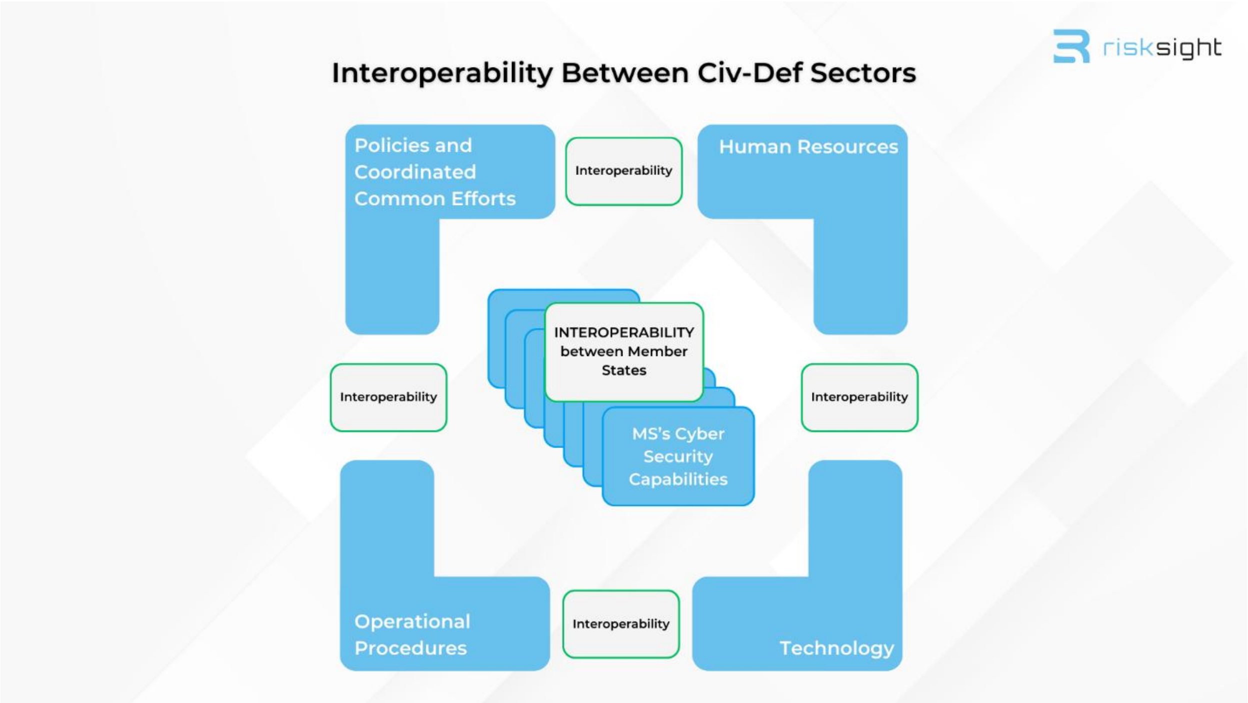
ECYBRDIGE. Work Package 8. Training Event 1. Information Sheet

General Information

The Work Package 8, Training, is integral to the success of the ECYBRIDGE project. Building upon the broader scope of the ECYBRIDGE project, Work Package 8 focuses on the critical cybersecurity matters between civil and defence sectors on a more granular level, tailoring the training for an operational level approach. Furthermore, the ultimate goal of Work Package 8 is to develop the interoperability between civil and defence sectors amongst EU Member States.


risksight
Interoperability Between Civ-Def Sectors
Policies and Coordinated Common Efforts
Interoperability
Human Resources
INTEROPERABILITY between Member States
Interoperability
Interoperability
MS's Cyber Security Capabilities
Operational Procedures
Interoperability
Technology

Throughout Work Package 8, four independent training sessions are hosted:

- **Training 1:** "Creating Shared Situational Awareness Between Civil and Defence Sectors in Cybersecurity". **12th – 16th of May 2025. Constanta, Romania.**
- **Training 2:** "Common and Coordinated EU Efforts (Incident Response & Management)". 8th – 12th of Sept 2025*. Varna, Bulgaria
- **Training 3:** "EU Cybersecurity Policy Framework in Civil-Defence Cooperation". 10th – 14th of Nov 2025*. Tallinn, Estonia
- **Training 4:** "The Decision-Making Process & Courses of Action as a part of Active Cyber Defence". 2nd – 6th of Feb 2026*. Brussels, Belgium

Training Event 1

Introduction

WP8. Task 1: Training - "Creating Shared Situational Awareness Between Civil and Defence Sectors in Cybersecurity"

Training 1 of Work Package 8 is designed to equip participants with the knowledge and skills to enhance the shared situational awareness between civil and defence sectors in the cybersecurity field. Required steps are explored in the order of the meaning of threat intelligence, sharing of information and its best practices and ultimately the pillars to a successful sharing network, resulting in shared situational understanding which when established in harmony, translates to shared situational awareness.

Key Takeaways for Training 1 are:

- Creating a common understanding of cyber threat intelligence
- Developing capabilities for information sharing
- Creating understanding of the whole-of-society approach

Target Audience

The Target Audience for the Work Package 8 Training Events is seen as a high-level audience working either at the operational or strategic level. Although technical level participants are very welcome, they are not the core focus of the training audience.

The foreseen Training Audience for the designated training should mostly qualify to the following general principles:

- Expertise in the government, internal security, defence and/or private sector
- Seniority of operational level management or higher
- General level understanding of organisational operational procedures, cyber operations, cyber crisis management and GRC mechanisms in cybersecurity
- Fluent in English (written, spoken)
- General computer skills (interaction with a web-based platform)

Sample profiles of attendees could be some of the following:

- **Government Officials** (e.g. mid-to-senior civil servants, policy advisors, IT-directors, cybersecurity liaisons etc.)
- **Military Officers** (e.g. cyber operations, intelligence, senior military staff involved in strategic and operational planning)
- **Private Sector Executives** (e.g. Chief Information Security Officers, Chief Information Officers)

- **Academia and Private Sector Subject Matter Experts** (e.g. cybersecurity, GRC, communications specialists/professors/researchers)
- **International & Security Organization Officials** (e.g. cybersecurity leaders and representatives, heads and strategic planners of CERTs)

Format

The three-day training activity seeks to facilitate rigorous academic, professional, and policy-driven learning actions through collaboration of experts in civil, defence and other supporting sectors. The Training Event is conducted in a hybrid format, both physically on site in Constanta, Romania as well as online via Microsoft Teams.

- REQUIREMENTS for Physical Attendance: Bring your own device, laptop required
- REQUIREMENTS for Virtual Attendance: Personal computer or laptop and MS Teams. Recommendation of 2 screens.

The training displays a diverse agenda featuring both theoretical and practical sessions that can include (but is not limited to) the following:

- Theoretical Presentations
- Seminar-Style Practical Discussions (e.g. Case Studies)
- Workshops (in Working Groups)
- Scenario-Based Simulations
- Q&A Sessions

Online software solutions and engagement tools are used to ensure interactivity and engagement of the participants throughout the sessions.

Time	Day 1 (Tue)
09:00 – 09:45	Kick-Off Ceremony
09:45 – 10:00	Setup Logistics
10:00 – 11:00	Cyber Threat Intelligence
11:00 – 11:30	Break
11:30 – 13:00	Whole of Society Approach
13:00 – 14:00	Lunch
14:00 – 15:30	Information Sharing – State of Play
15:30 – 16:00	Summary
16:00 – 17:00	Networking
Time	**Day 2 (Wed)**
09:00 – 09:15	Day Introduction
09:15 – 09:30	Setup Logistics
09:30 – 11:00	Information Sharing - Reporting
11:00 – 11:30	Break

11:30 – 13:00	Creating Shared Situational Awareness in the Operational Environment
13:00 – 14:00	Lunch
14:00 – 15:30	Pillars to a Successful Information Sharing Network
15:30 – 16:00	Summary
16:00 – 17:00	Networking
Time	**Day 3 (Thu)**
09:00 – 09:15	Day Introduction
09:15 – 09:30	Setup Logistics
09:30 – 11:00	Scenario-Based Simulation
11:00 – 11:30	Break
11:30 – 13:00	Scenario-Based Simulation
13:00 – 14:00	Lunch
14:00 – 15:30	Scenario-Based Simulation
15:30 – 15:45	Break
15:45 – 17:00	Closing Ceremony & Refreshments

Registration

The one and only applicable medium for registration is the online form: https://forms.office.com/e/fE7FpduHER

Without registering via the online form, the participation is not guaranteed!

Should there be any questions regarding the attendance and/or registration, please reach out to the lead organizers at markus.mynzer@risksight.io.