#EUDefenceIndustry
#StrongerEurope

NOVEMBER 2022
#EUDefence
#StrategicCompass

THE EU POLICY ON CYBER DEFENCE

Enhancing the EU's ability to prevent, detect, deter and defend against cyberattacks aimed at the EU and its Member States using all means available

WHY:

Cyberspace has become an increasingly contested strategic domain and a field for strategic competition

Cyber-attacks, espionage and disinformation campaigns targeting the EU and its Member States, including defence actors, are on the rise

Significant cybersecurity incidents can disrupt or damage critical infrastructure that our armed forces rely on

WHAT:

The EU Policy on Cyber Defence proposes to

- Increase cooperation among EU's cyber defence actors and develop mechanisms for leveraging capabilities at the EU level
- Boost our cyber defence capabilities, by individual Member States and through joint action
- Strengthen coordination and cooperation between military and civilian cyber communities to enhance more efficient crisis management within the Union
- Reduce our strategic dependencies in critical cyber technologies and strengthen the European Defence Technological and Industrial Base (EDTIB)
- Step up cooperation with our partners in the field of cyber defence
- Improve training, attracting, and retaining cyber talents

The EU Policy on Cyber Defence proposes several actions built around four pillars:

ACTING TOGETHER FOR A STRONGER EU CYBER DEFENCE

- Create an **EU Cyber Defence Coordination Centre** (EUCDCC) supporting enhanced situational awareness within the defence community
- Establish an operational **network for milCERTs** (Military Computer Emergency Response Teams) - **MICNET**
- Develop and strengthen the **EU Cyber Commanders Conference**
- Develop a **new framework CyDef-X project to support EU cyber defence exercises**
- Strengthen common EU detection, situational awareness and response capabilities through the **EU civilian infrastructure of Security Operation Centres (SOCs)**
- Establish a mechanism to gradually **set-up an EU-level cyber reserve** with services from trusted private providers
- Support **testing of critical entities** for potential vulnerabilities based on EU risk assessments

SECURING OUR DEFENCE ECOSYSTEM

- Develop **non-legally binding recommendations for the defence community**, inspired by NIS2, to contribute to an increased overall cyber defence maturity at national level
- Develop **recommendations on EU cyber defence interoperability requirements**
- Develop **risk scenarios for critical infrastructure** of importance to military communication and mobility
- Foster **cooperation between civilian and military standardisation bodies** for the development of harmonised standards for dual use products

INVESTING IN OUR CYBER DEFENCE CAPABILITIES

- Develop a **technology roadmap for critical cyber technologies for the EU** covering critical technologies for cyber defence and cybersecurity to assess the level of dependencies
- Develop **Emerging Disruptive Technologies (EDTs) Strategic Assessment** to support long term strategic investment decisions of Member States
- Develop **the ESDC Cyber Education, Training, Exercises and Evaluation (ETEE) platform** to generate more training capacities
- Establish an **EU Cyber Skills Academy,** considering specific skills needs for different professional profiles and sectors of activity, including the defence sector

PARTNERING TO ADDRESS COMMON CHALLENGES

- Strengthen **EU-NATO cooperation** in the field of cyber defence training, education, situational awareness and exercises
- Progressively **include cyber defence topics in EU-led dialogues**
- Increase assistance to partners through **cyber defence capacity building**