MARCH 2024
#EUDefence
#StrategicCompass

CYBER DIPLOMACY AND CYBER DEFENCE: EU EXTERNAL ACTION

The Strategic Compass provides further guidance on strengthening the EU's ability to prevent, deter and respond to cyberattacks. The EU is determined to promote and protect a global, open, stable and secure cyberspace for everyone to have a safe digital life. Increased cybersecurity is essential for the EU to become a resilient, green and digital Union.

Cyber threats are evolving very fast, with technologies being increasingly misused for:

- **Interference in democratic processes and elections**
- **Attacks against critical infrastructure**
- **Cyber espionage & intellectual property theft**
- **Ransomware as a business model for cyber criminals**
- **Censoring, observing and repressing citizens**

The EU stands for a global, open, stable and secure cyberspace based on:

- **GLOBAL CYBER RESILIENCE**
- **CONFLICT PREVENTION AND RULES BASED ORDER**
- **PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS**
- **COOPERATION WITH INTERNATIONAL PARTNERS**

EU CYBERSECURITY STRATEGY

The EU Cybersecurity Strategy will increase resilience, technological sovereignty and EU leadership; build operational capacity to counter malicious cyber activities; and promote cooperation for a global and open cyberspace.

The EU Cybersecurity Strategy covers 4 external policy areas:

LEADERSHIP ON INTERNATIONAL NORMS AND STANDARDS

- Contribute to the establishment a UN Programme of Action to Advance **Responsible State Behaviour** in Cyberspace;
- Diplomatic outreach & multilateral cooperation (e.g. United Nations);
- Confidence-building measures (e.g. OSCE, ASEAN Regional Forum).

PREVENTING, DETERRING AND RESPONDING TO CYBER-ATTACKS

- Implementing the **EU Cyber Defence Policy** to be better prepared for, defend against and respond to cyberattacks;
- Establish an **EU Cyber Defence Coordination Centre** to enhance situational awareness and coordinated response to cyber-attacks incl. through **Cyber Rapid Response Teams**;
- Sustained use of the **Cyber Diplomacy Toolbox**, including capacity building, political declarations, demarches, dialogues, sanctions, to **address persistent malicious behaviour** in cyberspace.

PARTNERSHIPS AND INTERNATIONAL COOPERATION

- **Dialogues** with third countries & international organisations;
- Develop inter-regional **partnerships** and set-up bi-regional networks of Cyber Ambassadors;
- Exchanges with **civil society, academics, private sector**.

EXTERNAL CYBER CAPACITY BUILDING

- Increase cyber resilience and cyber defence capabilities, as well as capacities of partners to investigate and prosecute cybercrimes and engage on cyber diplomacy;
- Around **30 projects** in cybercrime & cybersecurity, including in the **Western Balkans** and in the **Eastern and Southern neighbourhood**.