European Security and Defence College

Contributing to EU Integrated Approach
European Security Defence College

- ESDC Objectives
- ESDC Network
- ESDC Evolution of Activities
- ESDC Annual Circle
- CYBER ETEE PLATFORM
- Cyber Threat Intelligence
ESDC objectives

Council Decision (CFSP) 2016/2382

• to further enhance the common European security and defence culture within CSDP;
• to promote a better understanding of CSDP as an essential part of CFSP;
• to provide Union instances and Member States with knowledgeable personnel familiar with EU policies, institutions and procedures in the field of CFSP;
• to support civilian crisis management in the field of conflict prevention, and establishing or preserving the conditions necessary for sustainable development;

• to provide CSDP Missions' and Operations' personnel with a common understanding of functioning principles and a sense of common European identity;
• to provide training responding to training needs of CSDP Missions and Operations;
• to support EU partnerships in the field of CSDP/CFSP with those countries participating in CSDP missions;
• to help promote professional relations and contacts among participants in ESDC training activities;
• to promote the European Initiative for the Exchange of Young Officers.

• to provide Union instances and Member States with knowledgeable personnel familiar with EU policies, institutions, procedures and best practices in the field of Cyber Security and Defence.
ESDC in a nutshell (as of Sep 2018)

132 network members + 5 Associated Network Partners (ANP)

Running 114 activities in the past academic year

Since 2005 24000 alumni
Independent sui-generis organisation

- Legal capacity
- Embedded in the EEAS structures
- Council Decision (CFSP) 2016/2382

"Course participants shall be personnel dealing with strategic aspects in the field of CFSP and experts to be deployed in CSDP missions or operations"

- Certificates signed by HR/VP
- Curricula certified by 28 EU MSs in close cooperation with relevant EU institutions
Evolution ESDC activities

Trendline

Staff resources (including Cyber ETEC)
ESDC annual cycle

**Plan:** before summer break
- SC: priorities
- EAB: programming

**Do:**
- Run Courses

**Act:**
- Update curricula (Feb)

**Check:**
- GAREA (Sep)
- New policies
- Lessons learnt
- Curricula valid? (Nov)

**Requirements**
- EU Member States
- EUMTG
- EUCTG

**EAB + EU Structures**
Cyber Education, Training and Evaluation Platform under ESDC
Cyber Education, Training and Evaluation Platform under ESDC

AIM

To address cyber security and defence training among the civilian and military personnel, including for the CSDP requirements for all CSDP training levels as identified by the EU Military and Civilian Training Groups, and upscaling the training opportunities for the Member States.

At a later stage and depending on the further development of such a concept, the Cyber ETEE platform could advance ETEE opportunities for wider cyber defence workforce.
Cyber ETEE Platform will deal with all cyber domains:
Cyber ETEE Platform

WHAT: Cyber Activities

- Awareness
- Tactical
- Strategic
- Technical
- Legal
Cyber ETEE Platform

HOW: Work to be Carried out

- Education/Training
- Exercises
- Workshops/Conferences
- Research
Who are the potential stakeholders?

- Cybercrime
- Network Information Security
- Cyberdefence
- External relation - Policy
Cyber Education, Training and Evaluation Platform under ESDC

Potential stakeholders in Cybercrime

- Member States
- Europol/EC3
- Eurojust
- ECTEG
- CEPOL
Cyber Education, Training and Evaluation Platform under ESDC

Potential stakeholders in Network Information Security

• Member States
• European Commission
• ENISA
• CERT-EU
Cyber Education, Training and Evaluation Platform under ESDC

Potential stakeholders in Cyberdefence

• Member States
• European External Action Service
• EUMC
• EUMS
• EDA
• EU SATCEN
Potential stakeholders in External Relations - Policy

• Member States
• European Commission
• European External Action Service
• Council of the European Union
• EU ISS
Cyber Threat intelligence

- Evaluate the role of the human factor related with the cyber threat intelligence?
- Which is the relation between lessons learned and Cyber Threat Intelligence?
- Which is the relation between Training, cyber threat intelligence and threat landscape
Cyber Threat intelligence

• How it is link with the training schema presented?
• Are the Cyber Threat Intelligence relevant in all domains of Cyber Security?
• The Cyber Threat Intelligence can give us target oriented training?