

# Counter Improvised Explosive Devices

Centre of Excellence

## Events and Courses Catalog 2024





# INDEX

Preface ..... 3

C-IED COE Organization..... 4

Milestones..... 5

Our Vision and Mission..... 6

Some Key Points about C-IED ..... 7

Principles of C-IED..... 8

Main Events..... 9

Lessons Learned Workshop (**LLWS**)..... 10

Inter-Agency Workshop (**IAWS**)..... 11

Technology Workshop (**TECH WS**)..... 12

Education and Training Activities..... 13

C-IED Awareness Course (**CIAC**) ..... 14

C-IED Staff Officers Course (**CSOC**) ..... 15

Basic Field Exploitation Course (**BIFEC**) ..... 16

Weapons Intelligence Team Course (**WIT**) ..... 17

Weapons Intelligence Team Training Developer Course (**WIT TDC**)..... 18

Attack the Network Operational Course (**ATNOC**) ..... 19

Analyst’s Notebook Users Course (**ANUC**)..... 20

DOMEX Awareness Course (**DOMEX**) ..... 21

C-IED COE courses planned for 2024..... 22

Contact ..... 25



# Preface

The term Improvised Explosive Threat is used by the international community to identify a device placed or fabricated in an improvised manner to cause destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military ordnance but is normally devised from nonmilitary components. In most cases these explosive devices are used simultaneously by criminal or adversary actors. One of the most common is the Improvised Explosives Device (IED), whose use origins can be traced back centuries. During recent conflicts and in areas where violent extremist organizations operate the use of improvised explosive devices emerge as one of the most effective enemy weapons.

The IED is a weapon that threatens the security of not only of NATO forces, but the safety and wellbeing of civilian populations within conflict areas and in our homeland. The IED is a faceless weapon that can have significant strategic, political, operational, and tactical effects. State Actors and Threat Networks use IEDs because they are cost effective, easy to construct, composed of readily available dual use components, and are highly effective.

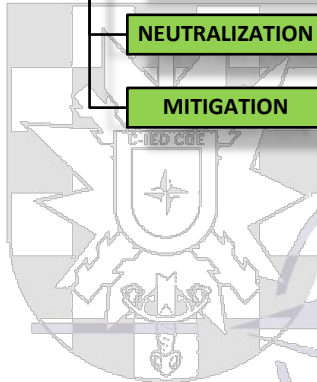
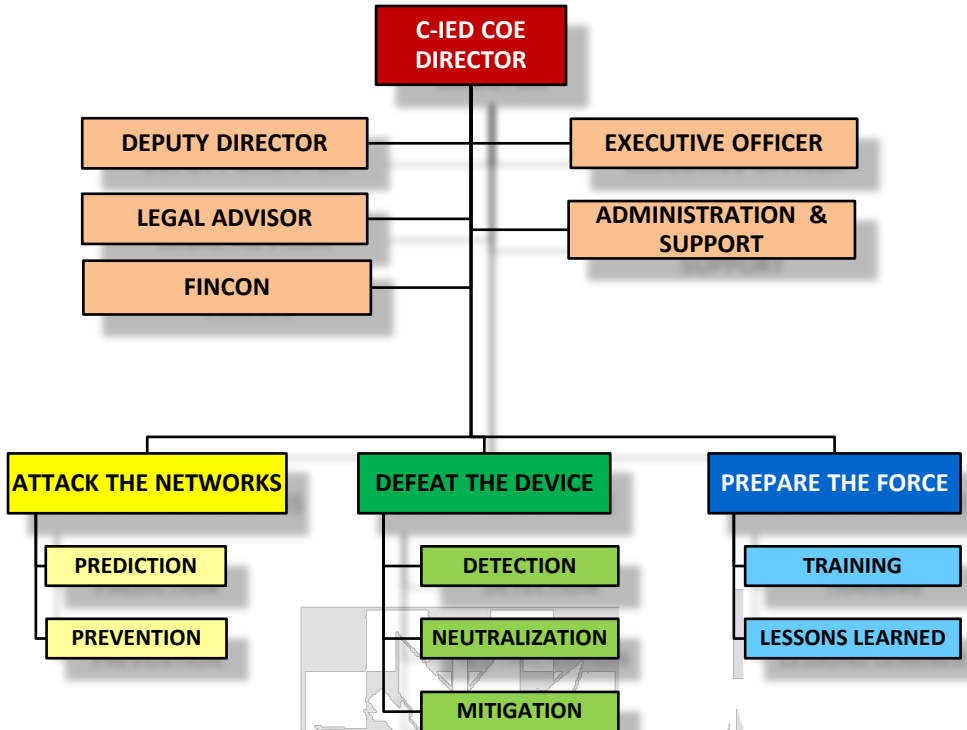
The use of IEDs and other improvised explosive threats by adversaries will continue to aid in global instability and have dramatic effects on the strategic environment for years to come. The fight to counter improvised explosive threats and the Threat Networks that employ them demand an increase in technical exploitation of evidence to end the cycle.

The Counter-IED Centre of Excellence (C-IED COE) is positioned to be the preeminent source of innovative expertise on all multinational aspects of the fight against IEDs and improvised explosive threats in support of the sponsoring nations; by becoming NATO's expert and focal point for C-IED; including related Technical Exploitation skills, education, and training for NATO and other Allies.

In its role as NATO's Department Head for C-IED Education and Training (E&T), the C-IED COE supports NATO Allied Command Transformation by defining the C-IED E&T requirements, developing and accrediting NATO C-IED related courses, and delivering specific C-IED courses to achieve a better trained and more globally connected C-IED community to combat the threat.



# C-IED COE Organization





# Milestones

In September 2007, the Spanish Minister of Defense announced the decision put forth an offer to host a NATO Counter Improvised Explosive Devices Centre of Excellence (C-IED COE), to serve as an international touchstone in the counter terrorism struggle.

The main intention was not only to contribute to the overall well-being of Alliance forces and civilians involved in operations, but also to the security of the allies and their homelands. Towards the end of 2007, the Spanish Chief of Defense, through the NATO's Allied Command Transformation, formally offered NATO a multinational Counter-IED COE. In 2008, Allied Transformation Command confirmed that Spain's concept to host a C-IED COE met with Allied principles and desires.

Prior to joining the community of NATO COEs, Allied Command Transformation certified that the C-IED COE concept, facilities, and level of readiness offered to Allies matched NATO standards. In June 2010, six countries signed the Memorandum of Understanding in Norfolk, Virginia. Furthermore, in June 2016, the C-IED COE earned a quality assurance unconditional accreditation and became an Educational and Training institution aligned with NATO quality assurance standards.

The Centre of Excellence is one of the main actors mentioned in the NATO C-IED Action Plan, which is "...aimed to reduce the strategic impact of IEDs..." in current and future conflicts by limiting their tactical and operational effects. It identifies actions required to be fulfilled by the Centre to focus on the high priorities and short to midterm requirements necessary for continuing effectiveness and success of the three pillars of C-IED; Defeat the Device, Attack the Networks, and Prepare the Force.



# Our Vision and Mission

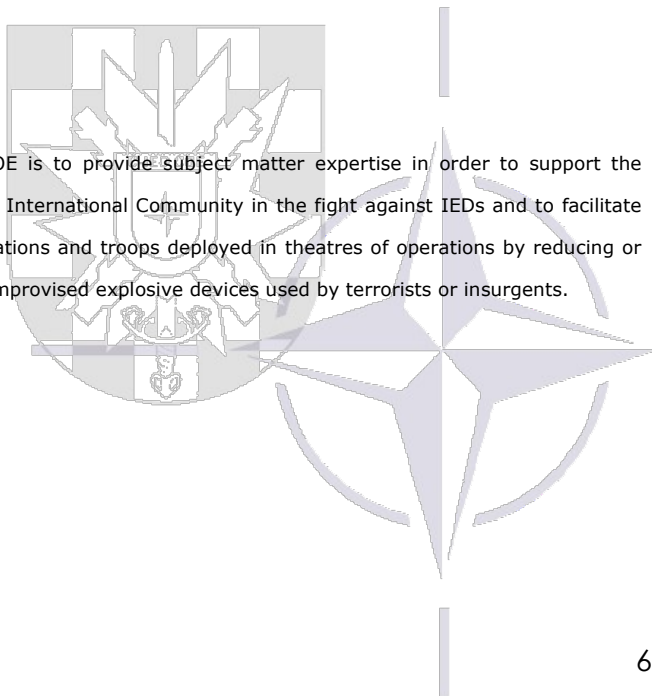
## Vision

The vision of the COE is to use a Comprehensive Approach to address challenges and threats, with the support of not only military personnel, but also with contributions from law enforcement, the intelligence community, academia, and the research & technology industry. The synergy of all these elements will contribute to the identification of terrorist / insurgent networks using IEDs, the IEDs themselves, and aid to counter other improvised explosive threats.

The C-IED COE is the natural venue for all C-IED issues in the NATO operational environment. The COE creates synergy in the C-IED community of interest by leading and participating in related working groups within NATO, the European Defense Agency, and other international organizations.

## Mission

The mission of the C-IED COE is to provide subject matter expertise in order to support the Alliance, its partners, and the International Community in the fight against IEDs and to facilitate increased security of Allied Nations and troops deployed in theatres of operations by reducing or eliminating the threats from improvised explosive devices used by terrorists or insurgents.





# Some Key Points About C-IED

Improvised explosive devices (IEDs) may be simple in design and easily made, or sophisticated, incorporating modern electronic components. IEDs are a sub-set of several forms of asymmetric physical attacks and enable adversaries to strike without being decisively engaged. IED proliferation has become so widespread that they have become a global threat in operational areas and at home. Through IED attacks, adversaries target our national willingness to participate in NATO operations and create fear among our civilian populations, making the IED a tactical weapon with potential strategic affects.

C-IED activities are principally against adversaries (namely people) and not only against the device itself. C-IED treats the IED as a systemic network-based problem and aims to defeat the IED system and the human network that employs them.

A successful C-IED approach requires wider understanding and support from all levels of government, especially those that direct, plan, and support operations. C-IED is required to support military activities across all operating domains and environments. It relies upon an integrated and comprehensive approach that is joint, inter-agency, and multinational. In domestic scenarios, C-IED involves local authorities, community leaders, and public awareness campaigns.

For the C-IED approach to be successful across all military activities, it must be embedded by knowledgeable C-IED specialists throughout the planning, preparation, and execution phases of operations.

C-IED is not focused on defensive activities to defeat the device or prepare the force. IED proliferation and innovative employment combined with IED's strategic impacts demand a more proactive and offensive approach to attack the threat network, as reflected in NATO doctrine.



# Principles of C-IED

**a. Unity of effort.** C-IED requires a comprehensive approach including joint, inter-agency, and multinational elements. The C-IED approach should be adopted by all friendly force elements from the onset of campaign planning. Mutual understanding, effective communication, and common doctrine and procedures are essential to the C-IED approach supporting unity of effort.

**b. Effective understanding and intelligence.** C-IED requires effective understanding and analysis of situations to ensure the development of appropriate measures. This must be informed by accurate, timely, predictive, and viable intelligence from the whole range of available sources. In joint, inter-agency and multinational environments, procedures must be established to ensure efficient information management and sharing. Effective exploitation feeds into intelligence, builds understanding and provides the means to deliver a proactive C-IED posture to defeat the IED system. The systematic exploitation of personnel, materiel, and documents directly supports operational intelligence through the development of specific targets and provides wider situational understanding. It also provides specialist technical intelligence (TECHINT) to support developing defensive measures and modifying friendly force TTP.

**c. Proactive posture.** The C-IED approach must have a proactive posture to gain advantage, sustain momentum and to keep or wrest the initiative to enable the freedom to operate. An entirely reactive posture concedes this to the adversary.

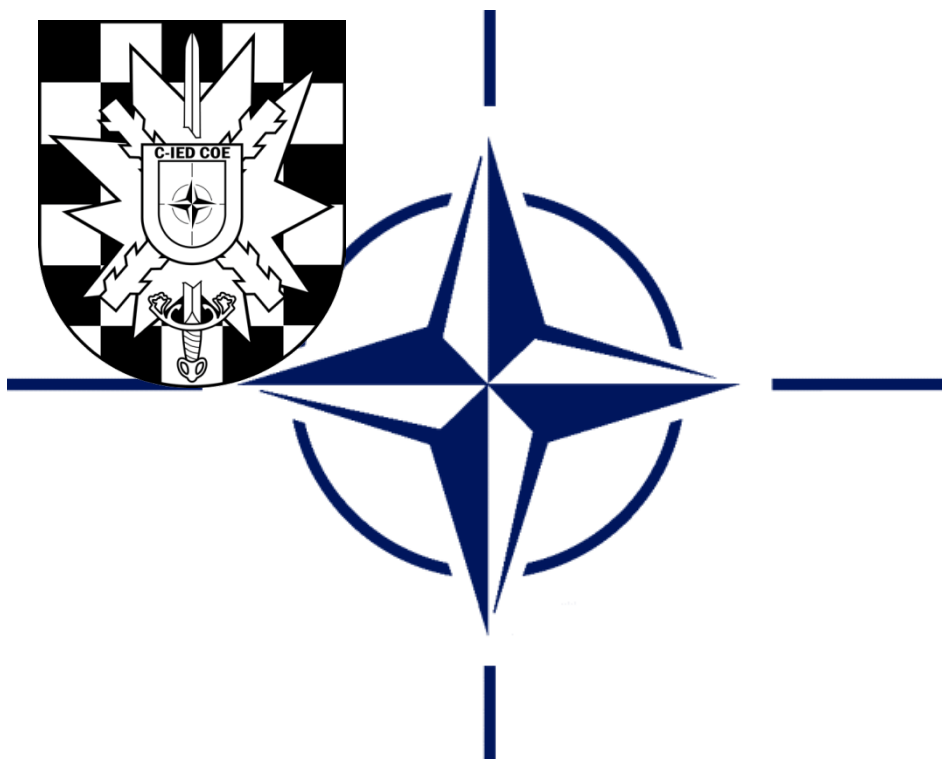
**d. Agility.** An effective force promotes learning and adapts more quickly than its adversary to ensure commanders can make timely decisions. In this context, the battle between the adversary and the Alliance represents an iterative action-reaction process; it is competitive learning. It embodies the ability to react to opportunities and to exploit Alliance successes and adversary failures. Agility also requires initiative at junior levels for the creation of new TTPs and modification of existing ones.

**e. Prioritization.** Priorities must be clear to commanders at all levels, especially for risk management and to effectively manage C-IED specialists who are a high demand, limited resource. There will be early opportunities to engage adversaries involved with the IEDs, but priorities may dictate the need to build the intelligence picture in preparation for larger offensive operations against the wider IED system.





# MAIN EVENTS





## Lessons Learned Workshop (LLWS)

### Aim

The aim of the LLWS is to contribute to the NATO Lessons Learned process and increase the knowledge of missions that different nations/agencies are conducting in areas with a high IED threat in order to facilitate and enhance interaction in the multinational C-IED community. The LLWS will be focused on several topics around LL in the C-IED area, like threat analysis from the theatre including LL from (technical) exploitation, cooperation amongst the COEs, and support to NATO DCB activities.

### Attendees

All military and Law Enforcement Community of Interest from: NATO organizations, NATO commands, nations, resolute support mission (RSM) contributing nations, EU and UN organizations, and Australia, Austria, Ireland, New Zealand, Sweden and Switzerland

### Content

The IED threat is a global challenge, with networks exceeding national borders. The LLWS is an appropriate opportunity for the community of interest (COI) to share and provide information for the benefit of our Alliance involved in international and/or national operations. The topics and objectives are various and can change at every LLWS.

### Remarks

The C-IED COE is designated as the NATO out of Theatre C-IED Lessons Learned Coordinator. Within this assignment the C-IED COE is supporting NATO commands, RSM contributing nations, EU/UN organizations, non-NATO Nations, and coalitions operating in IED environments. In coordination with the Joint Analysis and Lessons Learned Centre (JALLC), the C-IED Community of Interest (COI) was established on the NATO Lessons Learned Portal (NLLP), both on the NATO unclassified webpage and on NS-WAN. <https://nllp.jallc.nato.int/cmnt/Pages/Communities.aspx>

**Security Classification:** NATO UNCLASSIFIED or NATO SECRET CLASSIFIED. The security classification of the LLWS could change due to the content.



## CIED Inter Agency Workshop (IAWS)

### Aim

To bring together senior experts from the military, law enforcement, and other civilian agencies to discuss the multifaceted & comprehensive approach to countering threat networks, along with information sharing and networking.

### Attendees

National & multinational representatives from Military/Law Enforcement/Security Services.

### Content

It will cover different issues among several fields as they could be:

1. Threat update
2. Collection, processing, and analysis
3. Technical Exploitation/forensics
4. Targeting/engagement cycle
5. Countering Terrorism
6. Countering Financing
7. Countering Recruitment
8. Countering Influence/propaganda activities
9. Interoperability
10. Supportive technologies to Attack the Networks/Network Engagement Training tools

**Remarks:** Conducted in odd numbered years.

**Security Classification:** Up to NATO/EU Unclassified releasable to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



## CIED Technology Workshop (TECH WS)

### Aim

To bring together senior experts from the military, law enforcement, industry, and Academia to discuss research and development (R&D) initiatives plus recent technical advances regarding C-IED, along with information sharing and networking, including exposition and demos of different equipment.

### Attendees

National & multinational representatives from Military/Law Enforcement/Security Services, along with representatives from Academia and Industry.

### Content

It will cover different issues among several fields as they could be:

1. Threat update
2. Multinational & national initiatives in C-IED R&D
3. Technical Exploitation/forensics
4. Supportive technologies to Defeat the Device
5. Detection and Mitigation technologies
6. Last developments in support of C-IED enablers
7. Interoperability
8. Training advances
9. Counter Unmanned Aerial System (UAS)

**Remarks:** Conducted in even numbered years.

**Security Classification:** Up to NATO/EU Unclassified releasable to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



# EDUCATION & TRAINING ACTIVITIES





## C-IED Awareness Course (CIAC)

### Aim

To provide operational level HQ staff with an awareness of Counter IED strategies and supporting activities that may be integrated into existing operational planning and structures. The lectures and knowledge provided during this course are based on non-classified information from NATO documents and should be seen as references.

### Attendees

Staff Officers (OF-1 thru OF-5), Senior Non-Commissioned Officers (OR-7 and above) and civilian equivalent assigned at Operational Level Headquarters.

### Content

At the conclusion of the course, each student should be able to complete the following course objectives using the skills, techniques, and practical lessons learned during the course:

1. Interpret the threat from IEDs
2. Identify the IED link to patterns of behavior
3. Consider local sensitivities and culture
4. Comprehend current IED attack activities with the operational environment
5. Predict future IED activity
6. Identify emerging IED threats
7. Comprehend the NATO C-IED Strategy
8. Define the C-IED Activities
9. Align the Core C-IED Functions
10. Identify the C-IED related staff functions
11. Consider the HQ Organization requirements for C-IED
12. Relate to Staff processes
13. Outline military search capabilities
14. Outline Improvised Explosive Device Disposal (IEDD) capabilities
15. Outline C-IED exploitation capabilities
16. Outline local C-IED Influence Activities
17. Outline C-IED Electronic Warfare capabilities
18. Outline route clearance capabilities

### Remarks

1. 3–5 days course. The course will be **conducted based on external requests** (max 2 iterations a year). Up to 30 students.
2. Students should have language proficiency in English SLP 2323 in accordance with NATO STANAG 6001.

**Security Classification:** Not classified



# C-IED Staff Officers Course (CSOC)

**ETOC No.: IED-ED-23066**

## Aim

To provide C-IED Staff Officers and Senior Staff Assistants, at Upper Tactical and Operational levels, with the knowledge and skills to facilitate, manage and lead the C-IED effort, by drawing together and coordinating the expertise and efforts of the other staff branches, and become the Commanders' primary C-IED SME and operations advisor.

## Attendees

C-IED Staff Officers and senior Staff Assistants working in C-IED related positions within NATO or Australia, Austria, Ireland, New Zealand, Sweden and Switzerland. English Standard Language Proficiency according to STANAG 6001 – level 2 (SLP 3232).

## Content

At the conclusion of the course, each student should be able to complete the following course objectives using the skills, techniques, and practical lessons learned during the course:

1. Attendees will be able to define principles for organizing and conducting CIED activities in Operations.
2. Attendees will be able to describe the staff roles, responsibilities, and links related to an operational HQ's organization for CIED.
3. Attendees will be able to apply CIED principles, doctrine, concepts of operations, and HQ's responsibilities given a scenario-based problem.
4. Understand the Attack the Networks operations in C-IED operations. (Enable the exploitation cycle; contribute to the information and intelligence fusion, analysis and targeting process).
5. Attendees will be able to identify training gaps in relation to the operational requirements and contribute to the planning of C-IED training and provide C-IED related observations to the lessons learned process and act as a C-IED SME during the process.

## Remarks

1. It's mandatory to successfully complete the e-learning Advanced Distributed Learning (ADL) 207 C-IED course (<https://jadr.act.nato.int/>) to join the resident CSOC course phase,
2. 5-days course.
3. 3 iterations per year.
4. Up to 24 students per course.

**Security Classification:** NATO SECRET releasable to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



## Basic Field Exploitation Course (BIFEC)

### Aim

To provide an overview of the execution of C-IED field exploitation. This includes technical and forensic field exploitation of IED events in order to obtain immediate intelligence and to preserve evidence for further investigations and legal processes.

### Attendees

Approved NATO partners and non-NATO country members of governmental and non-governmental organizations. The ideal candidate for BIFEC comes from Explosive Ordnance Disposal, Engineers, Intelligence, Military Police, Law Enforcement, Special Operations, or Infantry backgrounds. The military rank of students attending the course normally ranges from NATO OR 6-8 to OF 1-3.

### Content

1. Contribute to the C-IED exploitation process
2. Conduct the WIT process
3. Draft and present appropriate C-IED level 1 exploitation reports
4. Produce a visual record of an IED event
5. Describe the adversary's tactics, techniques, and procedures (TTPs)
6. Assess the tactical use of IEDs in the IED events
7. Identify and describe the functioning of the different IED types
8. Describe the functioning of electrical and electronic components used to manufacture IEDs
9. Identify the different types of homemade explosives (HME) precursor components.
10. Describe the different types of commercial and military explosive charges
11. Identify the main types of military ordnance
12. Conduct fragmentation and crater analysis of an IED event

### Remarks

9 Days course. The course will be **conducted based on external request**. Max 2 iterations a year. Up to 12 students.

**Security Classification:** Not classified





# Weapons Intelligence Team Course (WIT)

**ETOC No.: IED-ED-3767**

## Aim

To provide essential Level 1 Exploitation Weapons Technical Intelligence (tactical level) training to teams able to respond to IED incidents – prior to their arrival in an Operational Theatre. Weapons Intelligence Teams will be trained to investigate IED incidents in any environment, and produce standardized tactical, technical, and forensic intelligence Level 1 reports that can feed the Operations and Intelligence cycle to more effectively understand and conduct Attack the Networks activities.

## Attendees

The course is open to NATO and Interoperability Platform Nations. English Standard Language Proficiency according to STANAG 6001 – level 2 (SLP 2323). The military rank of students attending the course normally ranges from NATO OR 6-8 to OF 1-3.

## Content

1. Contribute to the C-IED exploitation process
2. Conduct the WIT process
3. Draft and present appropriate C-IED level 1 exploitation reports
4. Produce a visual record of an IED event
5. Describe the adversary's tactics, techniques, and procedures (TTPs)
6. Assess the tactical use of IEDs in the IED events
7. Identify and describe the functioning of the different IED types
8. Describe the functioning of electrical and electronic components used to manufacture IEDs
9. Identify the different types of homemade explosives (HME) precursor components
10. Describe the different types of commercial and military explosive charges
11. Identify the main types of military ordnance
12. Conduct fragmentation and crater analysis of an IED event

## Remarks

1. A successful completed e-learning Advanced Learner (ADL) WIT- phase is mandatory to attend the 3 weeks WIT- Course resident phase
2. 2 iterations a year in Spain, Hungary, or Romania under C-IED COE direction. Up to 20 students each

**Security Classification:** NATO RESTRICTED rel. to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



# Weapons Intelligence Team Trainer Developer Course (WIT TDC)

## Aim

To improve the NATO Nations capability to train their own forces in Level 1 technical exploitation (including WIT), by educating trainers to design and conduct courses by increasing teaching skills and improving technical knowledge.

## Attendees

The course is open to attendees from across NATO nations and Australia, Austria, Ireland, New Zealand, Sweden and Switzerland. English Standard Language Proficiency according to STANAG 6001 – level 2 (SLP 2323). The military rank of students attending the course ranges from NATO OR 6-9 to OF 2-4.

## Content

1. Understanding of the technical exploitation capabilities and processes and their contribution in the C-IED circle
2. Conduct the WIT process
3. Understand how to design and develop Level 1 technical exploitation training

## Remarks

1. Students must be individually trained as follows: International or National level 1 technical exploitation
2. 5 day course (1 iterations per year)
3. Maximum of 24 students

**Security Classification:** NATO UNCLASSIFIED releasable to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



# Attack the Network Operational Course (AtNOC)

**ETOC No.: IED-ED-23069**

## Aim

To provide NATO Intelligence, Operations, Plans, Counter terrorism and C-IED Staff Officers and Senior Staff Assistants from upper tactical (LCC, MCC, ACC, SOCC) and operational level commands with the knowledge and skills to integrate the comprehensive AtN approach across the other HQ processes. Emphasis will concentrate on providing AtN related Situational Awareness, recommending ways to engage all networks and an assessment on the engagement effects. Attendees should have a background in Intelligence, Operations, Plans, Targeting, CT or C-IED.

## Attendees

The course is designed for staff personnel involved in C-IED AtN Staff Functions (Network Analysis and support to Targeting, Operations, Exploitation, ISR management, etc.) requiring a cross-functional approach. Therefore, the course is primarily aimed at Staff Officers (OF 2 to OF 4) and Senior Non-commissioned Officers (OR 8 to OR 9) directly supporting the abovementioned tasks. Bearing this in mind, other staff members are welcome as well. English Standard Language Proficiency according to STANAG 6001 SLP 3232.

## Content

The main characteristics of the course are:

1. It is focused on the execution and integration of AtN sub-processes.
2. The core of the course is based on a simulated practical exercise resolution.
3. The aim of the course is to provide Operational Level NATO HQ staff officers with an understanding of the framework to plan and conduct AtN operations in support of NATO missions including threat analysis.

Upon course completion, each student should meet the following course objectives using the skills, techniques, and practical lessons learned during the course:

1. Understand and demonstrate the purpose of the comprehensive approach to AtN.
2. Employ operational variables methods (PMESII, ASCOPE...) to develop Comprehensive Preparation of the Operational Environment (CPOE).
3. Understand and illustrate the structures, components, attributes, characteristics of overlapping networks.
4. Demonstrate how the C-IED pillar (Understanding & Intelligence) facilitates AtN and DtD.
5. Participate in the Joint Targeting Process to determine the desired effects necessary to achieve Commander's objectives.

## Remarks

1. 2 weeks course. 2 iterations per year
2. Maximum 24 students per iteration

**Security Classification:** NATO SECRET releasable to Australia, Austria, Ireland, New Zealand, Sweden and Switzerland



# Analyst's Notebook Users Course (ANUC)

## Aim

Training user course for IBM i2 Investigative Analysis Solution, providing students with the theoretical and practical assessment and knowledge of professional training for the "IBM i2 Analyst's Notebook®" software, teaching them on how to use this "data investigation and analysis" solution.

## Attendees

Military and Law Enforcement members involved in network analysis processes in their respective Headquarters, Agencies and Organizations. English Standard Language Proficiency according to STANAG 6001 – level 2 (SLP 2323).

## Content

1. Introduction to visual investigative analysis
2. Chart creation - basic information
3. Advanced features of Analyst's Notebook®
4. Working techniques for large volumes of information
5. Introduction and formatting of text files, Excel worksheets
6. Importing data files to create links Charts
7. Import exercises - various types of analysis
8. Analyst's Notebook® analysis functionalities
9. More import exercises
10. Introduction to Analyst's Notebook® timeline charts
11. Automatic generation of timeline charts
12. More exercises on timeline charts
13. Chart designs
14. Conditional formatting
15. Filters and histograms
16. Social Network Analysis – SNA (centralities)
17. Mapping with Google Earth (valid for other GIS)
18. Customizing the Analyst's Notebook®
19. Creation of entities, links, templates, etc.
20. Explanation of and practice C-IED add-on

## Remarks

5-days course. 3 iterations a year.

**Security Classification:** Not classified



# Document, Media, and Cellular Phone Exploitation (DOMEX)

**ETOC No.: IED-ED-35665**

## Aim

To enhance Technical Exploitation capabilities to level 1 (collection) enablers, focused in DOMEX discipline including Document Exploitation (DOCEX), Media Exploitation (MEDEX) and Cellular Phone Exploitation (CELLEX). The framework will be initial collection capabilities and the use of elementary tools and software to extract information at the tactical level for integration into the Technical Exploitation system (level 2).

## Attendees

Participants: NATO countries plus Australia, Austria, Ireland, New Zealand, Sweden and Switzerland and EDA pMS (participant Member States) 20-24 pax, and up to 8 instructors. (Contribution of external specialized experts is utilized)

Candidates to the course should be junior officers (2nd lieutenant – captain, OF-1 / OF-2), non-commissioned officers (staff sergeant to master sergeant, OR-6 to OR-9), law enforcement staff or other specialists who are working in the C-IED arena, Military Police or INTEL areas, or any WIT operator.

English Standard Language Proficiency according to STANAG 6001 – level 2 (SLP 2323).

Candidates must have basic working knowledge in Standard Automated Data Processing (ADP) and Communication and Information Systems (CIS).

## Content

Attendees should:

1. Acquire the basis to improve exploitation capabilities to concerned personnel in the DOMEX area, preparing them tactically and technically.
2. Be prepared to extract as much quality information as possible -using specific procedures, software and hardware- from mobile phones computers, and other digital devices.
3. Produce valuable basic Intelligence, ready to be transferred to the upper level in a proper and timely manner.
4. Understand DOMEX activities, procedures, organizations, products, and concerned databases and tools.
5. Understand the value of DOMEX to generate actionable intelligence.
6. Broaden up the existing acquired knowledge, and to practice DOMEX actions.

## Remarks

5-days course. 2 iterations a year

**Security Classification:** Not classified



## C-IED COE courses and events planned for 2024

***This is the C-IED COE planning for 2024 regarding courses approved by the Steering Committee on 25 October 2023. Below dates may change due to unforeseen reasons. No rights can be inferred according to this schedule.***

JAN	29	FEB	02	ESP	Analyst Notebook Users Course (ANUC) 24.1	15 seats available Military, Law Enforcement members & civilian analysts	5 days course Not classified No Fee
FEB	26	MAR	01	ESP	C-IED STAFF OFFICER COURSE (CSOC) 24.1	24 seats available C-IED Staff Officers and senior Staff Assistants	5 days course <b>NATO Approved</b> No Fee
MAR	04	MAR	15	ESP	AtN Operational Course (ATNOC) 24.1	24 seats available C-IED Staff Officers and Senior Staff Assistants	10 days course <b>NATO Approved</b> No Fee
MAR	12	MAR	13	ESP	Annual discipline conference		
APR	08	APR	19	ESP	DOMEX-course 24.1	12 seats available Open to military	10 days course <b>NATO Listed</b> No Fee
MAY	14	MAY	31	ROU	NATO Weapons Intelligence Team Course (WIT) 24.1	20 seats available OF 1-3 and OR 4-8 and	13 days course <b>NATO Approved</b> 125€ (for non-VNCF) (TBC)
MAY	28	MAY	30	ESP	Technology WS		
JUN	17	JUN	21	ESP	C-IED STAFF OFFICER COURSE (CSOC) 24.2	24 seats available C-IED Staff Officers and senior Staff Assistants	5 days course <b>NATO Approved</b> No Fee
JUN	24	JUN	28	ESP	Analyst Notebook Users Course (ANUC) 24.2	15 seats available Military, Law Enforcement members & civilian analysts	5 days course Not classified No Fee
JUN	25	JUN	27	ESP	LLWS		



SEP	10	SEP	27	HUN	NATO Weapons Intelligence Team Course (WIT) 24.2	20 seats available OF 1-3 and OR 4-8 and	13 days course <b>NATO Approved</b> 125€ (for non-VNCF) (TBC)
SEP	30	OCT	11	HUN	DOMEX-course 24.2	12 seats available Open to military	10 days course <b>NATO Listed</b> No Fee
OCT	21	OCT	25	ESP	C-IED STAFF OFFICER COURSE (CSOC) 24.3	24 seats available C-IED Staff Officers and senior Staff Assistants	5 days course <b>NATO Approved</b> No Fee
NOV	04	NOV	08	ESP	Analyst Notebook Users Course (ANUC) 24.3	15 seats available Military, Law Enforcement members & civilian analysts	5 days course Not classified No Fee
NOV	18	NOV	29	ESP	AtN Operational Course (ATNOC) 24.2.	24 seats available C-IED Staff Officers and Senior Staff Assistants.	10 days course <b>NATO Approved</b> No Fee
DEC	09	DEC	13	ESP	NATO Weapons Intelligence Team Training Developer Course (WIT TDC)	12 seats available C-IED Staff Officers and senior Staff Assistants.	5 days course



## Disclaimer

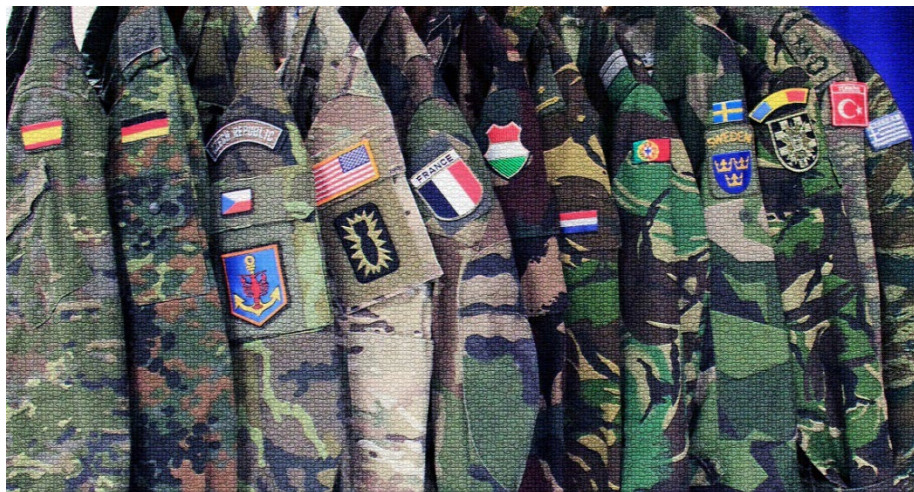
This publication is a product of the NATO C-IED Centre of Excellence. It does not necessarily reflect the policy or the opinion of NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for nonprofit and non-commercial purpose, provided that copies bear a full citation.

Unless identified, the photographs and sketches shown in this document are the sole property of the C-IED COE and the presentation copyrights owners have authorized its publication.

Designed by Sgt. Ropero C-IED COE Graphic and Photographic Section.





**For more information on C-IED COE contact:**

Email: [info@ciedcoe.org](mailto:info@ciedcoe.org)  
Phone: 0034 91 856 10 48  
Fax: 0034 91 856 23 90  
Web: [www.ciedcoe.org](http://www.ciedcoe.org)

**Address:**

Crta. M-618 Colmenar Viejo - Torrelodones km. 14  
28240, Hoyo de Manzanares  
Madrid, Spain