Cyber Crisis Management: Navigating Disinformation and Cyber Attacks in the AI Era

Berlin, 13–15 August 2025

Cosimo Melella

EU CyberNet

Federal Foreign Office

Funded by the European Union

Outlook

- **Why cyber crisis management and disinformation matter today**

- **The role of EU CyberNet and the summer school initiative**

- **2025's focus: AI and hybrid disinformation threats**

- **Training goals and target audience**

- **Overview of the 3-day agenda: theory, tools, and simulation**

- **Final mission: preparing EUCN trainers for the field**
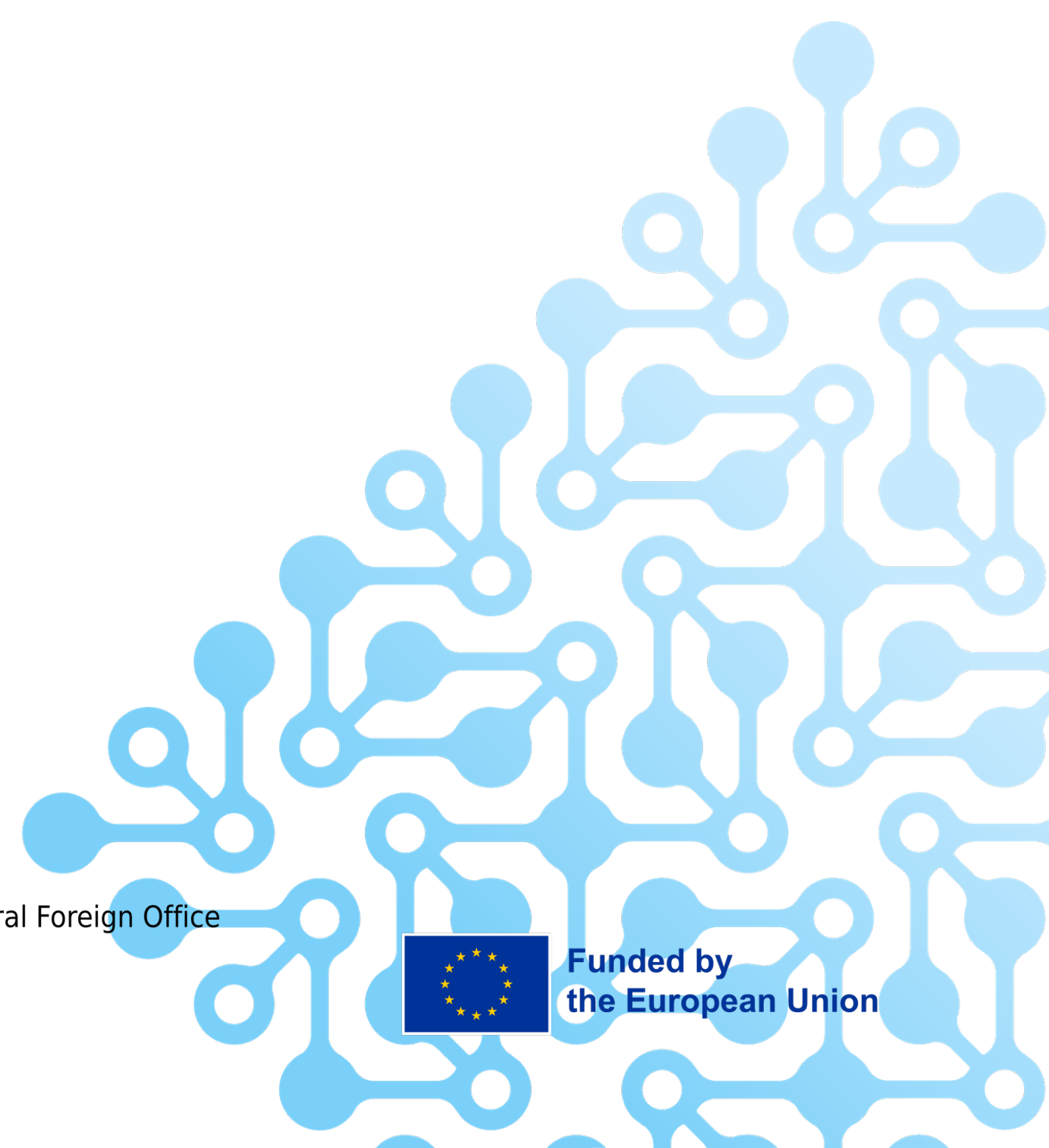
Cyber Crisis Management: Navigating Disinformation and Cyber Attacks in the AI Era

EU CyberNet

Federal Foreign Office

Funded by the European Union

D.O.D.O

- **Why cyber crisis management and disinformation matter today**

- The role of EU CyberNet and the summer school initiative

- 2025's focus: AI and hybrid disinformation threats

- Training goals and target audience

- Overview of the 3-day agenda: theory, tools, and simulation

- Final mission: preparing EUCN trainers for the field

EU CyberNet

Federal Foreign Office

Funded by the European Union

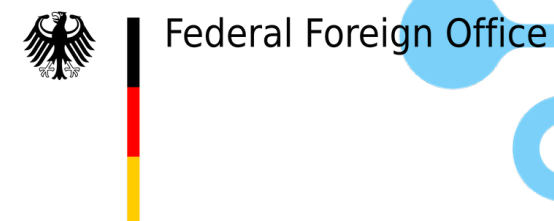# Why cyber crisis management and disinformation matter today

In today's digital battlefield, disinformation campaigns are no longer isolated threats, they are integrated into broader hybrid operations, often supported by artificial intelligence and timed to exploit societal vulnerabilities.

- Disinformation has become a strategic weapon, used to destabilize elections, institutions, and crisis responses.

- AI-powered deepfakes and bots make false narratives more credible, scalable, and hard to detect.

- Cyberattacks are now multi-layered, combining physical system breaches with information manipulation.

- In the absence of trust and coordination, public confusion delays response, making crises more damaging.

D.O.D.O. OÜ

D.O.D.O

- Why cyber crisis management and disinformation matter today

- **The role of EU CyberNet and the summer school initiative**

- 2025's focus: AI and hybrid disinformation threats

- Training goals and target audience

- Overview of the 3-day agenda: theory, tools, and simulation

- Final mission: preparing EUCN trainers for the field

**Cyber Crisis Management:
Navigating Disinformation and
Cyber Attacks in the AI Era**

EU CyberNet

Federal Foreign Office

Funded by
the European Union

The role of EU CyberNet and the summer school initiative

EU CyberNet serves as the European Union's operational hub for cyber expertise, training professionals, supporting capacity building, and responding to emerging digital threats globally.

- 500+ cyber experts across cybersecurity, cybercrime, diplomacy, AI, and data protection.

- Delivers global training, needs assessments, and expert missions to partner countries.

- Summer School launched in 2022 to refresh skills and prepare new EUCN trainers.

- 2025 edition addresses AI-enabled disinformation and hybrid threats.

EU CyberNet

Federal Foreign Office

Funded by
the European Union

D.O.D.O

- Why cyber crisis management and disinformation matter today

- The role of EU CyberNet and the summer school initiative

- **2025's focus: AI and hybrid disinformation threats**

- Training goals and target audience

- Overview of the 3-day agenda: theory, tools, and simulation

- Final mission: preparing EUCN trainers for the field

EU CYBERNET SUMMER SCHOOL 2025
**Cyber Crisis Management:
Navigating Disinformation and
Cyber Attacks in the AI Era**

EU CyberNet

Federal Foreign Office
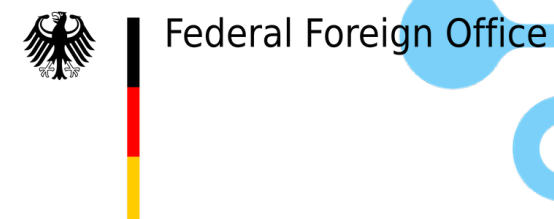
Funded by
the European Union

2025's focus: AI and hybrid disinformation threats

The 2025 Summer School addresses the fusion of AI and disinformation as a growing cyber crisis threat. Unlike traditional cyberattacks, today's threats target minds and emotions as much as machines.

- Deepfakes and synthetic content now enable the creation of highly realistic false narratives.

- Automated bots, chatbots, and algorithmic promotion accelerate the spread of disinformation.

- Cyber crises increasingly involve a psychological front, targeting emotions and perception.

- False information spreads significantly faster than facts, making response coordination more difficult.

EU CyberNet

Federal Foreign Office

Funded by the European Union

D.O.D.O

- Why cyber crisis management and disinformation matter today

- The role of EU CyberNet and the summer school initiative

- 2025's focus: AI and hybrid disinformation threats

- **Training goals and target audience**

- Overview of the 3-day agenda: theory, tools, and simulation

- Final mission: preparing EUCN trainers for the field

EU CyberNet

Federal Foreign Office
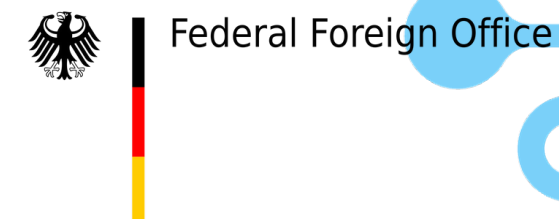
Funded by the European Union

Training goals and target audience

The EUCN Summer School equips professionals with the expertise to navigate today's most complex disinformation challenges, and to become multipliers in the field. With the goal of:

- Learn to detect, analyse, and counter AI-driven disinformation across digital platforms

- Understand how disinformation undermines cyber resilience and erodes public trust

- Use AI-powered tools and operational frameworks for crisis detection and response

- Prepare to act as EUCN trainers, delivering future workshops and advisory missions

EU CyberNet

Federal Foreign Office

Funded by the European Union

D.O.D.O

- Why cyber crisis management and disinformation matter today

- The role of EU CyberNet and the summer school initiative

- 2025's focus: AI and hybrid disinformation threats

- Training goals and target audience

- **Overview of the 3-day agenda: theory, tools, and simulation**

- Final mission: preparing EUCN trainers for the field

EU CyberNet

Federal Foreign Office

Funded by
the European Union

# Overview of the 3-day agenda: theory, tools, and simulation

Over the course of three days, participants will move from foundational knowledge to hands-on simulation. The agenda blends strategic theory, real-world case studies, technical tools, and collaborative crisis response.

- **Day 1: Framing the Threats**
  - Understand hybrid warfare, the psychology of disinformation, and the erosion of trust in democratic institutions. Includes real-world case studies and AI's offensive and defensive roles.

- **Day 2: Tools, Protocols & Applied Practice**
  - Gain hands-on experience with frameworks like DISARM, OpenCTI, and threat modeling. Learn how to mitigate disinformation using AI-enabled detection.

- **Day 3: Simulation, Ethics & Strategic Debrief**
  - Participate in a live multi-phase cyber crisis simulation. Engage in ethical reflection and regulation discussions. Conclude with group presentations and trainer preparation for future EUCN missions.

EU CyberNet

Federal Foreign Office
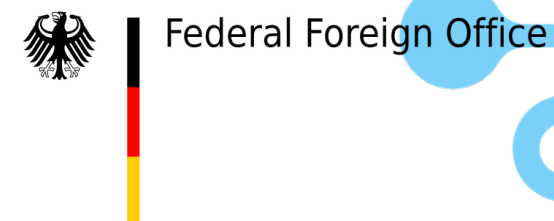
Funded by the European Union

Day 1: Framing and Case Studies

- Explore how hybrid warfare combines cyberattacks, disinformation, and psychological operations.

- Examine real-world case studies of disinformation campaigns and their real-time impact.

- Understand the dual use of AI: as a tool for generating and detecting disinformation.

- Analyse how social media ecosystems accelerate the spread and reach of false narratives.

EU CyberNet

Federal Foreign Office

Funded by the European Union
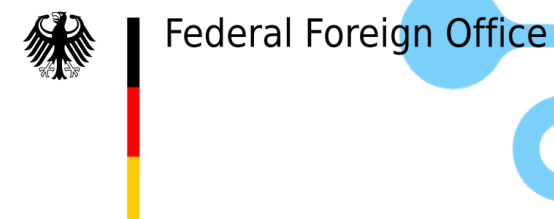
Day 2: Tools and Simulation

- Learn how G7/NATO rapid response frameworks, DISARM, and OpenCTI support structured, real-time threat tracking.

- Use AI-powered tools to detect and classify disinformation and information laundering.

- Explore risk profiling, proactive messaging, and strategic communication under uncertainty.

- Apply knowledge during a multi-phase simulation simulating disinfo escalation and coordinated cyberattacks.

**Cyber Crisis Management:
Navigating Disinformation and
Cyber Attacks in the AI Era**

EU CyberNet

Federal Foreign Office
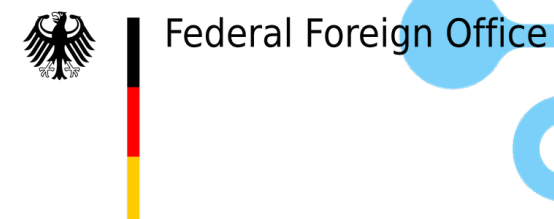
Funded by
the European Union
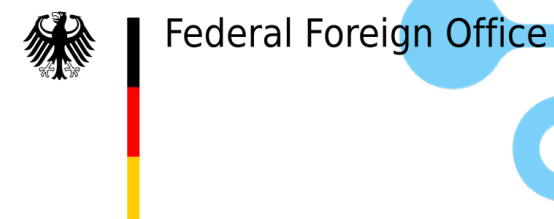
Day 3: Ethics and Wrap-up

- Discuss current AI regulations and the ethical boundaries in deploying disinformation detection and generation tools.

- Present outcomes from the table-top simulation and assess team strategies under realistic pressure.

- Final debrief and feedback session, review key lessons and define the path toward becoming an EUCN field trainer.

EU CYBERNET SUMMER SCHOOL 2025
**Cyber Crisis Management:
Navigating Disinformation and
Cyber Attacks in the AI Era**

Federal Foreign Office

Funded by
the European Union

D.O.D.O

- Why cyber crisis management and disinformation matter today

- The role of EU CyberNet and the summer school initiative

- 2025's focus: AI and hybrid disinformation threats

- Training goals and target audience

- Overview of the 3-day agenda: theory, tools, and simulation

- **Final mission: preparing EUCN trainers for the field**

EU CyberNet

Federal Foreign Office
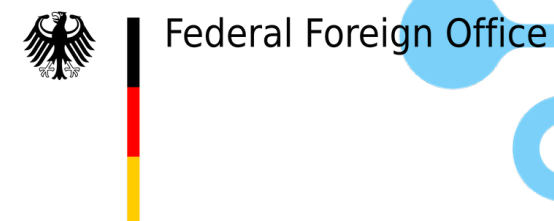
Funded by
the European Union

Final Mission: Preparing EUCN Trainers for the Field

The summer school culminates in a clear mission: to empower participants to become trusted EUCN trainers, ready to advise, train, and lead during cyber crises.

- Apply newly acquired knowledge to support EUCN missions globally.

- Become a multiplier: transfer skills to national and international audiences.

- Be ready to respond to cyber crisis scenarios involving disinformation and AI threats.

- Support partner countries with strategic advice, tools, and best practices.

- Strengthen the EU's collective resilience through proactive engagement.

EU CyberNet

Federal Foreign Office

Funded by the European Union

D.O.D.O. OÜ

Thank You!

Questions ?

EU CYBERNET SUMMER SCHOOL 2025

**Cyber Crisis Management:
Navigating Disinformation and
Cyber Attacks in the AI Era**

EU CyberNet

Federal Foreign Office

Funded by
the European Union