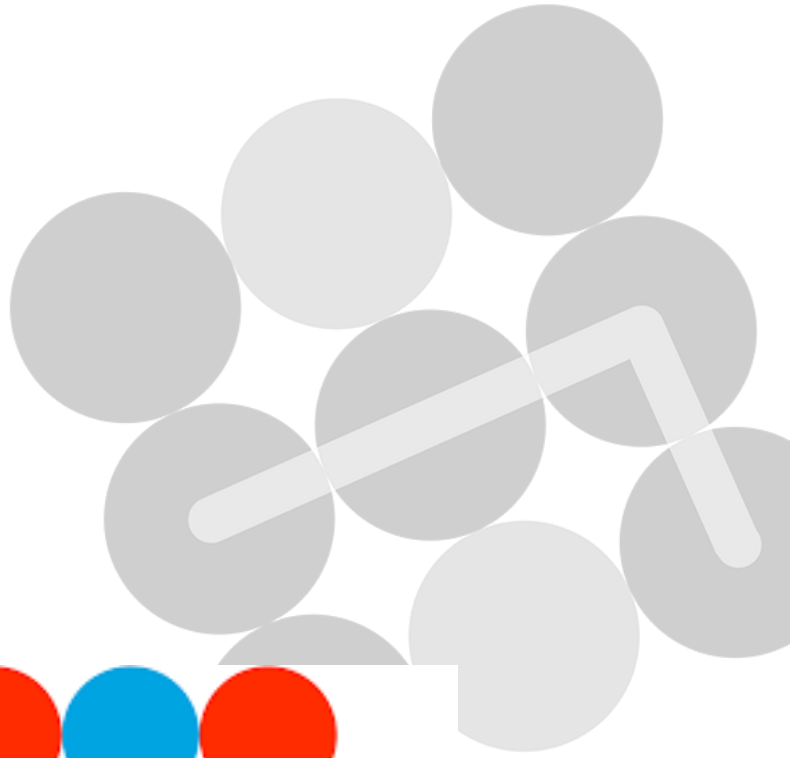
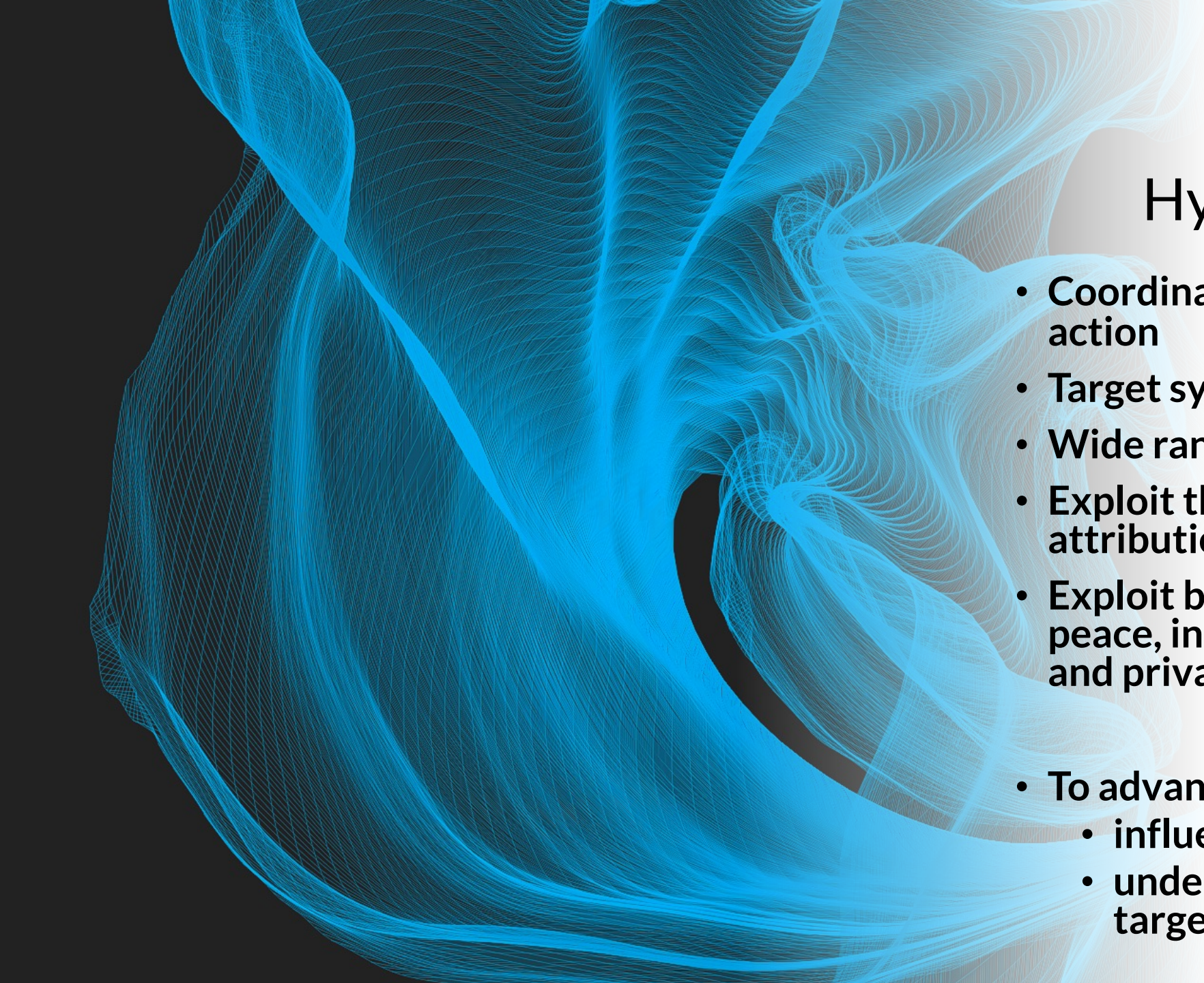
Dr. Josef Schroefl, CoI
Mobile +358 40 5540482
josef.schroefl@hybridcoe.fi
www.hybridcoe.fi

- Inaugurated in 2017 acc. Joint Framework on countering hybrid threats from 2016
- Currently 34 member states (last was Bulgaria)
- Secretariat (atm 45)
- CoI´s network: appr. 800
- Annual budget 4,2M€. Host country FI funds half of the core budget, half comes from the PS
- First and (until now) only EU/NATO entity



Hybrid CoE

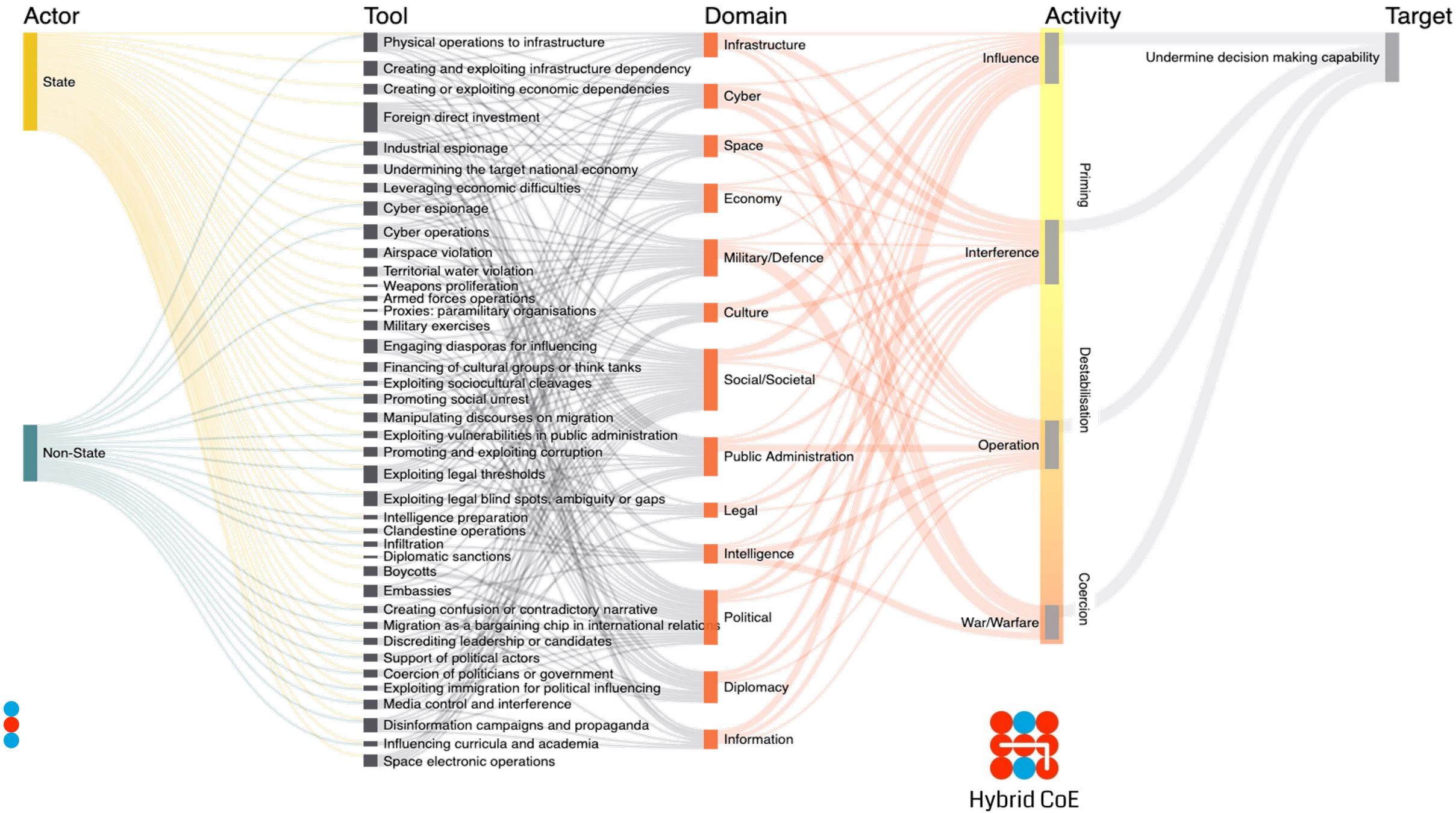
Hybrid CoE



Hybrid threats

- **Coordinated and synchronised action**
- **Target systemic vulnerabilities**
- **Wide range of means**
- **Exploit thresholds of detection and attribution**
- **Exploit borders between war and peace, internal and external, public and private**

- **To advance strategic objectives by**
  - **influencing decision-making**
  - **undermining and/or hurting the target**


Actor
Tool
Domain
Activity
Target
State
Non-State
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Influence
Interference
Operation
War/Warfare
Priming
Destabilisation
Coercion
Undermine decision making capability

Hybrid CoE

The European Centre of Excellence for Countering Hybrid Threats

Hybrid CoE

- **Strategic**
- **Independent**
- **Policy-relevant**

- ***Increase awareness***
- ***Share best practices***
- ***Facilitate networking***
- ***Lead discussion***

Communities of Interest (COIs)

- COIs are networks of practitioners (or researchers) from Member States and institutions
- COIs for multidisciplinary sharing of best practice, experience and expertise for participants to better understand, defend against and respond to Hybrid threats
- Space to coordinate action
- Intellectual matchmaking
- Multidisciplinary approach

Network based approach

Workstrands in 2022

COI HI

- Deterrence
- Safeguarding democratic processes
- Non-State Actors

COI V&R

- Resilience
- Maritime hybrid threats
- Economy
- Instrumentalized migration
- Aviation and Space

COI S&D

- StratDoc Analysis
- CPH/Cyber
- HYFUTEC
- Hybrid warfare, Strategy and defence

R&A

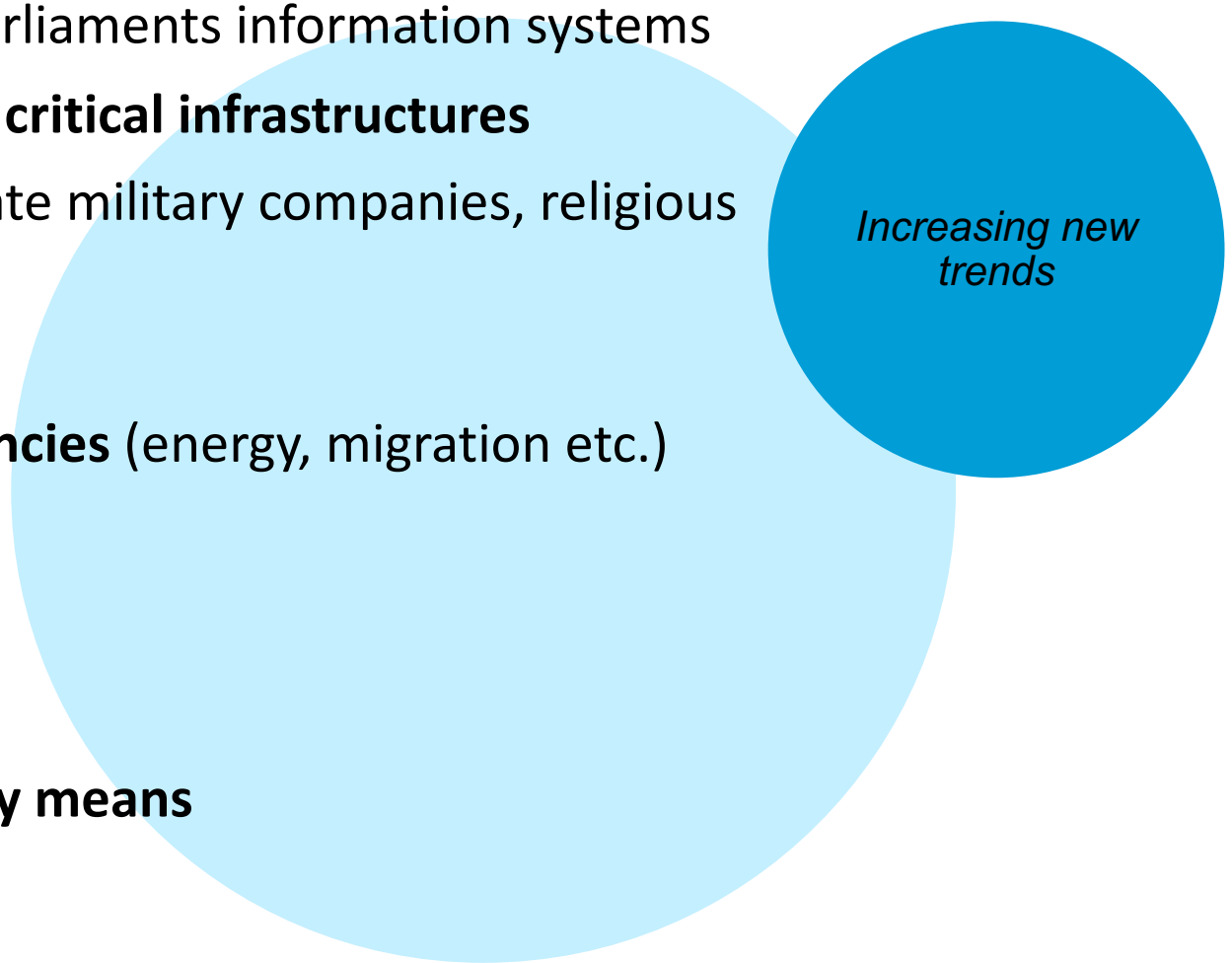
- Strategic Insights: Emerging trends and challenges, Regional studies and Domain studies
- Seeing Red
- Building Resilience
- External partnered projects (HYBNET, Resilient Civilians)

T&E

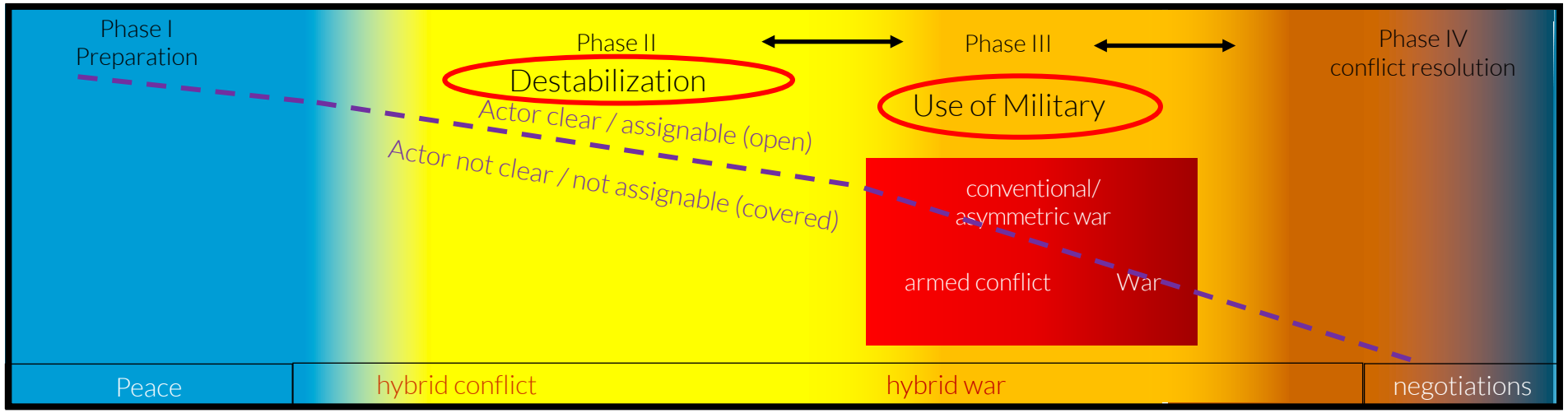
- Support to NATO & EU exercises
- Support to COIs and R&A
- Capacity building for Participating States

Recent trends

- **Hacking of Western** governments' and parliaments information systems
- Increasing **foreign ownership of Western critical infrastructures**
- Enlarging **forms of non-state actors** (private military companies, religious communities etc) used **as proxies**
- **Increasing use of 'lawfare'**
- **Weaponizing commodities and dependencies** (energy, migration etc.)
- **Economic coercion**
- Disturbances in **critical infrastructure**
- **Polarization driven by disinformation**
- Leveraging and normalizing use of **military means**
- **Individuals as targets/tools**



Environment of hybrid Crisis/Conflict/War



Use of as much as possible Power in all Domains
Infrastructure, Cyber, Space, Economy, Military, Culture, Social, Public Admin., Legal, Intelligence, Diplomacy, Political, Information

by (exemplary list):
Extortion, media oppression, political isolation / ostracism, propaganda, boycotts of trade, financial speculation, monetary policy, influencing or restricting social media and the Internet, use of conventional, subconventional warfare through legal / illegal forces, cyber and information warfare, use of terror and crime, etc.

Threat environment drivers

Globalization

Competition

New Technologies

- Globalization and the changes in world order
- Increasing strategic competition
- Democratization of conflict/warfare
- Role of new technologies
- COVID-19
- War in Ukraine

➢ Conflict and competition

➢ Implications for deterrence

Hybrid CoE Project: Cyber Power in Hybrid Conflict/Warfare (I)

Whole of society/state-approach?

An underlying question is, whether the existing Cyber Crisis Coordination mechanisms can contribute to Hybrid Crisis-Coordination mechanisms on a "Whole of State/Society Approach?

Breaking the Dominance of other Domains?

Can Cyber Power break the dominance of the other domains and eventually become the dominant Domain?

Can a first strike in the Cyber Domain decide a war/battle?, - is a Cyber-"Blitzkrieg" possible?

Outcome: Main points (I)

EU and NATO have established a good basis to counter cyber and hybrid threats, but it´s still not enough. Much more EU/NATO coop. is needed!

Cyber is inherent in all domains but the cyber domain is as important to protect as land, sea, air and space but the difference is, - it´s man-made

Cyber has become a part of collective security. Therefore, - **national Cyber crisis management mechanisms could be used also against hybrid threats**, but that needs a comprehensive, whole-of-state/society cooperation/approach

Cyber-Blitzkrieg is theoretically already possible, - practically not. But the **growth of new technologies** have the capacity to shape public opinion as well as to increase the importance of the cyber-domain. It is easy to predict, **that Cyber Power becomes more dominant** then now.

Conclusions

- All have vulnerabilities and weak spots – what are yours?
- Rational and intellectually honest analysis is required
- Dialogue with the people is essential – listen carefully, raise awareness
- Corner stones of democracy challenged: elections in special focus; freedom of speech, rule of law
- Comprehensive All-govt – inter-institutional approach vital; Hybrid CoE as a catalyst
- Demand for joint actions, joint training and beyond borders cooperation

“The contribution of Cyber in Hybrid Conflict” 11 – 15 September 2023, Hybrid CoE/EDA Helsinki/FIN

Content:

- key elements of cyber defense and hybrid threats,
- training for understanding cyber threats in hybrid campaigns
- networking + exchange across communities
- Intensive exercise part exploring the dynamics of cyber-hybrid interactions

Hybrid CoE/EDA future Project: Cyber Power in Hybrid Conflict/Warfare

The cyber- and hybrid aspects of cognitive warfare ?

- Is cognitive warfare equivalent to information warfare, or broader, like cyber warfare? What are the differences?
- Can cognitive warfare be countered by means of cyber defence, or do we need an additional cognitive defence with cyber elements?
- How are instruments of cognitive warfare combined with other hybrid threat instruments in operations against Western societies?

Outcome: Main points (II)

in the era of cyber warfare, it is also essential to understand the effects of cognitive elements. Adversaries are intent upon influencing us and our thinking to penetrate decision-making circles, whether focused on energy-related decisions, applying for NATO membership, elections or something else.

It also means that economic and national security are now two sides of the same coin. To destabilize democratic states, hybrid threats are employed in cyber operations, information warfare, cyber-enabled disinformation operations, foreign direct investment, as well as in social media to manipulate large numbers of people.

Sovereignty will duly take on a new meaning. Consequently, not only land borders have to be defended but also the cyber and information space, as well as the control of data.

Questions ?

Dr. Josef Schroefl, Col
Mobile +358 40 5540482
josef.schroefl@hybridcoe.fi
www.hybridcoe.fi