR14 building) is **Hestia Hotel Kentmanni** which is located only 350 meters away. Short overview of the hotel:

Hestia Hotel Kentmanni (address Kentmanni 13, 10116 Tallinn, Estonia) is a 4 hotel located at an exclusive central street lined by chic city homes, boutiques, restaurants and the embassy of the United States of America. The hotel offers a luxurious and quiet environment in the center. Hotel is loved by business travelers, couples and families. The small and private spa is open to our guests only. This oasis of peace and quiet allows guests to relax in heated reclining chairs, a jacuzzi, steam or Finnish sauna, or to simply rest in front of the fireplace after a long flight or a busy workday.*

Spa access included on room prices.

Location:

Distance from the Old Town – 0.7 km

Distance from the port – 4.3 km

Distance from the airport – 3.7 km

The second hotel which we recommend for the course and workshop participants is **'Original Sokos Hotel Viru'**, which is located also in the very centre of Tallinn within a few minutes' walk of the old town and about 700 meters away from the training venue (CR14 building).

Short overview of the hotel:

In Tallinn, Viru has always been the vibrant city hotel where history meets the present. Time has made it unique and genuine. Our relaxed and friendly service makes our guests return over and over again. Here, you get something you cannot find elsewhere. In the middle of everything and everyone. A wide range of different rooms, restaurants, entertainment and recreation services, a conference and banquet centre, a shopping centre and an interesting KGB Museum – all under one roof.

At Original Sokos Hotel Viru, we give you the best tips from locals to make your visit memorable. Your important moments at Viru will continue to live in your heart and ours.

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.

Getting to the Hotel

Lennart Meri Tallinn Airport is located just 4 km from the city centre, so transport to the city centre takes surprisingly little time. By car, Tallinn Airport is just 10 minutes away.

Transportation costs are not covered by the NATO CCDCOE.

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

By tram: Tram no 4 from the airport to the city centre operates a frequent schedule, the tram stop is located next to the airport terminal towards the city. Single journey tickets can be bought in cash from the driver for €2. The closest stops to the Original Sokos Hotel Viru/ CR14 training venue are the Hobujaama or Viru stops.

More detailed information in this link.

Administration fee

The course participants are not allowed to leave the course venue during the course due to the COVID-19 pandemic risks. During the course day, coffee breaks and lunch will be provided for the participants (see the details below). All of the COVID-19 related countermeasures costs and coffee /lunch breaks related costs will be included in the **mandatory 130 € Administration fee. Invoice will be sent out via email together with the course confirmation.**

Coffee breaks

Coffee breaks are organised by the NATO CCDCOE during the course week. The cost of the coffee breaks are included in the Administration fee. Coffee breaks include coffee, tea, water and snacks.

Lunch breaks

Based on the guidelines provided above, the course participants are not allowed to leave the course venue during the course due to the COVID-19 pandemic risks. The cost of the lunch breaks are included in the Administration fee.

Lunch possibilities in the close neighbourhood

When the COVID-19 pandemic risks indicated governmental restrictions are not applied, the following lunch possibilities can be considered:

There are several lunch possibilities in the close neighbourhood of the training venue. Only 100 meters away is Solaris Centre which has 14 great places to eat for every taste – japanese, asian, italian, european cuisines and the largest selection of vegan food in the city. Also fresh baked goods and delicious desserts.

Vapiano - Vapiano's menu is based on simple, authentic Italian cuisine:pizza, pasta and salads, plus antipasti and dolci (sweets). Freshness and quality of ingredients is at the centre of attention.

LIDO - LIDO is part of a Latvian restaurant chain. LIDO's dishes are served straight from the oven based on our own special recipes, which do not have any preservatives in them!

TOKUMARU - the first authentic Japanese restaurant in Estonia!

CHI ASIAN FOOD - the menu at Restaurant CHI is based on Thai, Chinese and Indian cuisine. We have a great and rich menu with many choices of fish, meat and vegetable dishes.

Also café Komeet, bakery GUSTAV, Blender, Boost, Hesburger, café Reval.

Dress code

There is no strict dress code: smart casual and uniform are accepted.

General course schedule

Day 1 - Day 4 (Monday – Thursday)

9:00 1st Session

10:30 Break

10:45 2nd Session

12:15 Lunch Break

13:30 3rd Session

15:15 Break

15:30 4th Session

17:00 End of course day

(Remark: an overview of the NATO CCDCOE is given on the first day)

Day 5 (Friday)

9:00 1st Session

10:30 Break

10:45 2nd Session

12:15 Lunch Break

13:30 3rd Session

15:15 End of day 5

General Information

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 events@ccdcoe.org

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 NATO CCDCOE is staffed and financed by 29 member nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Australia, Canada, Ireland, Japan, Luxembourg, the Republic of Korea, Ukraine and others have expressed interest in joining the Centre.

CCDCOE Flagships

Locked Shields is a unique international cyber defence exercise organised by CCDCOE since 2010 offering the biggest and most complex technical live-fire challenge in the world. This annual exercise enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects.

More than 1200 cyber experts from nearly 30 nations took part in Locked Shields in 2019 (video of the Locked Shields 2019 execution on NATO CCDCOE YouTube channel). In addition CCDCOE organises a technical red teaming cyber defence exercise Crossed Swords annually with the aim of training penetration testers, digital forensics professionals, situational awareness experts filling the role of the attacking team at Locked Shields. In 2021 and 2022, all exercises are planned to be delivered with partially an option for participants and organisers to take part or contribute remotely.

CyCon, the annual International Conference on Cyber Conflict, is the annual meeting place for the transatlantic cyber security community. The conference, taking place in Tallinn since 2009, attracts every spring more than 600 participants. In 2021, the first virtual CyCon drew over 800 viewers. 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 published in the conference proceedings. Conference recordings can be found on the Centre's YouTube channel. 14th International Conference on Cyber Conflict (CyCon 2022) will be held from 31 May through 3 June 2022 in Tallinn, Estonia. CyCon 2022's central theme is Keep Moving!

The Tallinn Manual 2.0 is the most comprehensive guide for policy advisors and legal experts on how International Law applies to cyber operations carried out between and against states and state actors. An invaluable analysis by an international group of renowned scholars, published in 2017, that serves to inspire both academic research and state practice. The Tallinn Manual process is continuing with a legal, technical, strategic and operational assessment of cyber scenarios. The Tallinn Manual 3.0 was launched in 2021 and the CCDCOE invites experts around the world to contribute to the revision of this globally influential resource for legal and policy advisors dealing with cyber issues.

Full Spectrum Cyber Security Training

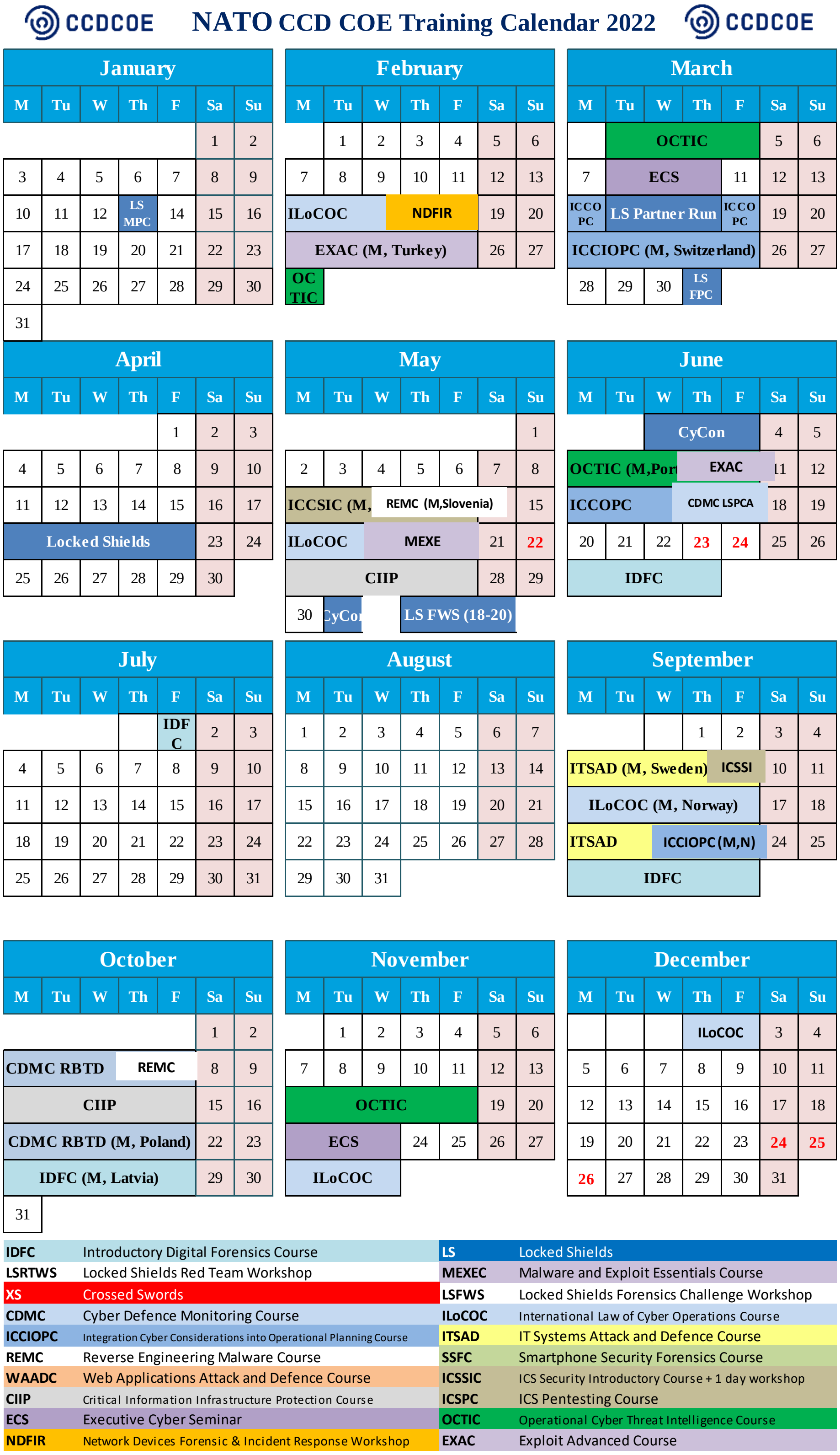
NATO CCDCOE promotes continuous learning in cyber security. Our training courses are based on the latest research and cyber defence exercises. NATO CCDCOE is committed to improving our training offerings to address the changing needs of the ever-developing cyber security field.

As of January 2018, CNATO CDCOE is responsible for identifying and coordinating education and training solutions in cyber defence for all NATO bodies across the Alliance. NATO Allied Command Transformation has provided NATO CCDCOE with an unconditional quality assurance accreditation for its contribution to high-quality NATO Education and Training.

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. NATO CCDCOE Training Calendar



CCDCOE NATO CCD COE Training Calendar 2022 CCDCOE

January

M	Tu	W	Th	F	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	LS MPC	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

February

M	Tu	W	Th	F	Sa	Su
	1	2	3	4	5	6
7	8	9	10	11	12	13
ILoCOC		NDFIR			19	20
EXAC (M, Turkey)					26	27
OC TIC						

March

M	Tu	W	Th	F	Sa	Su
	OCTIC				5	6
7	ECS			11	12	13
ICCO PC	LS Partner Run			ICCO PC	19	20
ICCIOPC (M, Switzerland)					26	27
28	29	30	LS FPC			

April

M	Tu	W	Th	F	Sa	Su
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
Locked Shields					23	24
25	26	27	28	29	30	

May

M	Tu	W	Th	F	Sa	Su
						1
2	3	4	5	6	7	8
ICCSIC (M,		REMC (M,Slovenia)				15
ILoCOC		MEXE			21	22
CIIP					28	29
30	CyCo		LS FWS (18-20)			

June

M	Tu	W	Th	F	Sa	Su
		CyCon			4	5
OCTIC (M,Por		EXAC			11	12
ICCOPC		CDMC LSPCA			18	19
20	21	22	23	24	25	26
IDFC						

July

M	Tu	W	Th	F	Sa	Su
				IDF C	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

August

M	Tu	W	Th	F	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

September

M	Tu	W	Th	F	Sa	Su
			1	2	3	4
ITSAD (M, Sweden)			ICSSI		10	11
ILoCOC (M, Norway)					17	18
ITSAD		ICCIOPC (M,N)			24	25
IDFC						

October

M	Tu	W	Th	F	Sa	Su
					1	2
CDMC RBTD		REMC			8	9
CIIP					15	16
CDMC RBTD (M, Poland)					22	23
IDFC (M, Latvia)					29	30
31						

November

M	Tu	W	Th	F	Sa	Su
	1	2	3	4	5	6
7	8	9	10	11	12	13
OCTIC					19	20
ECS			24	25	26	27
ILoCOC						

December

M	Tu	W	Th	F	Sa	Su
			ILoCOC		3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

IDFC	Introductory Digital Forensics Course	LS	Locked Shields
LSRTWS	Locked Shields Red Team Workshop	MEXEC	Malware and Exploit Essentials Course
XS	Crossed Swords	LSFWS	Locked Shields Forensics Challenge Workshop
CDMC	Cyber Defence Monitoring Course	ILoCOC	International Law of Cyber Operations Course
ICCIOPC	Integration Cyber Considerations into Operational Planning Course	ITSAD	IT Systems Attack and Defence Course
REMC	Reverse Engineering Malware Course	SSFC	Smartphone Security Forensics Course
WAADC	Web Applications Attack and Defence Course	ICSSIC	ICS Security Introductory Course + 1 day workshop
CIIP	Critical Information Infrastructure Protection Course	ICSPC	ICS Pentesting Course
ECS	Executive Cyber Seminar	OCTIC	Operational Cyber Threat Intelligence Course
NDFIR	Network Devices Forensic & Incident Response Workshop	EXAC	Exploit Advanced Course

Annex B. Official Education & Training Contacts

Nation/Organization	Name	E-mail address
Austria	Peter Schlossern	peter.schlossern@bmlv.gv.at
Belgium	Nicole Wouters	ACOSIS-CYBER-STAFF-ET@mil.be
Canada	Candace Smigelski	Candace.Smigelski@forces.gc.ca
Cyprus	Captain Evangelos Englezakis	cyberdefenceoffice@mod.gov.cy
Czech Republic	Michael Tomáš	M.Tomas@nukib.cz
Croatia	Damir Sacher	damir.sacher@morh.hr
Denmark	Niels Poul Petersen	NPP@FMN.DK
Estonia	LTC Tamás Nagy	tamas.nagy@ccdcoe.org
Finland	Major Markus Riihonen	markus.riihonen@mil.fi
France	Mr Ronan RIOU	ronan.riou@def.gouv.fr
Germany	Dr. Christina Cerny	ChristinaCerny@bundeswehr.org
Greece	Nikolaos Stamatelatos	n.stamatelatos@hndgs.mil.gr
Hungary	LTC Tamás Nagy	tamas.nagy@ccdcoe.org
Italy	CWO Nicola DAMIAN (ITA AF) OR-9	primo.form2s@smd.difesa.it
Latvia	Mr. Gatis Mezītis	gatis.mezitis@mod.gov.lv
	Mr. Edgars Kuikucans	edgars.kuikucans@mod.gov.lv
Lithuania	NCSC/CERT-LT	info@nksc.lt
Luxembourg	Armée luxembourgeoise - Bureau Formation	Bureau.Formation@armee.etat.lu
Netherlands	Cyber Trainings Center	cwtc.cyber.opleidingen@mindef.nl
Norway	Ingrid Winther	Ingrid.Winther@ccdcoe.org
Poland	Marcin Janowski	m.janowski@ron.mil.pl
Portugal	LCDR Rui Costa	rmcosta@emgfa.pt
Romania	Ionut Olaru	ionut.olaru@cyberint.ro

Slovakia	Cyber Defence Center of the Slovak Republic	training-svk@mosr.sk
Slovenia	LTC Samo Flisek	samo.flisek@mors.si
South Korea	SY Park	cooperation@ncsc.go.kr
Spain	LTC Tamás Nagy	tamas.nagy@ccdcoe.org
Sweden	Jan Axel Gotthard Wünsche	Jan.Wunsche@ccdcoe.org
Switzerland	Eglin Maurice GS-VBS	Maurice.Eglin@gs-vbs.admin.ch
Turkey	Maj Emre HALISDEMIR	emre.halisdemir@ccdcoe.org
United Kingdom	Lt Cdr Deborah Wiseman	Deborah.Wiseman671@mod.gov.uk
United States	Mr. Charles Hansis	charlesjames.m.hansis.civ@mail.mil
NATO Command Structure	Nikolaos FOUGIAS	Nikolaos.FOUGIAS@shape.nato.int