
Hybrid CoE
Partners in security
Analyze. Inform. Train.

Overview of Hybrid CoE and Recent Hybrid Threats

The European Centre of Excellence for Countering Hybrid Threats

- Inaugurated in 2017 by 9 EU/NATO countries (FI, UK, DE, FR, SE, US, LT, LV, PL)
- Now 35 Participating States – EU MS and NATO Allies
- EU and NATO close stakeholders
- International secretariat in Helsinki (50 staff)
- Annual budget approximately 5,0 M€
- Strategic, independent & policy-relevant

→ ***International hub of experts with networks across the Euro-Atlantic***

Hybrid CoE

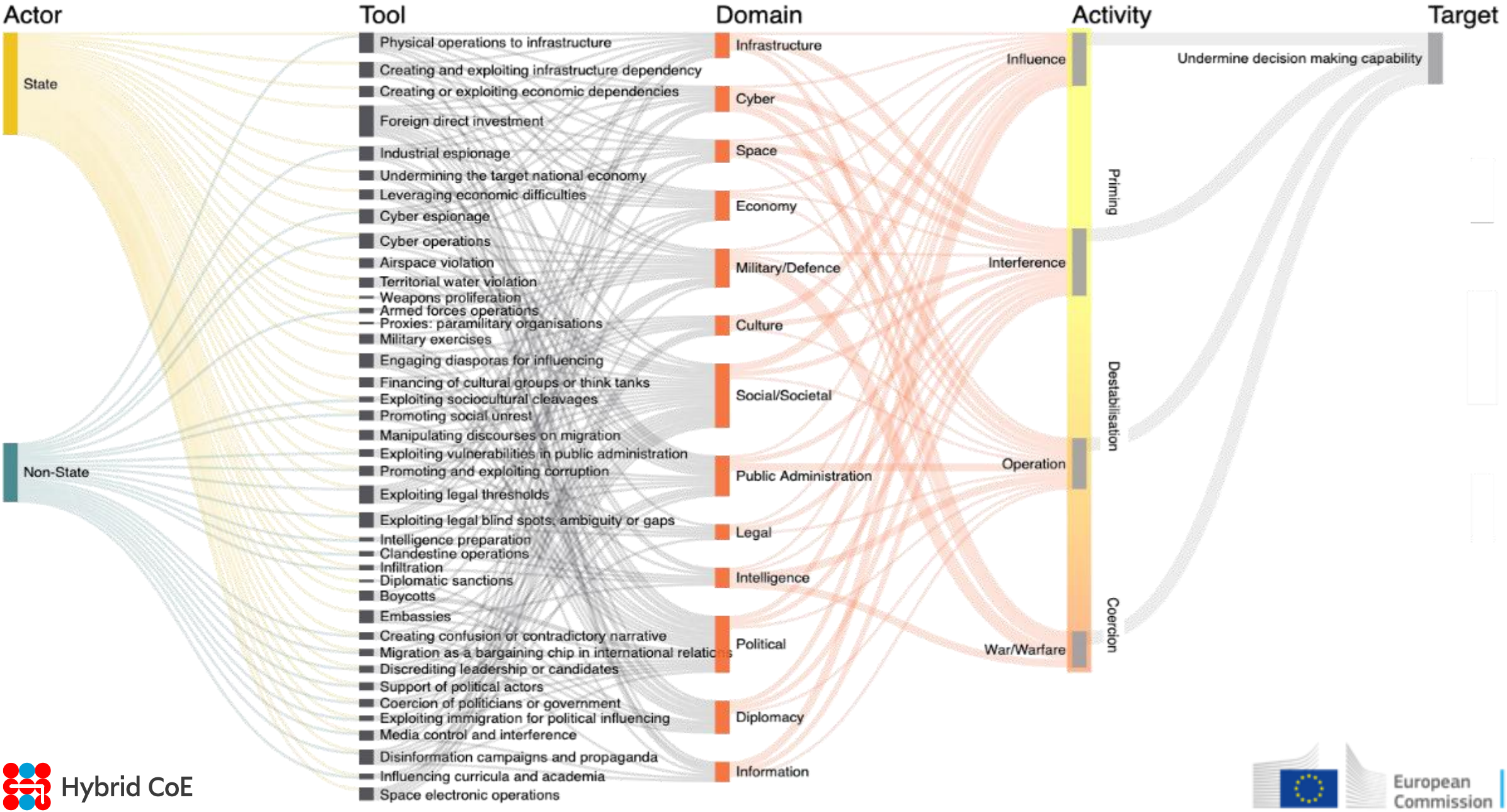
Our objectives

- Strengthen the capacities of our Participating States to counter hybrid threats
- Foster EU-NATO cooperation
- Increase awareness & lead discussion

Hybrid threats: A new way to describe old threats in a new environment

- Coordinated and synchronised actions using a wide range of means
- Targeting states' and institutions' systemic vulnerabilities
- Exploiting the thresholds of detection and attribution
- Exploiting borders between war and peace
- Targeting democratic values, principles and institutions

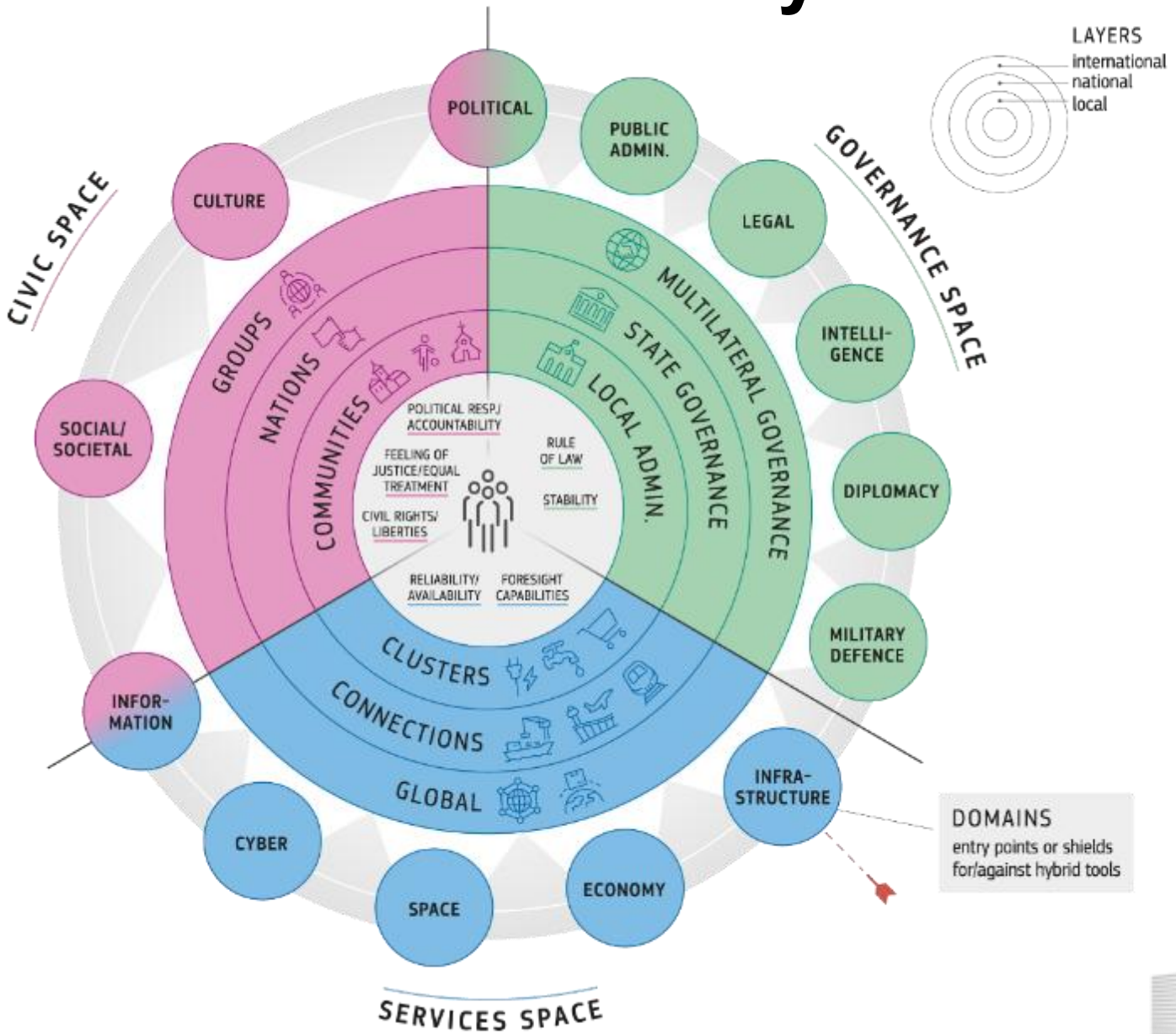
The Landscape of Hybrid Threats – A Conceptual Model



Hybrid CoE

European Commission

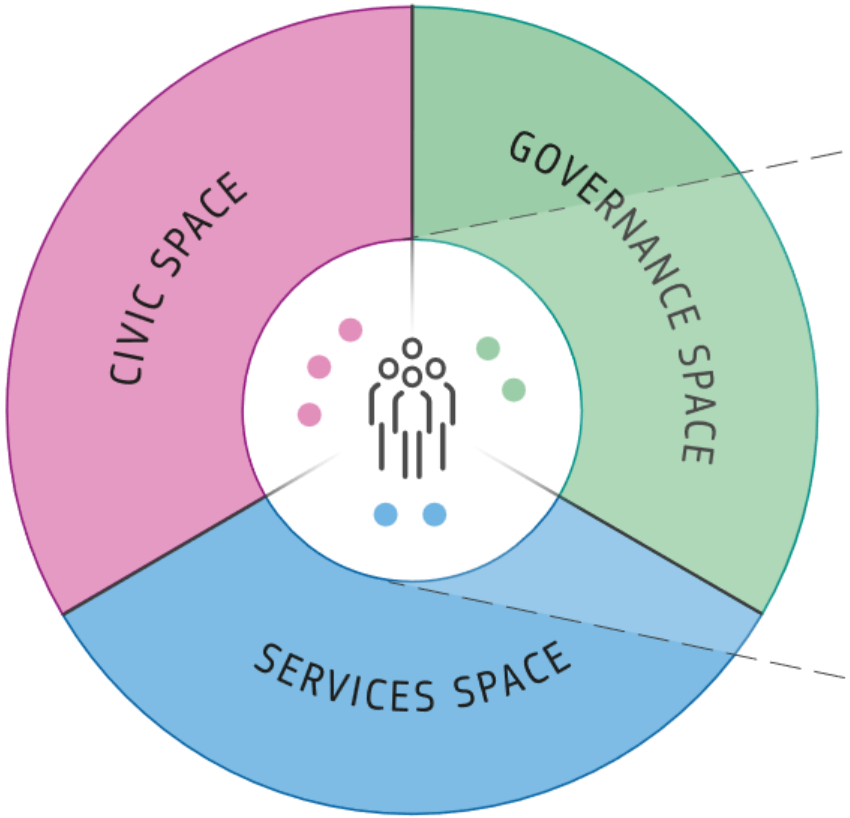
Comprehensive Resilience Ecosystem



Hybrid CoE

European Commission

Foundations of democracy: ultimate targets

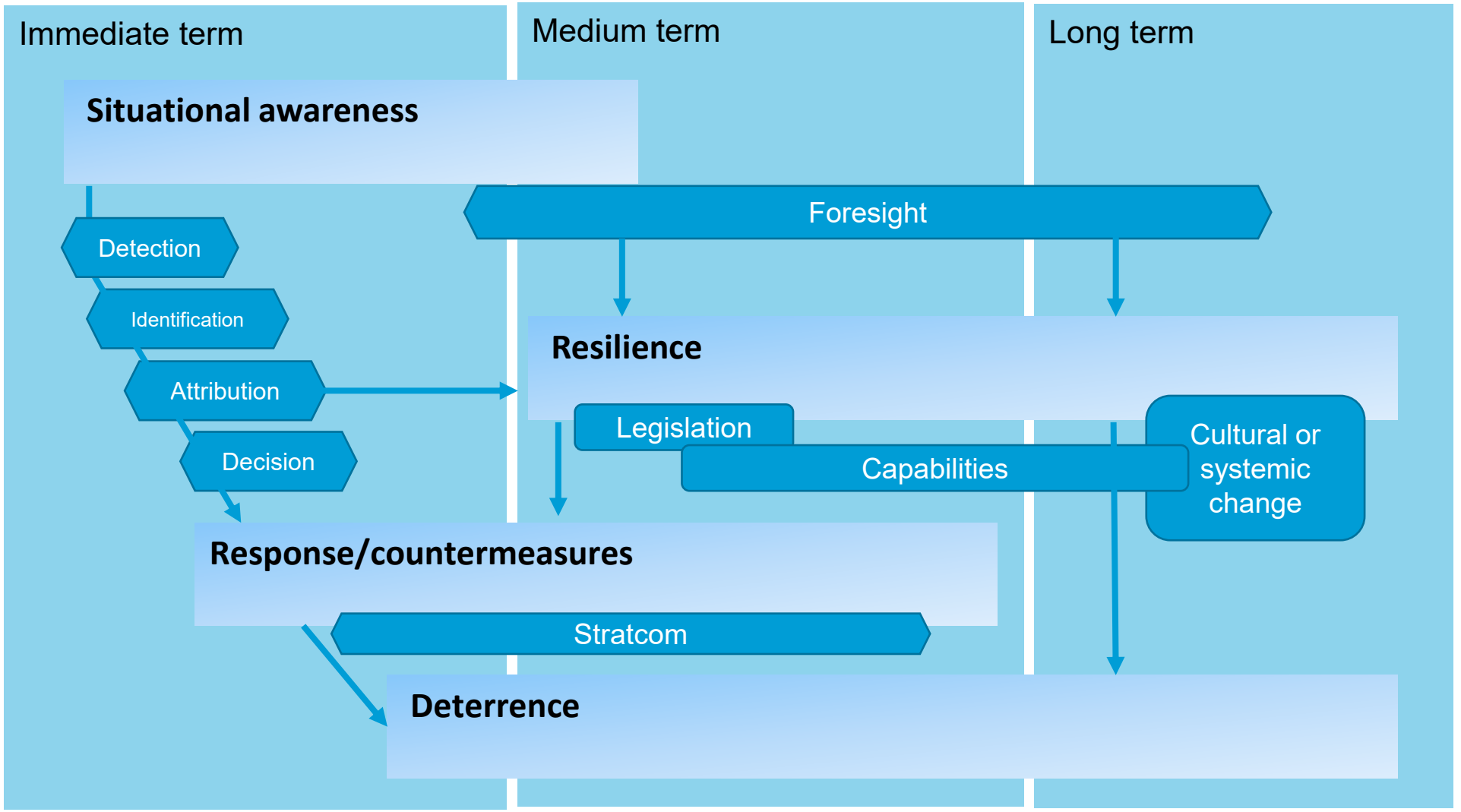


CORE FOUNDATIONS OF DEMOCRACY

- Feeling of justice and equal treatment
- Civil rights and liberties
- Political responsibility and accountability
- Rule of law
- Stability
- Reliability / availability
- Foresight capabilities

Responding to hybrid threats

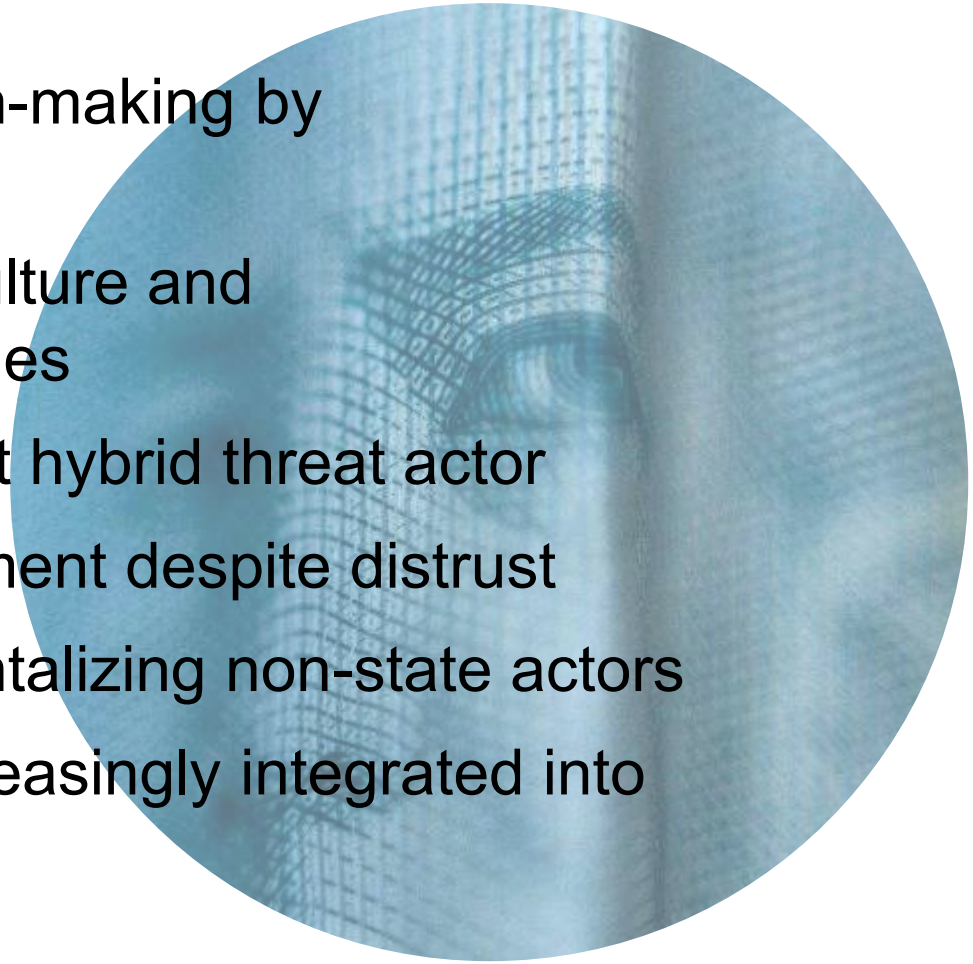
Hybrid CoE



Recent hybrid threat trends

Intensity and hostility increasing – new states adopting hybrid tools

- Russia manipulating Euro-Atlantic decision-making by escalation of hybrid threats
- Russia targeting elections, weaponizing culture and history and exploiting strategic dependencies
- China solidifying its role as an omnipresent hybrid threat actor
- Hybrid threat actors deepening their alignment despite distrust
- Hybrid threat actors increasingly instrumentalizing non-state actors
- Advanced and emerging technologies increasingly integrated into hybrid threats



Hybrid CoE

Cyber and Hybrid Threats

Cyber Related Hybrid Threats

- Direct cyber attacks
  - DDoS
  - Ransomware
  - Cyber espionage
  - Wipers
- Attacks that indirectly affect cyber
  - Disinformation campaigns
  - Attacks on critical infrastructure
    - Energy
    - Communications

Recent examples

Hybrid CoE

Russian actors use various cyber realated measures

- Targets
  - Critical infrastructure
  - Under-sea cables
  - Politicians and Elections infrastructure
- Methods
  - Hacktivists and non-state actors
  - Shadow fleet
  - AI and emerging technologies

Hybrid CoE

Iran conducts a coordinated cyber campaign targeting multiple countries worldwide

- Multiple threat actors
- 20+ countries reported attacks
  - Israel
  - Gulf states
  - Beyond:
    - Asia, North America, Europe, Africa
- Attacks on governments, high-ranking officials, financial sector, critical infrastructure, defence industry

Hybrid CoE

AI democratizing advanced cyber capabilities

Automated phishing campaigns

Mass surveillance through compromised security cameras

Coordinated DDoS attacks

Hybrid CoE

Use of AI in Hybrid Operations

- Generative AI has reportedly been used by multiple actors
  - Information operations
  - Reconnaissance
  - Malware creation
  - Automation of various tasks
- Usage of AI in kinetic attacks may be less obvious

It can be difficult to assess when AI has been used in hybrid operations

Hybrid CoE

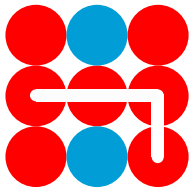
North-Korean cyber attacks

- Offensive operations used to fund the state
- Ransomware
- Supply-chain attacks
- IT workers

Hybrid CoE

North Korean IT workers

- Using generative AI for:
  - Job interviews
  - Performing their jobs
- Lowers the barrier of entry
  - The IT workers do not need much prior training
- The salary goes to fund the DPRK



Hybrid CoE

Partners in security
Analyze. Inform. Train.