



2023
21-23
MARCH

Cyber Range **- Cybersecurity** **in practice**



www.cstcoe.mil.pl



EUROPEAN SECURITY AND DEFENCE COLLEGE

And

CYBER SECURITY TRAINING CENTRE OF EXCELLENCE, WARSAW, POLAND

(Eksperckie Centrum Szkolenia Cyberbezpieczeństwa)

Invitation to the course:

“Cyber Range – Cybersecurity in Practice”

(Activity number 22-23/215/1 PILOT)

21 – 23 March 2023

The Cyber Security Training Centre of Excellence (CST CoE) under the auspices of the European Security and Defence College (ESDC) is organising a **residential course, specialized at tactical-technical levels, from 21 to 23 March 2023 in Warsaw, Poland**. The course is linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade¹,

Cyber threats affect all areas and business domains where processes are supported by information and communication technologies (ICT). IT vulnerabilities pose a real threat to organizations and might result in real losses. Unauthorised access to IT resources, information leakage, service disruption, ransom requests are issues that cybersecurity teams face every day.


In response to these circumstances, the European Union has been actively working on creating adequate, flexible and coherent cybersecurity environment, which covers not only political and legal frameworks, but also capabilities development including education and training programmes. Within the subject area, the collective efforts of Cyber Security Training Centre of Excellence (Eksperckie Centrum Szkolenia Cyberbezpieczeństwa - ECSC, Warsaw, Poland) and the European Security and Defence College have led to the launch a Cybersecurity in Practice course. The course is now offered to the EU community as a part of ESDC's Cyber Education Training Exercise and Evaluation (ETEE) platform.


The overall goal of this course is to improve participants' knowledge as well as practical skills in increasing the security of IT infrastructure they are responsible for. Following scenarios, students will learn to conduct some penetration testing to identify potential vulnerabilities and weaknesses in order to eventually gain direct access to target resources. Thus, they will learn about the available cybersecurity tools and how they can be used in three different scenarios operating within the Cyber Range environment. The scenarios will present and enable testing of virtual machines and networks in Reconnaissance, Exploitation, Wifi - Hacking, Web Pentesting.

The course will be held in English and will consist of both lectures and practical exercises.

The course will be run on the Cyber Range, a training platform which delivers unique opportunities for reflecting IT infrastructure and enacting complex scenarios including conducting cyber-attacks in dedicated virtual environment. The Cyber Range environment enables to raise awareness, acquire knowledge and experience related to cyberspace and possible threats therein.

Participants should be technical personnel (mid-ranking officials, engineers and technicians) from the Member States and the EU Institutions Bodies and Agencies dealing with technical aspects of cybersecurity. An additional advantage will be the basic knowledge of the principles of network operation and Linux systems (distributions) at the basic level.

Paweł DZIUBA

Director of CST CoE

Holger OSTERRIEDER

Head of the ESDC

Annexes

1. Course administrative instructions
2. Programme
3. Venue « Cyber Security Training Centre of Excellence, Warsaw”
4. Additional personal information required to enter military facility

¹ Shaping Europe's future, <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>



Annex 1

Course administrative instructions

The course is suitable to technical personnel (mid-ranking officials, engineers and technicians) dealing with cybersecurity. It will be held in English and can accommodate up to 12 participants (civilian and military) staff from EU Member States, relevant EU institutions and agencies. Due to the technical nature of this course it is recommended that attendees were familiar with Linux operating system including usage of terminal tool and basic network configuration aspects.

Applications from the EU Member States and institutions are to be filled out by the national ENLIST nominators via the ESDC secure registration system via the following link <https://esdc.europa.eu/enlist/login>, **no later than 10th February 2023**.

A list of relevant ENLIST nominators can be retrieved from the ESDC website at <https://esdc.europa.eu/nominators/>.

The course will consist of two mandatory parts. **Online part** (asynchronous) will be delivered through ESDC's e-learning platform while **live part** (*residential*), containing lectures and exercises in lab environment, is to be held at Cyber Security Training Centre of Excellence facilities in Warsaw.

The e-learning part will be available for those who will be selected as of 17th February 2023.

The particular cases covered during the lectures will be further modelled and simulated within Cyber Range environment where respective scenarios will be executed and examined by course participants. The results will be later assessed and discussed within course attendees.

All international travel, transportation, accommodation costs during the course are to be covered by the sending authorities. It is recommended that participants arrive at Warsaw Airport on Monday, March 20, 2023. Participants should arrange their own travel and accommodation. We suggest choosing the Polonia Palace Hotel, from which the training organizer provides a shuttle transport to the course venue. Reservations should be made by February 23, using the http link sent by the course organizer. No-cost cancellation will be possible up to 7 days before arrival. Further information will be sent to participants after registration.

The dress code is business attire for both civilians and military personnel.

The format of the course is residential in Warsaw. However, given the unpredictable nature of the COVID-19 pandemic and possible changes to restrictions imposed on public events and international travel in the upcoming months, the organisation of the course in a face to face format might not be possible. In that case, the course will be canceled. Please do not book flights and accommodation before receiving the confirmatory message.

Supporting services:

- All administrative information, programmes and material will be made available to accepted participants through the ESDC's e-learning platform (ILIAS LMS).

Course points of contact

PoC at the European Security and Defence College:

Mr. **Giuseppe ZUFFANTI**,
Training Manager (Cyber) ESDC
Tel: +32 2 584 42 49, mobile: +32 460 84 42 49
E-mail: giuseppe.zuffanti@eeas.europa.eu

PoC at the Cyber Security Training Centre of Excellence, Warsaw, Poland:

Col AF Michal **MAJEWSKI**
Tel: +48 261 837 996
E-mail: michal.majewski@ron.mil.pl

Ms Joanna **ARCHACKA-STACHURA**
Tel: +48 571 221 051
E-mail: j.archacka-stachura@ron.mil.pl



European Security and Defence College (ESDC)

“Cyber Range – Cybersecurity in Practice”

(22-23/215/1 PILOT)

PROGRAMME

21 March – 23 March 2023 – Residential form

Cyber Security Training Centre of Excellence (CSTCoE)

Warsaw, Poland

(Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, Warszawa, Polska)

Course Venue:

ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

Director of CST CoE

Mr. Paweł DZIUBA

Course Director

COL AF Michał Majewski



DAY 1	Tuesday, 21 March 2023 (CEST)
09:00 – 09:20	<u>Registration</u> <u>Welcome coffee</u>
09:20 – 09:40	Welcome address and course opening: <ul style="list-style-type: none"> • Cyber Security Training Centre of Excellence (CSTCoE), Warsaw • European Security and Defence College (ESDC) and the Cyber Education, Training, Evaluation and Exercise (ETEE) Platform, Brussels
09:40 – 11:15	<p style="text-align: center;">SESSION 1 – Hands-on classes in Cyber Range environment: Introduction to penetration testing tools. Practical & initial penetration test.</p> <p style="text-align: center;"><i>Scenario 1</i></p> <p style="text-align: center;"><i>Keywords: Enumeration</i></p>
11:15 – 11:30	<u>Coffee break</u>
11:30 – 12:45	<p style="text-align: center;">SESSION 2 – Hands-on classes in Cyber Range environment: Exercise – Exploitation & Post Exploitation environment.</p> <p style="text-align: center;"><i>Scenario 1</i></p> <p style="text-align: center;"><i>Keywords: Kali Linux (Metasploit, MSFVenom, SEToolkit)</i></p>
12:45 – 13:30	<p style="text-align: center;">SESSION 3 – Hands-on classes in Cyber Range environment: Exercise – Phishing & Password Cracking.</p> <p style="text-align: center;"><i>Scenario 1</i></p> <p style="text-align: center;"><i>Keywords: SEToolkit, John the Ripper</i></p>
13:30 – 13.45	Wrap-up and closing remarks
13:45 – 15:15	Group photo & Lunch Break
15:15 – 19:00	<u>Transportation to the hotel & Guided Tour</u> (Warsaw & History of Poland)
19:30 -21:00	<u>Icebreaker Dinner</u>



DAY 2	Wednesday, 22 March 2023 (CEST)
09:00 – 09:30	<u>Welcome coffee</u>
09:30 – 11:00	SESSION 4 - Hands-on classes in Cyber Range environment: Network architectures in the context of web application security. <i>Scenario 2</i> <i>Keywords: Network Infrastructure, Web Servers, Reconnaissance, Enumeration.</i>
11:00 – 11:15	<u>Coffee break</u>
11:15 – 12:30	SESSION 5 - Hands-on classes in Cyber Range environment: Different types of vulnerabilities in web technologies. <i>Scenario 2</i> <i>Keywords: Web technologies, Vulnerabilities, Misconfigurations.</i>
12:30 – 14:00	SESSION 6 - Hands-on classes in Cyber Range environment: Lateral movement inside the organization's network. <i>Scenario 2</i> <i>Keywords: Living off the land – operations behind the organization's firewall.</i>
14:00 – 14:15	Wrap-up and closing remarks
14:15-15:30	<u>Lunch break</u>

DAY 3	Thursday, 23 March 2023 (CEST)
08:50 – 09:20	<u>Welcome coffee</u>
09:20 – 10:30	<p align="center">SESSION 7 – Theory of WiFi Hacking, Cracking & WiFi Tools</p> <p align="center"><i>Scenario 3</i></p> <p align="center"><i>Keywords: Parrot OS, Aircrack</i></p>
10:30 – 10:45	<u>Coffee break</u>
10:45 – 12:25	<p align="center">SESSION 8 - Hands-on classes in Cyber Range environment: Exercise – complex scenario for WiFi Hacking – WiFi Recon - Practical</p> <p align="center"><i>Scenario 3</i></p> <p align="center"><i>Keywords: WiFi Recon</i></p>
12:25 – 13:45	<p align="center">SESSION 9 - Hands-on classes in Cyber Range environment: Exercise – complex scenario for WiFi Hacking – Network Forensic & Analyzing of PCAP file – Practical.</p> <p align="center"><i>Scenario 3</i></p> <p align="center"><i>Keywords: Network Analysing</i></p>
13:45 – 14.10	<u>Wrap-up</u>
14:10 – 14:30	<p><u>Certificate Ceremony</u></p> <ul style="list-style-type: none"> • <i>Cyber Security Training Centre of Excellence (CSTCoE), Warsaw</i> • <i>European Security and Defence College (ESDC), Brussels</i>
14:30 – 14:40	<i>Closing remarks – End of the course</i>
14:40 – 15:35	<u>Lunch break</u>

Place of the course: Cyber Security Training Centre of Excellence



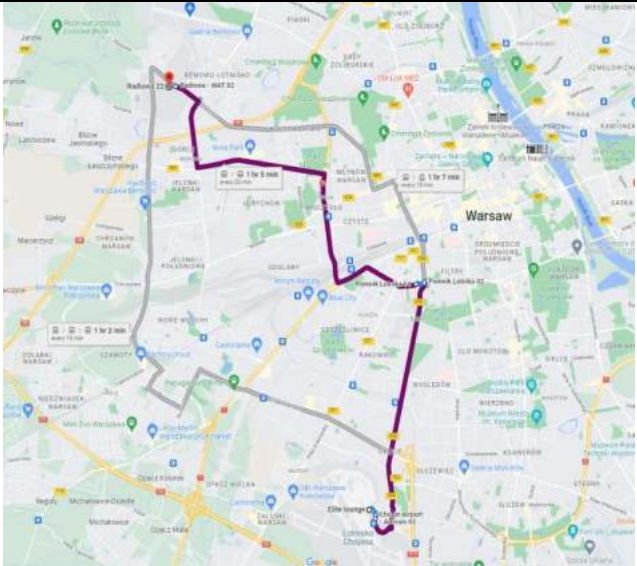


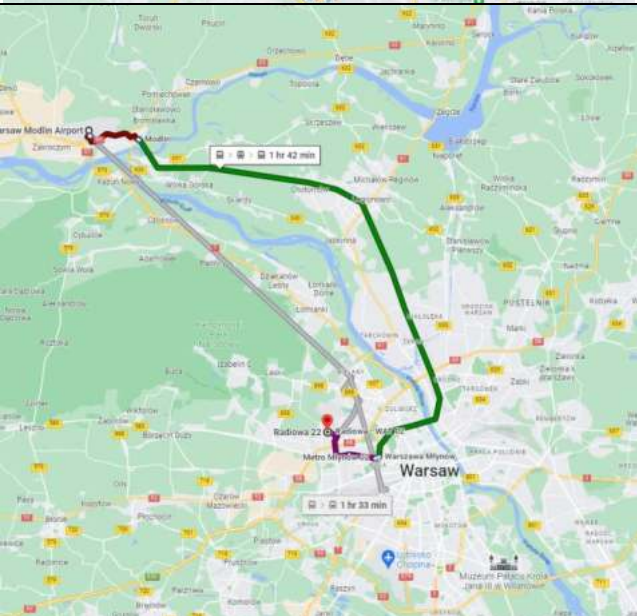
Adress: Kaliskiego 2 (entrance from Radiowa, gate No. 4, building WAT 65)

00-908 Warsaw, Poland

Phone: + 48 22 261 83 79 90 | **Mail:** cstcoe@mon.gov.pl | **Web:** <https://cstcoe.mil.pl/en>

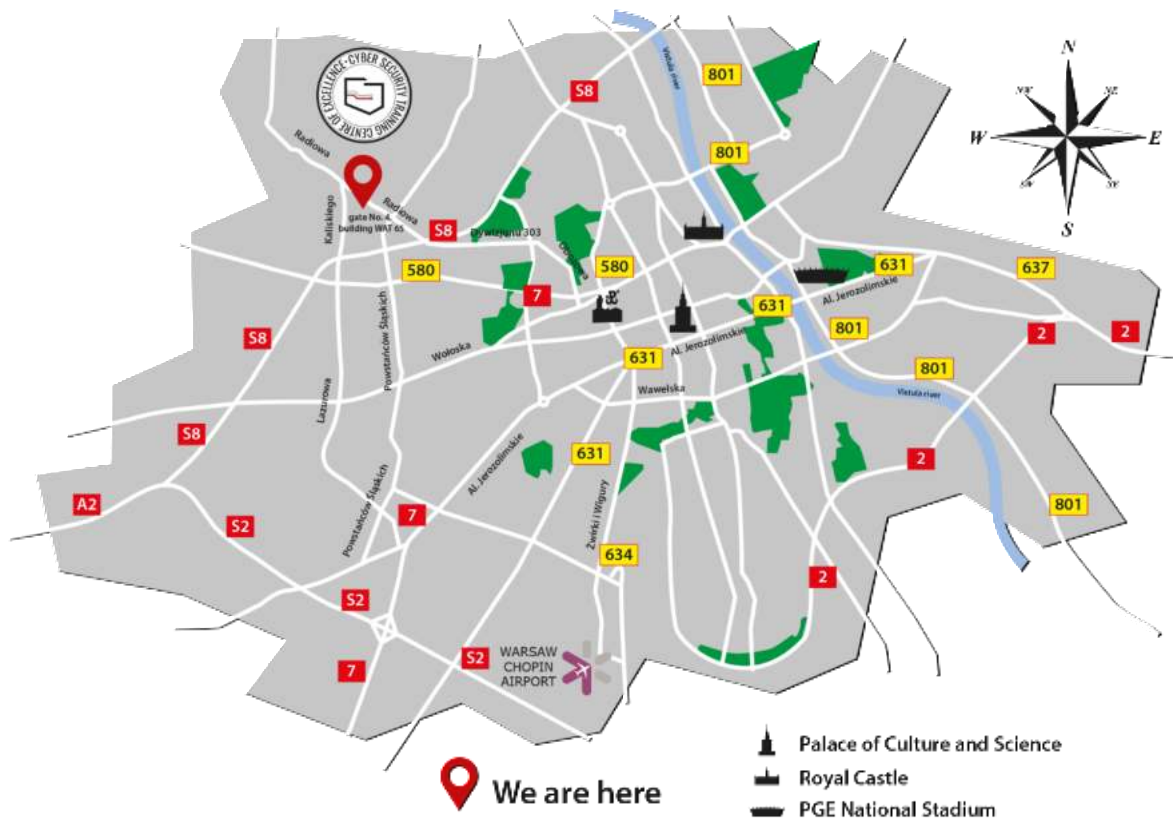
In case of any changes to the organisation of the course, CST CoE will send an appropriate notification to enrolled individuals.

Information on the proposed hotel from which shuttle service will be provided will be communicated at a later date to those who qualify for the course.

Driving direction	Access route
<p>1. From the Warsaw Chopin Airport to the CST CoE</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <p>Active link</p>	
<p>2. From the Masovian Warsaw-Modlin Airport to the CST CoE</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <p>Active link</p>	



Link to public transport in Warsaw: [how can I get to](#)





Annex 4

Additional personal information required to enter military facility

Please be informed, that due to national security regulations, in order to get an access to Cyber Security Training Centre of Excellence facilities additional personal information is required. Therefore, all qualified for this course candidates will be kindly requested to provide below information not later than 24th February 2023 (deadline due to procedures connected with issuance of an access permission).

Complete set of information should be sent via email to PoCs at Cyber Security Training Centre of Excellence listed in Annex 1.

- name, second name (if applicable) and surname
- nationality
- organization/company
- job title
- course name
- date of birth
- ID type (national ID/passport) and number
- military rank (if applicable)
- security clearance (if applicable) - please indicate information domain (national, EU/UE, NATO) and security level

Please bear in mind that any delays or lacks in above information might result with a risk regarding access to the venue of a course.