Cyber Crisis & Trust in the EU

Berlin, 13–15 August 2025

Cosimo Melella & Rosaria Talarico

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

Outlook

D.O.D.O. OÜ

- Trust as a Strategic Target
- The Lifecycle of a Cyber Crisis
- Attribution Obfuscation and Fingerprinting
- Disinformation and Social Engineering
- Malinformation: Truth as a Weapon
- Disinformation in Crisis Scenarios
- Strategic Communication & Resilience
- Artificial Intelligence: A Double-Edged Sword
- Conclusion: Cybersecurity = Trust Security

EU CyberNet
Federal Foreign Office
Funded by the European Union

Training Objectives

D.O.D.O. OÜ

- Understand the definitions, lifecycle, and impact of cyber crises in the EU context
- Identify the key EU legislation: NIS2 Directive, Cyber Resilience Act (CRA), and Cyber Solidarity Act (CSOA)
- Explore the hybrid threat landscape, including **disinformation**, **phishing**, **false flag operations**, and **trust erosion**
- Analyze advanced tactics such as obfuscation techniques, **malinformation**, and **AI-based disinformation strategies**

EU CyberNet

Federal Foreign Office

Funded by the European Union

Trust as a Strategic Target

D.O.D.O. OÜ

In cyber crisis scenarios, trust is the real strategic objective

Undermining public trust in institutions, media, and digital systems is a powerful destabilization tool

Crises that shake confidence also impair democratic resilience and effective governance

Once trust is lost, recovery becomes exponentially more difficult

EU CyberNet

Federal Foreign Office

Funded by the European Union

The Lifecycle of a Cyber Crisis

D.O.D.O. OÜ

- **Prevent**: Apply cybersecurity best practices, raise awareness, share threat intelligence
- **Prepare**: Conduct joint exercises, define SOPs, align stakeholders
- **Respond**: Coordinate across technical (CSIRTs), operational (CyCLONe/ENISA), and political (IPCR) levels
- **Recover**: Rebuild systems and public trust, ensuring transparency and accountability throughout

EU CyberNet

Federal Foreign Office

Funded by the European Union

The Lifecycle of a Cyber Crisis

D.O.D.O. OÜ

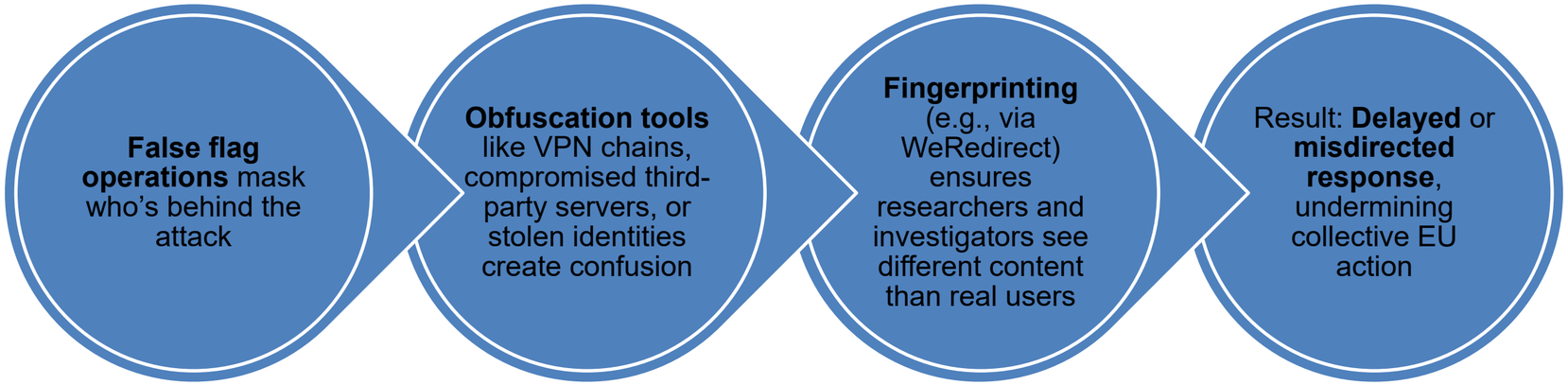
EU CyberNet

Federal Foreign Office

Funded by the European Union

Attribution Obfuscation and Fingerprinting

D.O.D.O. OÜ



EU CyberNet

Federal Foreign Office

Funded by the European Union

Disinformation and Social Engineering

D.O.D.O. OÜ

Phishing and **fake news** exploit the same human weakness: **trust**

These tactics are designed to evoke emotion, bypass reasoning, and provoke impulsive decisions

Algorithms create personalized information bubbles that reinforce existing beliefs and block opposing views

The battlefield is not the device, it's **the mind**

EU CyberNet

Federal Foreign Office

Funded by the European Union

Malinformation: Truth as a Weapon

D.O.D.O. OÜ

- **Malinformation** = true information shared with malicious intent
- **Examples:** data leaks, stolen emails, context-manipulated truths
- **Purpose:**
  - Blackmail or public humiliation
  - Delegitimize institutions or individuals
  - Incite public distrust and emotional backlash
- **Malinformation shows that even truth can be weaponized**

EU CyberNet

Federal Foreign Office

Funded by the European Union

Disinformation in Crisis Scenarios

Disinformation is not a side effect, it’s often strategically paired with cyberattacks

Tactics include:

High-quality videos and memes

Emotional storytelling (“helmeted narratives”)

Strategic timing to shape public perception post-incident

Target is not infrastructure, it’s **the cognitive and emotional response** of citizens

Federal Foreign Office
Funded by the European Union

Strategic Communication & Resilience

D.O.D.O. OÜ

- **A cyber crisis is** always also **a communication crisis**
- **Disinformation** thrives in information vacuums**: silence is vulnerability**
- **Effective crisis communication should be:**
  - Rapid and transparent
  - Credible and fact-based
  - Coordinated across institutions
- **Empowering citizens with media literacy is essential to long-term resilience**

EU CyberNet

Federal Foreign Office

Funded by the European Union

Strategic Communication & Resilience

D.O.D.O. OÜ

EU CYBERNET SUMMER SCHOOL 2025

Cyber Crisis & Trust in the EU

EU CyberNet

Federal Foreign Office

Funded by the European Union

Artificial Intelligence: A Double-Edged Sword

D.O.D.O. OÜ

- **AI creates** sophisticated **fake content** (deepfakes, fake articles, AI-generated profiles)
- **Algorithms** amplify and **target disinformation campaigns to specific audiences**
- **But AI** also supports:
  - **Detection and tracking of disinformation**
    - **Pattern recognition**
  - **Counter-propaganda efforts**
- The critical question: **Who controls the narrative**, the algorithm or democratic oversight?

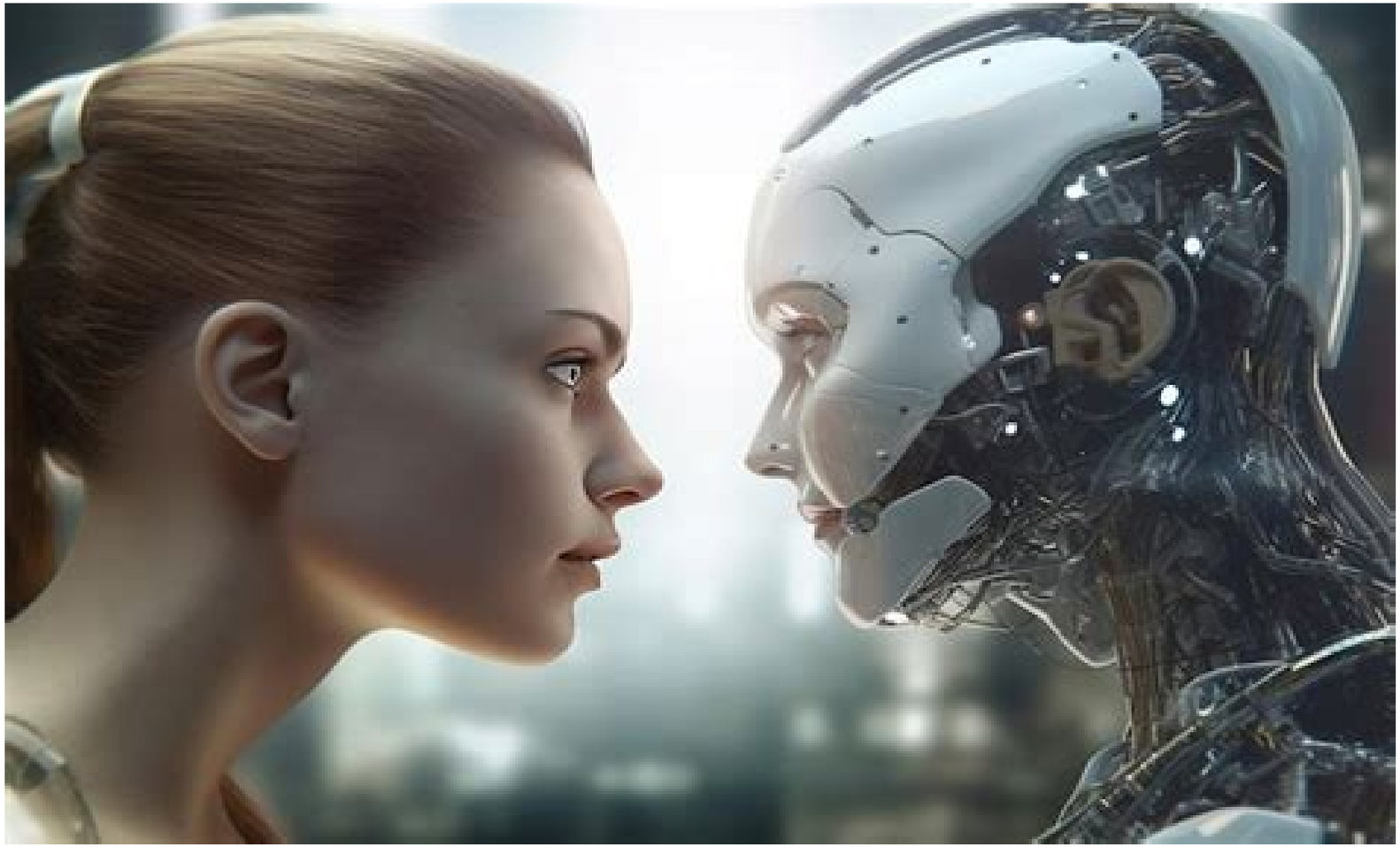
EU CyberNet

Federal Foreign Office

Funded by the European Union

Artificial Intelligence: A Double-Edged Sword

D.O.D.O. OÜ



EU CYBERNET SUMMER SCHOOL 2025

Cyber Crisis & Trust in the EU

EU CyberNet

Federal Foreign Office

Funded by the European Union

Conclusion: Cybersecurity = Trust Security

D.O.D.O. OÜ

The line between cyber and cognitive warfare is blurring

Trust is as critical as physical infrastructure, and even harder to restore

Safeguarding trust requires:

Coordinated EU-level responses

Strong public communication

Resilient, educated civil societies

Whoever shapes the narrative shapes the outcome

EU CyberNet

Federal Foreign Office

Funded by the European Union

D.O.D.O. OÜ

Thank You!

Questions ?

EU CyberNet

Federal Foreign Office

Funded by the European Union