MARCH 2022
#EUDefence
#StrategicCompass

CYBERSECURITY: 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**
- **Spreading online disinformation**
- **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 5 external policy areas:

LEADERSHIP ON INTERNATIONAL NORMS AND STANDARDS

- Diplomatic outreach & multilateral cooperation (e.g. United Nations)
- Confidence-building measures (e.g. OSCE, ASEAN Regional Forum)

PARTNERSHIPS AND INTERNATIONAL COOPERATION

- Dialogues with third countries & international organisations
- Exchanges with civil society, academics, private sector

EXTERNAL CYBER CAPACITY BUILDING

- Increase cyber resilience & capacities of partners to investigate and prosecute cybercrimes
- Around 20 projects in cybercrime & cybersecurity in the Western Balkans and in the Eastern and Southern neighbourhood

EU CYBER DEFENCE COOPERATION & CAPABILITY DEVELOPMENT INITIATIVES

- Developing an EU Cyber Defence Policy to be better prepared for and respond to cyberattacks
- Permanent Structured Cooperation (PESCO) projects (e.g. Cyber Rapid Response Teams will allow deployable teams to respond to cyber-attacks)

PREVENTING, DETERRING AND RESPONDING TO CYBER THREATS AND ATTACKS

- Use of the cyber diplomacy toolbox: political declarations, demarches, dialogues, sanctions
- In February 2022, following the Russian invasion of Ukraine with substantial cyberattacks, the EU has offered support to increase Ukraine's cyber resilience and defence, the PESCO Rapid Response Team has been activated to help Ukraine defend against cyberattacks