27-29
SEPTEMBER

2022

Cyber Range – defensive capabilities

CYBER SECURITY TRAINING CENTRE of EXCELLENCE
and EUROPEN SECURITY and DEFENCE COLLEGE

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 – defensive capabilities"

(Activity number 22-23/212/1)

27 – 29 September 2022

The Cyber Security Training Centre of Excellence (CST CoE) under the auspices of the European Security and Defence College (ESDC) is organising the residential course, specialized at strategic-tactical-technical levels, from 27 to 29 September 2022 in Warsaw, Poland.

Digital transformation offers EU citizens the opportunity to reach out beyond historical borders and geographical locations. However, there is a number of challenges associated with cyber domain that need to be tackled in order to make cyberspace resilient to cyber threats.

In response to these challenges, European Union community has its own vision of Europe's digital future and is strongly determined to shape it successfully. Highly skilled digital professionals together with secure and sustainable digital infrastructures, according to *Digital Compass* [1], are defined as crucial challenges for "The European Way for the Digital Decade". By extension, education, exercises and training are widely seen as milestones for meeting above mentioned expectations and needs.

In order to achieve these strategic goals, Cyber Security Training Centre of Excellence in Warsaw (*Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, Warszawa*) together with the European Security and Defence College, is pleased to invite officials from the EU Member States, EU Institutions and Agencies to participate in the course. This course is an activity of the ESDC's Cyber Education Training Exercise and Evaluation (ETEE) platform.

This course follows the current trend of building platforms, also known as cyber training grounds or Cyber Range (CR) platforms. Such solutions allow to simulate a wide array of cyber threats, thanks to which specialists trained in realistic conditions can develop skills required to react to a variety of incidents occurring in the cyber domain and to mitigate the consequences of attacks in cyber domain.

The aim of this course is to develop a more comprehensive approach to advanced exercises and training using new cyber defence technologies and scenarios. This course brings together civilian and military officials [2] and will provide a better understanding of how efficient and useful competences could be gained using CR platform. It will translate to enhanced skills of digital professionals and contribute to building cyber-resilience and strategic autonomy – a pillar of CSDP. The course will be held in English and based on the Cyber Range platform. It will be the opportunity to assess and discuss the importance of CR as a virtual training environment and to share skills.

This course is dedicated to mid-level to senior officials (recommended/expected with IT competences or experience) from MSs, EU Institutions and Agencies dealing with the aspects of cybersecurity and in need of understanding of the cybersecurity threats from a technical perspective. The course is scheduled to take place on the 27-29 September 2022 in in-person format in Warsaw, Poland.

Paweł DZIUBA
Director of CST CoE

Dirk Dubois
Head of ESDC

Annexes

1. Course administrative instructions
2. Draft programme
3. Venue "Cyber Security Training Centre of Excellence (CST CoE)"
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

[2] This course is the opening of next 2-course series devoted to IT engineers and technicians

Annex 1

Course administrative instructions

The course will be held in English and can accommodate a maximum of 12 participants. It is open to mid-ranking to senior officials (civilian and military) from EU Member States, relevant EU institutions and agencies.
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 5 of September 2022**.
A list of relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/.

The course will consist of an **online part** (asynchronous) on the ESDC's e-learning platform and a **live part** , face to face part, both parts being compulsory.

The e-learning part will be available for those who will be selected from 9 September 2022. The topics covered during the face-to-face sessions will be explored in an interactive manner in sessions followed by Q&As, panel discussions and group activities.

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, 26 September 2022. 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 9 September, using the password 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 on site, 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 cancelled. 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 Cyber Security Training Centre of Excellence, Warsaw, Poland

Col AF Michal **MAJEWSKI** Tel: +48 261 837 996 E-mail: michal.majewski@ron.mil.pl	Maj. Jan **KOLOWSKI** Tel: +48 261 837 945 E-mail: j.kolowski@ron.mil.pl	Ms Joanna **ARCHACKA-STACHURA** Tel: +48 571 221 051 E-mail: j.archacka-stachura@ron.mil.pl

Annex 2

European Security and Defence College (ESDC)

"Cyber Range – defensive capabilities"

(22-23/212/1)

DRAFT PROGRAMME

27 September – 29 September 2022 – Residential form

Cyber Security Training Centre of Excellence
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 Michał Majewski

DAY 1	Tuesday, 27 September 2022 (CEST)
08:30 – 09:00	*Registration* *Welcome coffee*
09:00 – 09:45	Course opening • Short presentation of CST CoE • Short presentation the European Security and Defence College (ESDC) and the Cyber ETEE Platform, Brussels
09:45 – 10:00	Welcome session – introduction of instructors and participants Informal Tour-de-Table
10:00 – 10:10	Introduction to the course - presentation of the course objectives. Brief overview of the competence of the team of specialists at CST CoE responsible for Cyber Range training, who organise advanced training and games
	SESSION 1 Overview of the CST CoE's CyberRANGE platform and its potential use.
10:10 – 10:45	• *Presentation*
10:45 – 11:00	*Coffee break*
	SESSION 2 Presentation of the technical aspects of the CyberRange platform design. Possibilities of using the CYBER RANGE tool for organising training for participants in various locations.
11:00 – 12:15	• *Demonstration*
12:15 – 13:30	*Lunch break*
	SESSION 3 Activities in the cyberspace domain in the escalation phase and during the conflict in Ukraine.
13:30 – 14:30	• *Presentation*
	SESSION 4 Case study. Groupwork.
14:30 – 15:30	• *Seminar*
15:30 – 15:45	Group photo
15:45 – 15:55	*Summary*

DAY 2	Wednesday, 28 September 2022 (CEST)
08:30 – 09:00	*Welcome coffee*
09:00 – 09:15	Introduction to the workshop, discussion of the concept and delivery
	SESSION 5 Kill Chain – explanation of the problem.
09:15 – 09:45	- *Presentation*
09:45 – 11:30	SESSION 6 Presentation of the scenario prepared for the workshop. Background – embedding the discussed topics in reality, activities and techniques, discussion on the basis of the operation of APT groups.
	- *Demonstration, Presentation*
11:30 – 11:45	*Coffee break*
	SESSION 7 Environment – presentation and description of the environment virtualised in CyberRange in which the workshop will be conducted.
11:45 – 12:15	- *Demonstration*
12:15 – 13:30	*Lunch break*
	SESSION 8 Workshop – conducting a scenario, discussing the next steps and the steps performed by the attacker.
13:30 – 14:30	- *Demonstration*
	SESSION 9 Mapping of selected techniques onto the MITRE ATT&CK matrix and discussion of mitigants.
14:30 – 15:30	- *Demonstration*
15:30 – 15:40	*Summary*
15:40 – 16:00	*Questions and Answers*
19:30 – 21:00	*Icebreaker Dinner*

DAY 3	Thursday, 29 September 2022 (CEST)
08:30 – 09:00	*Welcome coffee*
09:00 – 09:05	Introduction to the third day of the course
	SESSION 10 Computer fraud as the most frequently handled incidents (86%), including phishing (77% of total incidents)
09:05 – 10:00	- *Presentation*
	SESSION 11 How criminals work - phishing - the practical part
10:00 – 11:00	- *Demonstration*
11:00 – 11:15	*Coffee break*
	SESSION 12 Presenting the course *"Pentester Tools - Basic Course"*
11:15 – 11:45	- *Presentation*
	SESSION 13 Presenting the course "*Cyber Range - Cybersecurity in practice"*
11:45 – 12:00	- *Presentation*
12:00 – 13:15	*Lunch break*
	SESSION 14 Cyber Range - Effectiveness of raising digital competence digital competence of staff responsible for cyber security
13:15 – 14:00	- *Seminar*
14:00 – 14:10	*Summary*
14:10 – 14:20	Certificate Ceremony
14:20 – 14:40	Closing Remarks - End of the Course

Annex 3

Place of the course: Cyber Security Training Centre of Excellence

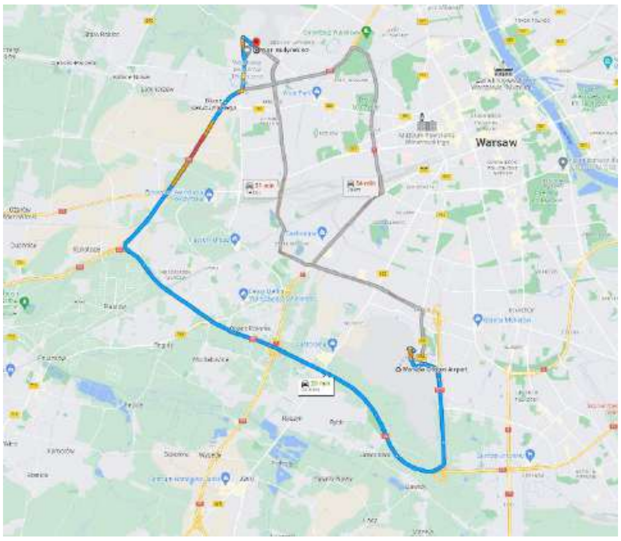
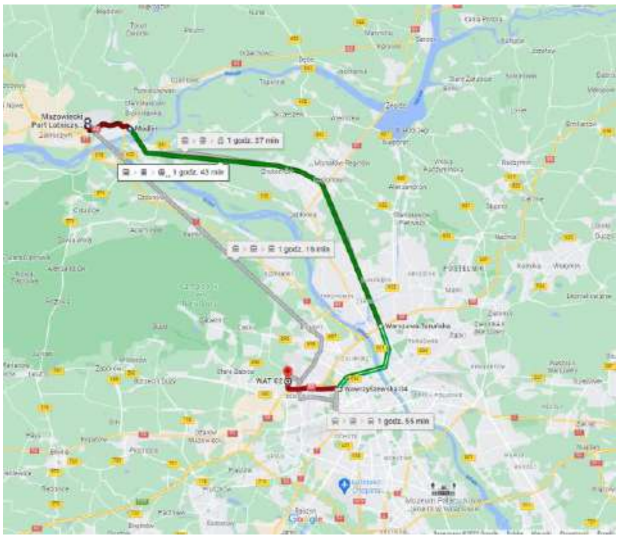
Adress: Kaliskiego 2 (entrance from Radiowa, gate No. 4, building WAT 65)

00-908 Warsaw, Poland

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

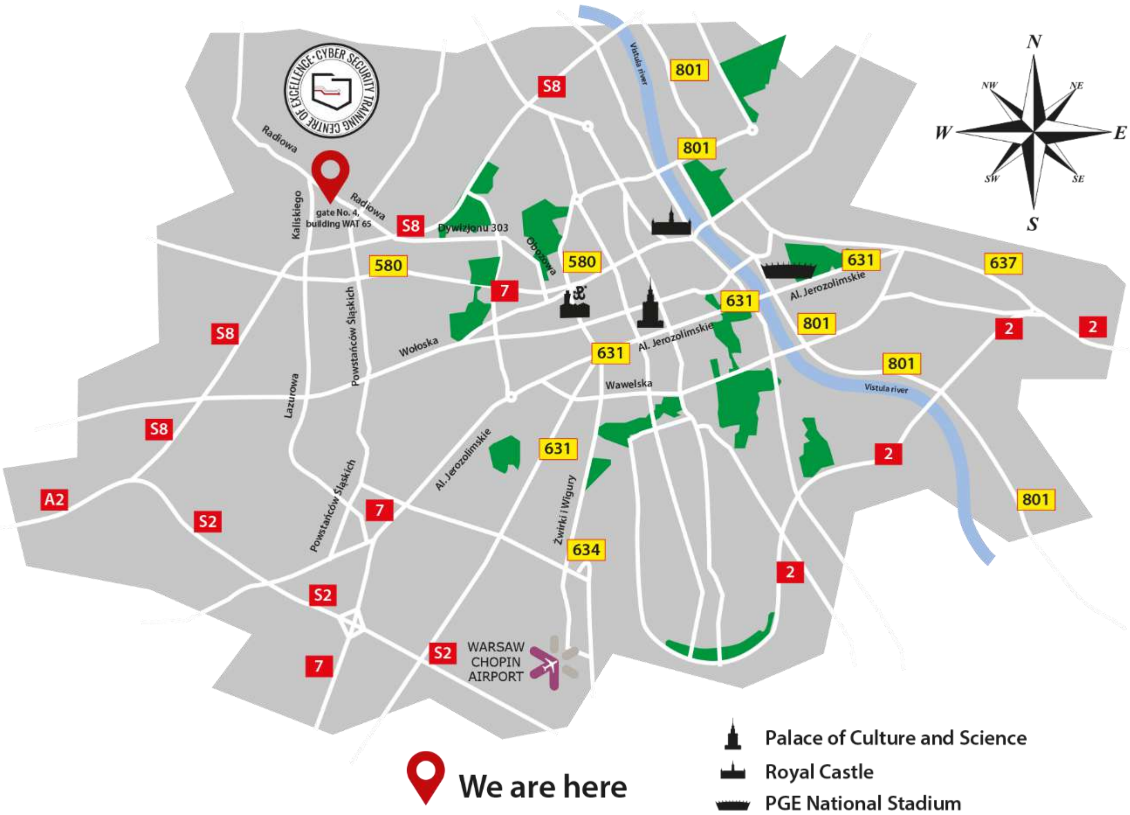
In case of any changes to the organisation of the course, CST CoE will send an appropriate notification to enrolled individuals.

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
1. From the Warsaw Chopin Airport to the CST CoE 🚆 TAXI	
2. From the Masovian Warsaw-Modlin Airport to the CST CoE 🚆 TAXI	 1 godz. 37 min 1 godz. 43 min 1 godz. 16 min 1 godz. 55 min WAT 65

S2 523 175

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 9th September 2022 (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.