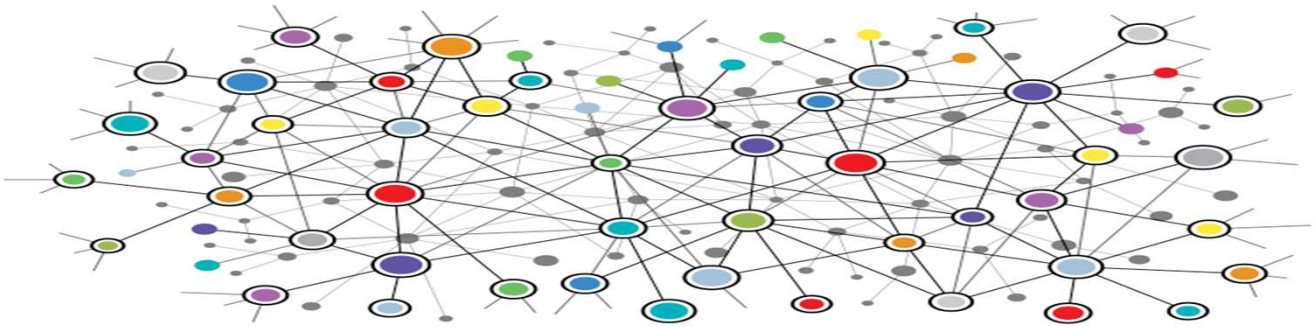
A4: Special Issues in Energy, Environment and Climate Change

HYBRID THREATS & ENERGY SECURITY

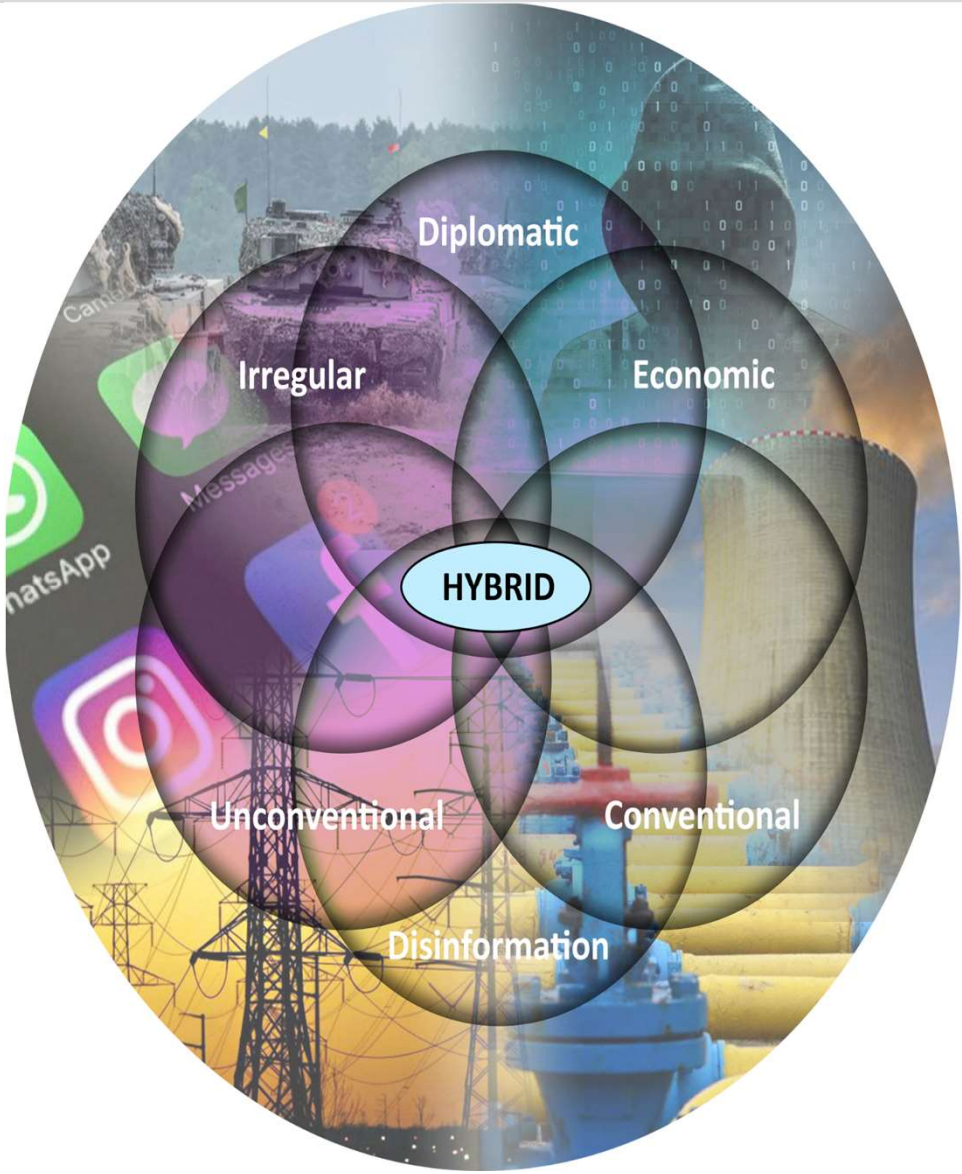
Andrew Liaropoulos
Associate Professor

6/12/2025



Structure

- **Introduction**
- **Defining the hybrid environment**
- **Hybrid threats to the energy sector**
- **Countering hybrid threats to the energy sector**
- **Conclusion**



Introduction

Questions:

- **How do hybrid threats affect the energy sector?**
- **How can we counter hybrid threats to the energy sector?**
- **How can we enhance resilience in the energy sector?**

Goal: Holistic understanding of the full spectrum of hybrid threats to the energy sector and ways to counter such threats.

Defining the hybrid environment

- **Semantics are important:** hybrid war / conflict / campaign…threats

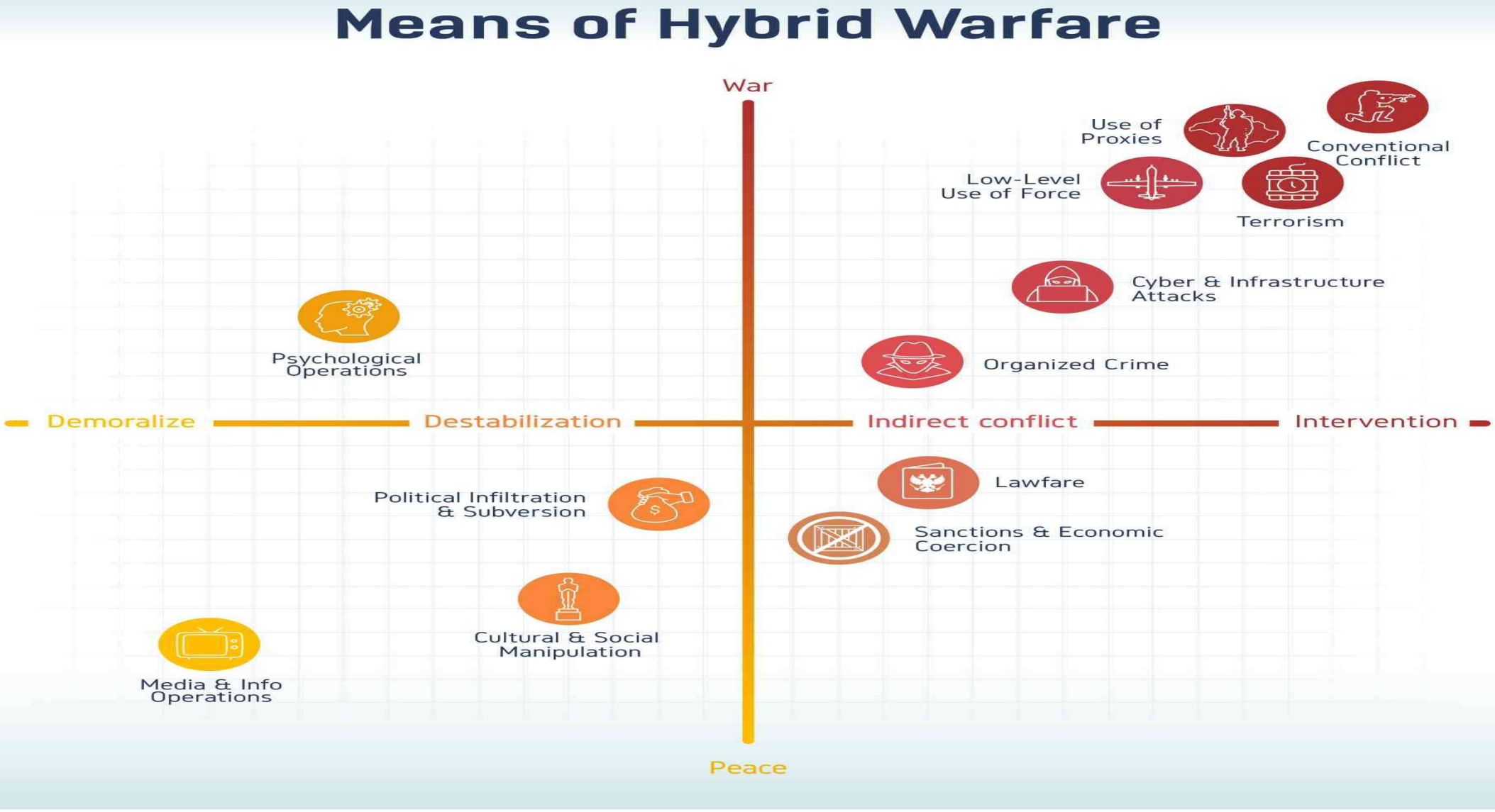
- **Hybrid** refers to a combination or mixture of two or more distinct elements, typically resulting in something that incorporates both qualities or characteristics. The specific meaning of ***hybrid*** depends on the **context** in which it is used.

Definition of hybrid threats

NATO: 'broad, complex, adaptive, opportunistic and often integrated combinations of conventional and unconventional methods.' According to NATO, 'these activities could be overt or covert, involving military, paramilitary, organized criminal networks and civilian actors **across all elements of power**.'

EU: a 'mixture of coercive and subversive activity, conventional and nonconventional methods (i.e. **diplomatic, military, economic, technological**), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare'.

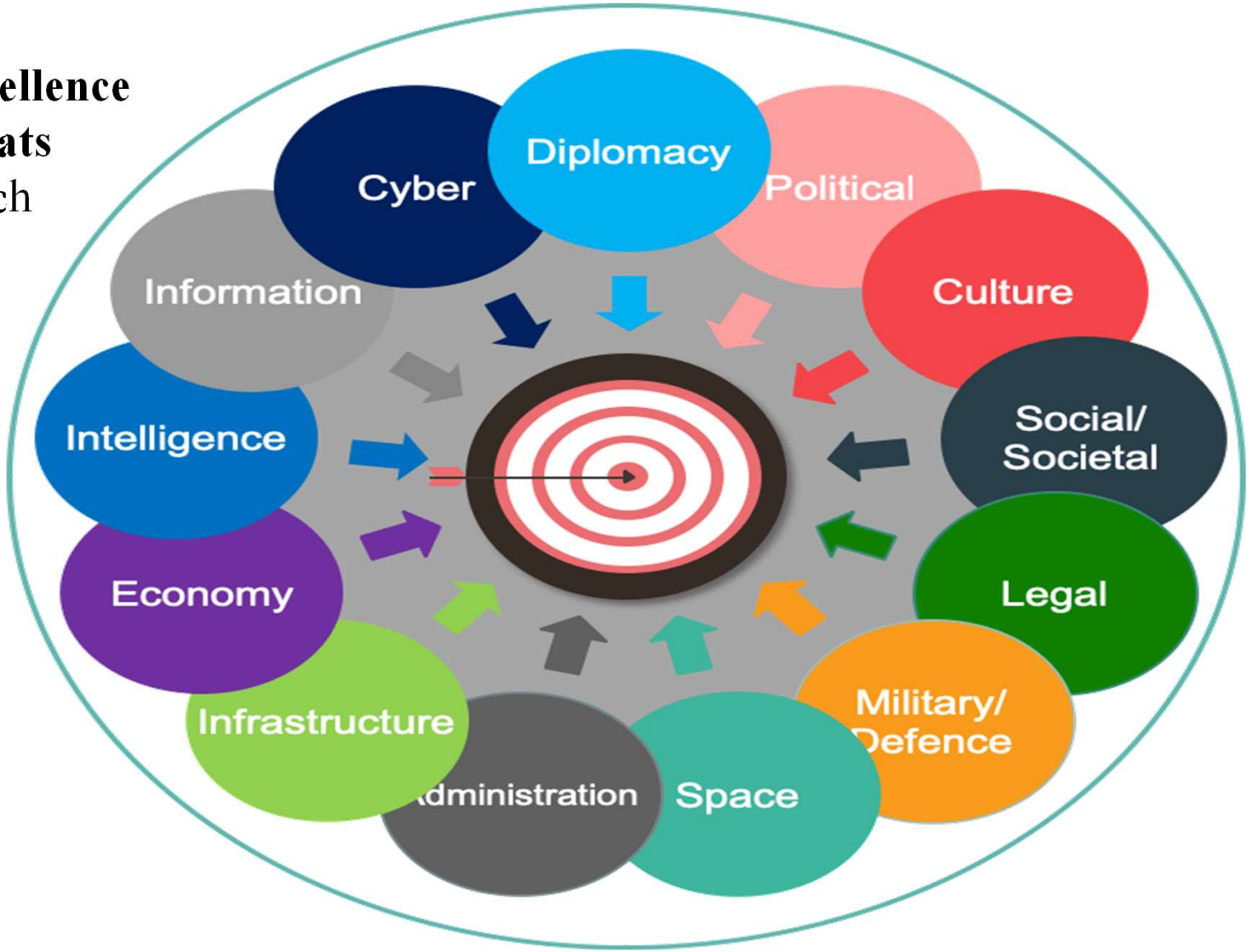
Defining the hybrid environment



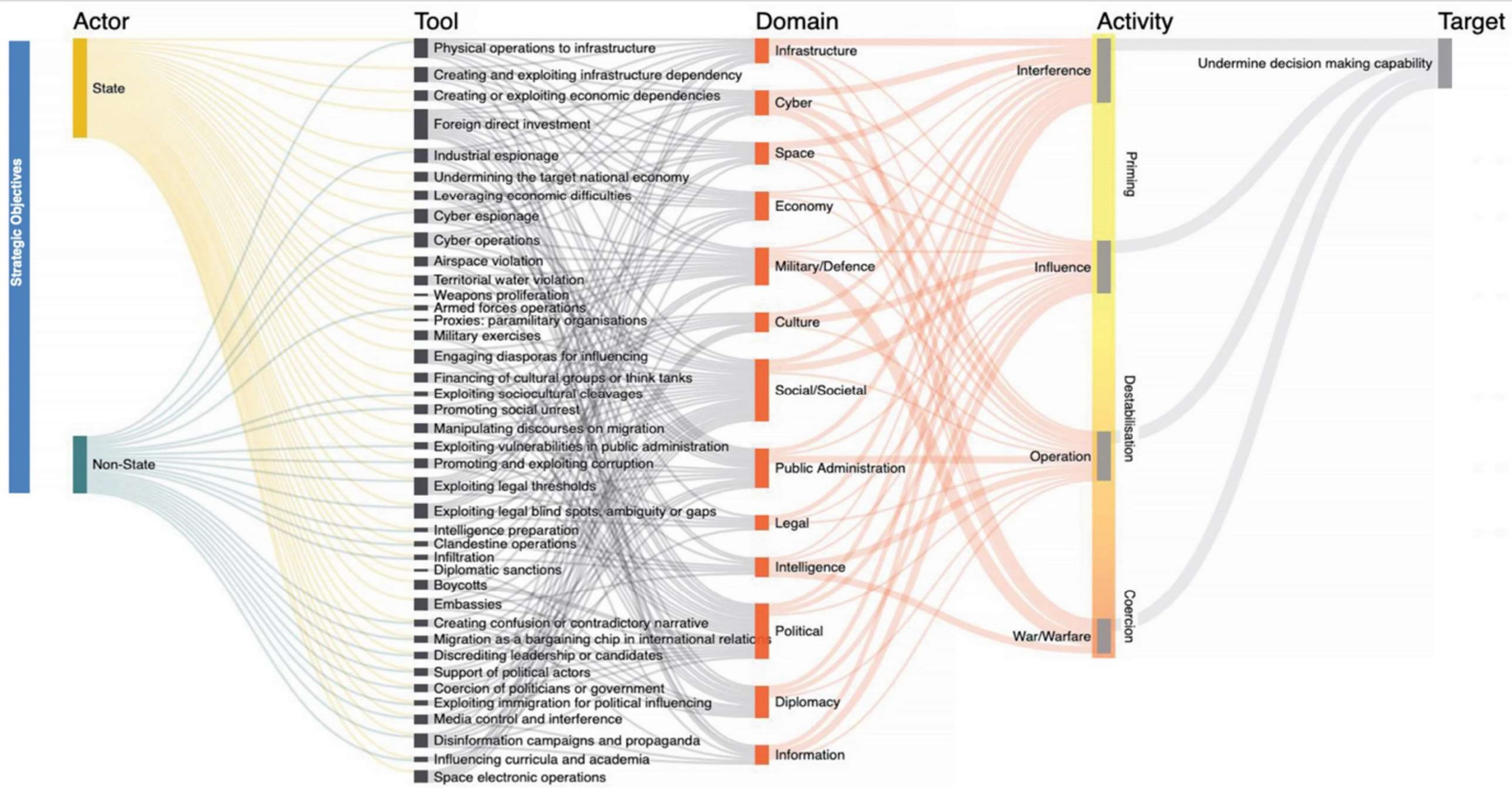
Defining the hybrid environment

The **European Centre of Excellence for Countering Hybrid Threats** offers **13 domains** across which hybrid threats can materialize.

Hybrid CoE



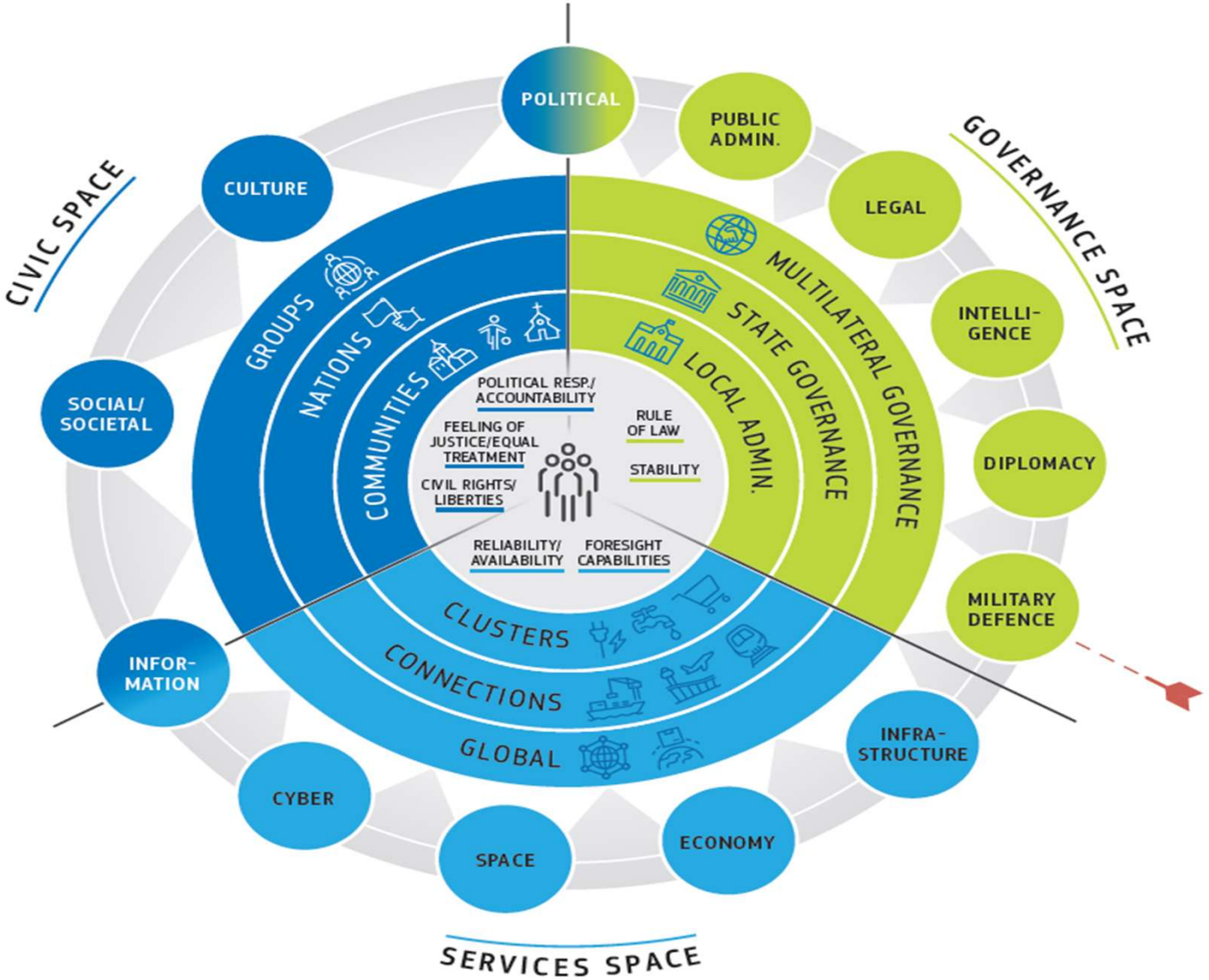
Defining the hybrid environment



Defining the hybrid environment

‘Hybrid is the dark reflection of our comprehensive approach.
We use a combination of military and non-military means to stabilize countries.
Others use it to destabilize them.’

NATO Secretary General
Jens Stoltenberg, May 2015



Hybrid Threats to the Energy Sector (Scenarios)

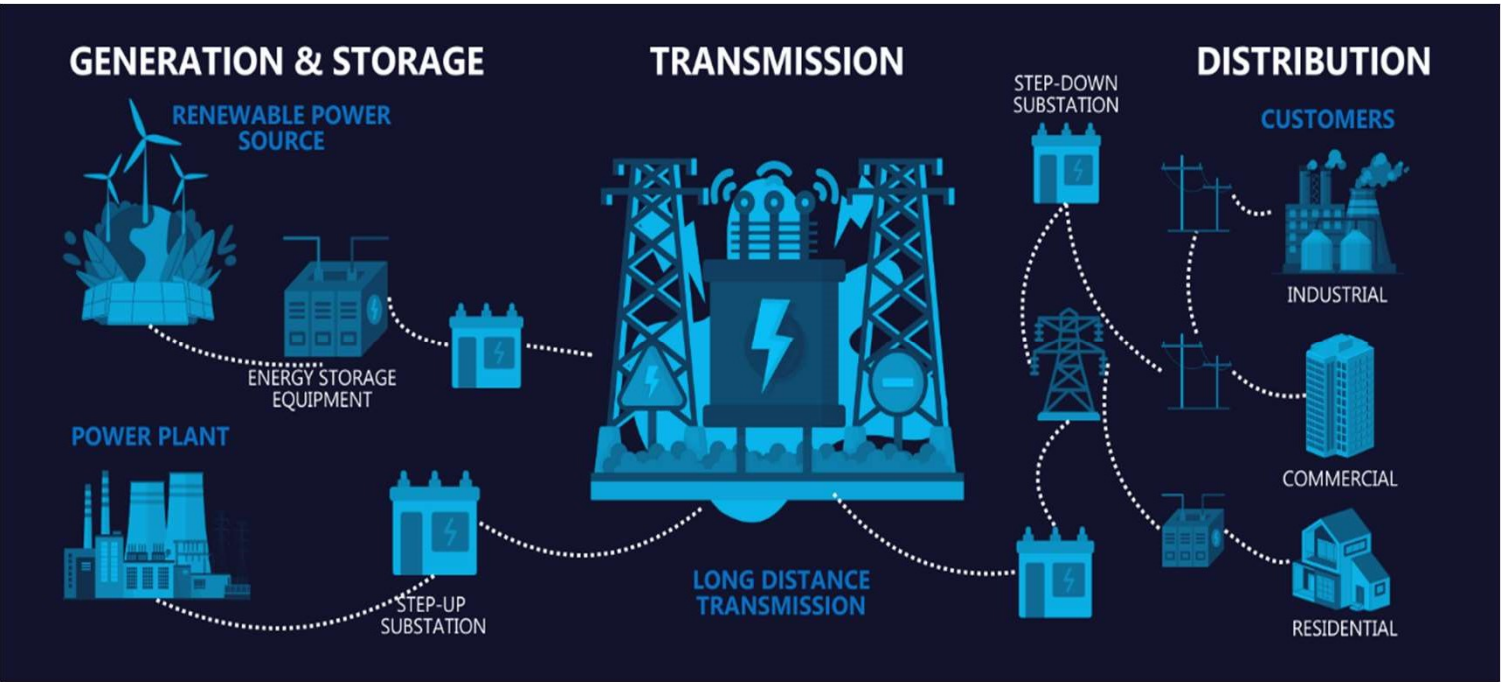
Actor	Tools	Domains	Activities	Target
State	Cyberattack / Ransomware	Infrastructure	Operation	Disrupt energy flow
Non-state	Physical Sabotage	Infrastructure	Operation	Destroy infrastructure, Disrupt energy flow
Non-state	Disinformation Campaign	Information	Influence / Interference	Undermine decision making capability, Undermine trust

Cyber-operations / cyber-tools

Goal: Disrupt energy infrastructures, undermine / delay energy projects, access to critical data

Methods: Ransomware, Malware, DDoS attacks, cyber-espionage, etc.

Examples: Stuxnet, Saudi Aramco, Black Energy, SolarWinds, etc.



Disinformation and Information Manipulation

Goal: Influence public opinion, delay projects, undermine trust

Methods:

- Coordinated campaigns to spread false narratives about the safety or environmental impact of energy infrastructure (e.g., pipelines, LNG terminals, nuclear plants).
- Amplifying local opposition groups to create social division around energy projects.
- Misrepresenting the causes of energy price increases, to provoke political pressure.

Examples:

- **Disinformation around nuclear energy in Europe:** European security agencies have reported state-backed media outlets amplifying misleading narratives about nuclear safety to increase public opposition to new reactors. **Goal:** delay nuclear expansion, increase reliance on externally supplied fossil fuels, and exploit societal divisions.
- **Polarized narratives on wind farms:** In several EU countries, disinformation campaigns have framed offshore wind projects as harmful to ecosystems or maritime livelihoods. Intelligence reports indicate the amplification often originates from actors whose geopolitical interests benefit from slowing renewable deployment.

Economic Coercion and Market Manipulation

Goal: Undermine energy security or political stability

Methods:

- A state-controlled energy supplier suddenly altering gas or oil delivery volumes to exert political pressure (e.g. Russia's Gazprom, Ukraine).
- Manipulating energy supply contracts or offering preferential pricing to create dependency on a single supplier. (e.g. Russia-Belarus preferential gas pricing).
- Buying strategic stakes in foreign energy companies or infrastructure to gain leverage (e.g. Rosneft extended billions of dollars in loans to Venezuela's state oil company, PDVSA, in exchange for access to key oil fields, Russia's Gazprom purchasing parts of European gas storage and pipeline networks).
- Foreign direct investment can lead to profound dependencies and vulnerabilities of the state concerned. It can enable a hostile actor to gain access to sensitive information, such as network structures and sensitive technologies (e.g. China General Nuclear (CGN) investment in UK Nuclear Power Projects).

Economic Coercion and Market Manipulation

Examples:

- **Gas Supply Manipulation (Europe, 2021-2022):** A major state-owned supplier reduced volumes through specific pipelines during periods of high demand. **Result:** heightened price volatility, political pressure on energy-importing nations, and public concern about energy security. Widely described in EU energy-security reports as a hybrid coercive tactic.

- **Strategic Investments in Critical Energy Infrastructure:** State-linked companies purchasing stakes in foreign grid operators, ports, or energy storage facilities. The strategic objective: long-term leverage over essential infrastructure and political influence.

- **Exploiting infrastructure dependency:** A state can abuse its dominant market position and ownership of energy supply to support foreign policy objectives (energy blackmail, e.g. EU-Russia-Ukraine).

Physical Sabotage or Covert Disruption

Goal: Disrupt energy cycles, raise costs, or reduce public confidence

Methods:

- Interfering with supply chains (e.g., components for grid equipment) to degrade reliability.
- Encouraging vandalism or orchestrating low-tech disruption of power lines, transformers, or fuel transportation routes.
- Interfering with maritime chokepoints that impact LNG shipping or oil transport (e.g. Iran, Strait of Hormuz).
- Covertly supporting environmental disruptions (e.g., forest fires) that affect transmission corridors (e.g. PKK-related sabotage on the Kirkuk-Ceyhan oil pipeline).
- Disrupting transportation networks (rail, ports, trucking) that deliver fuels or essential equipment.

Physical Sabotage or Covert Disruption

Examples:

- **Pipeline Infrastructure Damage:** Several incidents involving non-cyber physical interference with natural gas pipelines and offshore energy assets have been investigated by European states. Although attribution is often uncertain, such actions are treated as potential hybrid threats aiming to undermine trust in supply security.

- **Disruption of Rail and Fuel Logistics (Ukraine & Eastern Europe):** Interference, sometimes through local proxies, with rail lines carrying energy commodities has been documented over years of conflict. **Goal:** create shortages, raise operational costs, and complicate national resilience.

Lawfare / Regulatory Manipulation

Goal: Shape energy policy or regulatory outcomes, delay or block critical projects

Methods:

- Coordinated legal challenges to delay construction of energy facilities (e.g. environmental organizations lawsuits, Atlantic Coast Pipeline, US & Trans Mountain Pipeline expansion, Canada).
- Use of international arbitration mechanisms to pressure states over contracts or environmental statutes.
- Large LNG terminals, interconnectors, or pipelines have faced simultaneous legal challenges filed by groups later linked (indirectly) to foreign influence networks.

* **Lobbying or covert influence efforts** to push favorable regulations, delay renewable-energy adoption, or obstruct diversification. Such tactics can delay projects for years, increasing dependency on external suppliers.

Weaponization / Manipulation of everything…

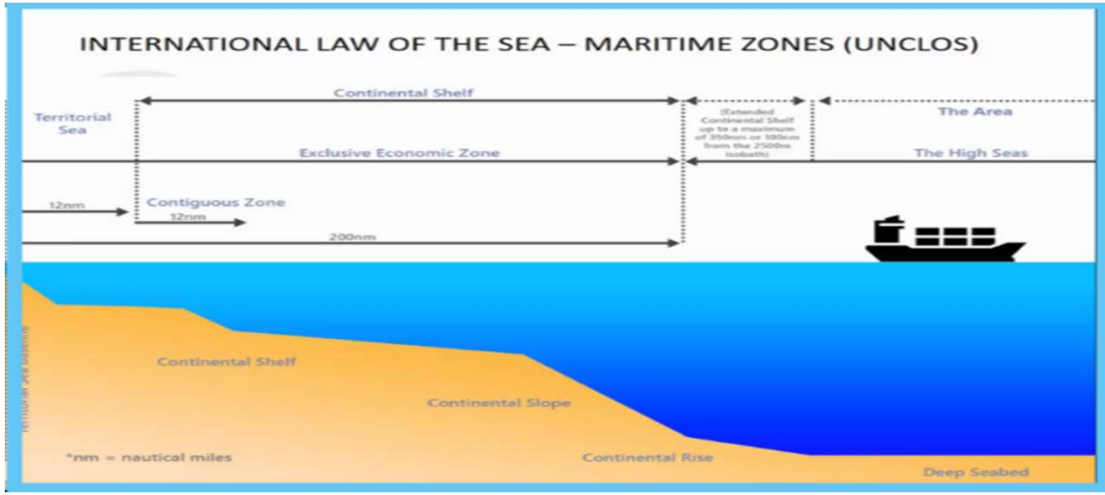
Goal: create political pressure, undermine energy projects, and cause operational challenges.

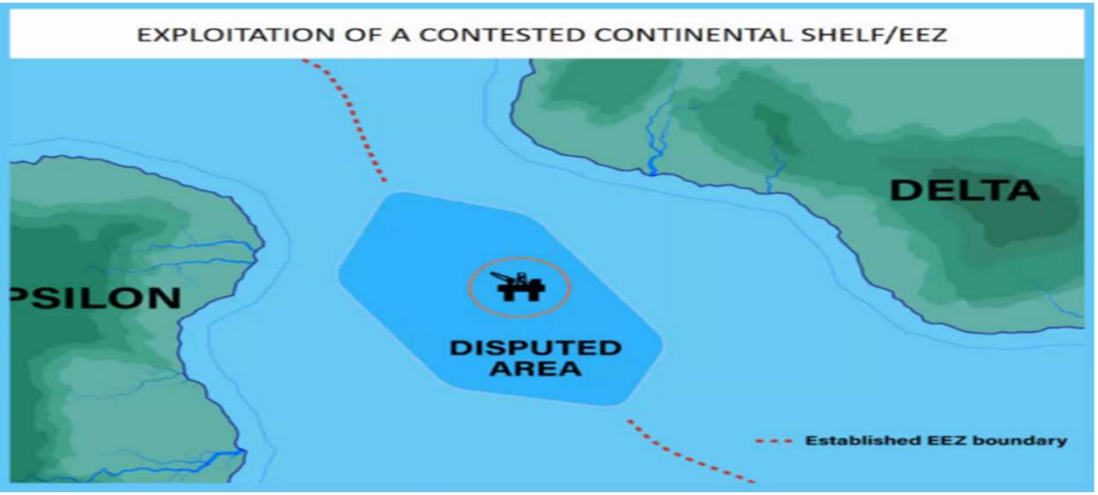
Methods:

- **Conduct industrial espionage**: spying on energy infrastructure and its vulnerabilities by different means as well as stealing sensitive research results on new energy technologies or datasets.
- **Using orchestrated migration flows** to destabilize areas where key energy infrastructure is located, complicating security and logistics.
- **Manipulating shared water resources** crucial for hydroelectric plants or cooling systems in thermal/nuclear power stations.
- In regions with shared river systems, upstream countries have occasionally **altered water flow** at politically sensitive times, pressuring downstream states with hydropower dependencies.
- **Funding front groups or NGOs** that indirectly align with the adversary's geopolitical interests.

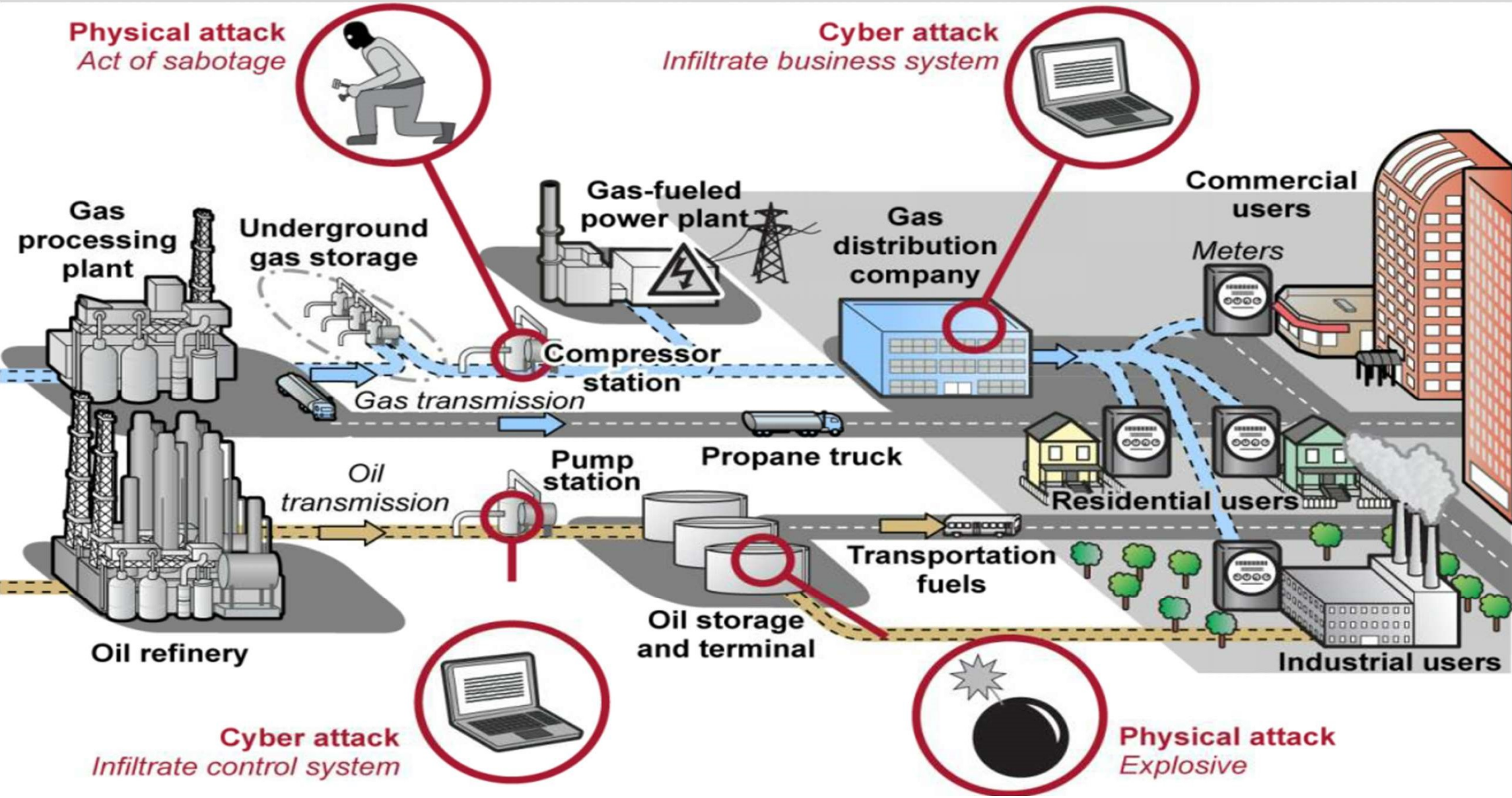
Weaponization / Manipulation of everything…

- **Airspace / Territorial water violation:** Airspace or territorial water violation can be defined as an unauthorized intrusion into the water or air borders of a country. A hostile actor uses this tool to test the detection and response capabilities of the targeted country, as well as to test the boundaries. Energy infrastructure are sometimes intrinsically exposed, e.g., if they are located near coastal waters and are therefore particularly susceptible to erosion, but also hostile human interference. The latter challenge could become even more complex with renewables, as offshore wind farms are, for example, in the coastal foreshore of the oceans and are therefore particularly exposed.

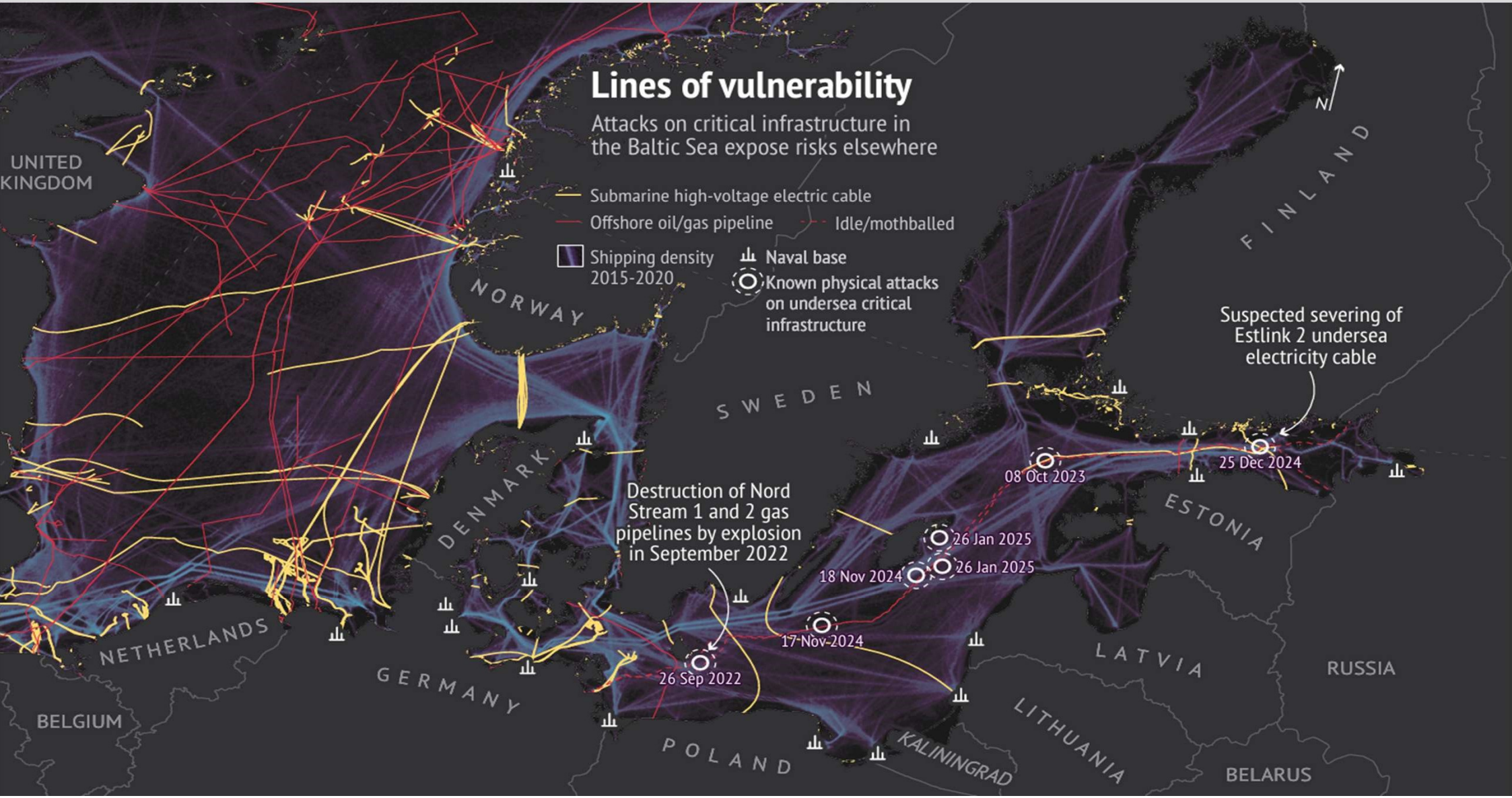




Hybrid Threats to the Energy Sector



Hybrid Threats to the Energy Sector



Hybrid Threats to the Energy Sector

- **2019-22, Saudi Aramco:** drone & rocket attacks by Houthis at pipeline pump station and petroleum storage facilities.

- **2022 September, Nord Stream:** ‘blame game’ Russia, US, Ukraine, the sabotage operation involved a small sailing boat and a team of six people, a combination of Ukrainian soldiers and civilians.

- **2023, October, Balticconnector:** a vital Baltic Sea gas pipeline linking Estonia and Finland, the sabotage ‘accident’ involves a Hong Kong-flagged container ship.

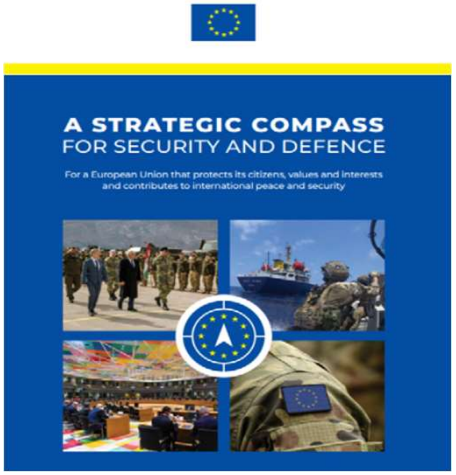
- **2024, March, Kalinigrad:** Russian law enforcement authorities in the Kaliningrad region arrested a German citizen on charges of sabotaging a gas distribution station.

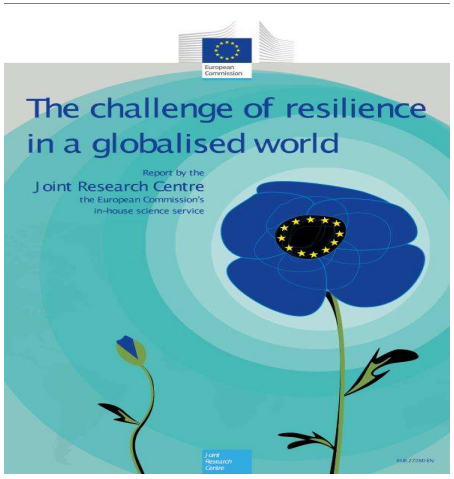
Hybrid Risk Assessment Matrix

Threat Category	Mechanism	Likelihood	Impact	Risk
Disinformation & social manipulation	Narratives that undermine support for infrastructure projects	High	Medium	High
Economic coercion & supply manipulation	Withholding energy deliveries or adjusting contract terms	Medium	High	High
Influence operations in regulatory environments	Lobbying via proxies to shape energy policy	Medium	High	Medium
Physical disruption of assets	Sabotage of pipelines, transformers, or logistics routes	Medium	High	High
Supply-chain interference	Restricting access to turbines, transformers, critical minerals	Medium	Medium	Medium
Lawfare & bureaucratic warfare	Filing coordinated lawsuits or environmental challenges	Medium	Medium	Medium
Environmental/resource manipulation	Manipulating water flows needed for hydropower or cooling	Low	Medium	Low

Countering hybrid threats to the energy sector

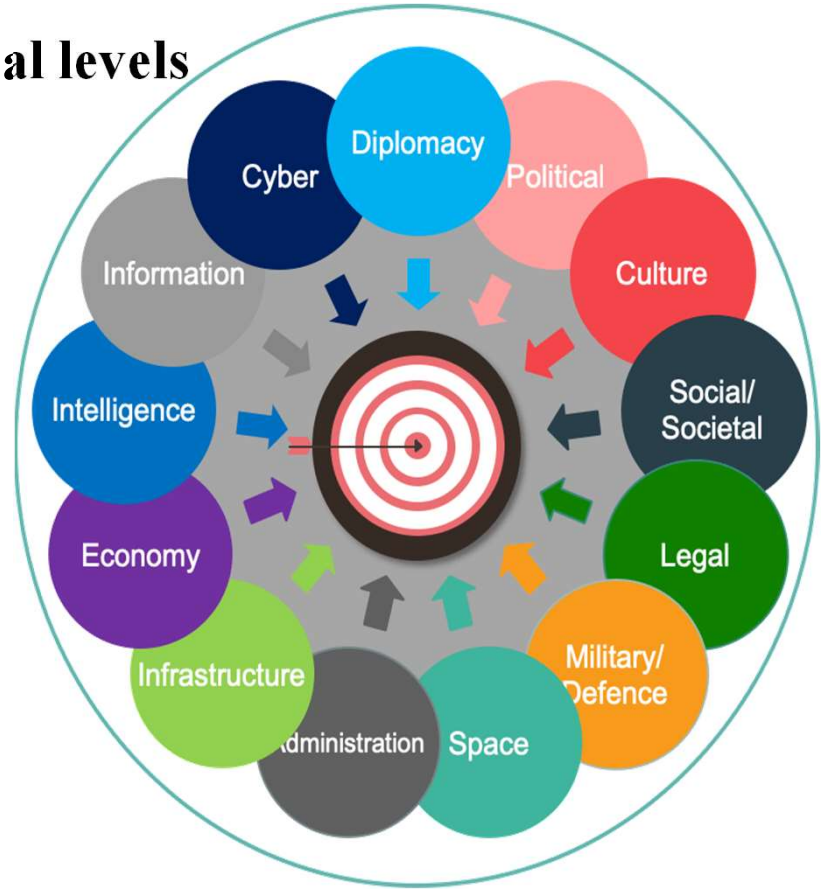
- EU Hybrid Toolbox (EUHT) = **umbrella framework**
- EU Strategic Compass
- EU Hybrid Response Teams
- EU Hybrid Fusion Cell
- Cyber Diplomacy Toolbox
- EUvsDiSiNFO
- Foreign Information Manipulation Interference Toolbox (FIMI)
- Integrated Political Crisis Response (IPCR)





Countering hybrid threats to the energy sector

- **Connecting the dots** of a hybrid campaign that is related to the energy sector
- **Attribution problem**
- **Coordinate all necessary tools at the national & regional levels**
- **Enhance resilience (cyber/societal/energy)**
- **Diversification or energy sources**
- **Whole of government / whole of society approach**



Questions

Scenario: “Operation Cold Front”

Background

A third-country adversary - State X - seeks to undermine EU cohesion during a winter period of high energy demand. The EU has recently increased its renewable-energy interconnections, reducing State X’s geopolitical leverage. State X therefore uses hybrid tactics to disrupt public trust in the EU’s energy security and to increase political pressure in targeted Member States.

Phase 1: Strategic Preparation (Covert, Low-Attribution Actions)

Disinformation & Information Manipulation

State X activates a network of proxy media outlets and inauthentic social media accounts. Narratives spread include:

- Claims that newly built offshore wind infrastructure is “unsafe” and “vulnerable to collapse.”
- Conspiracy theories alleging corruption in EU grid-modernization contracts.
- Fabricated stories about imminent rolling blackouts in specific Member States.

Phase 2: Grey-Zone Pressure on Critical Energy Infrastructure

Economic Coercion

- State X’s state-owned energy company abruptly announces “technical issues” and reduces natural gas flow to a single EU country.
- This reduction is small enough to provide plausible deniability but significant enough to trigger market anxiety.

Scenario: “Operation Cold Front”

Phase 3: Cyber Disruption (Limited, Reversible)
Cyber Intrusions
A pro-State X hacking group performs:

- Reconnaissance on the supervisory control systems (SCADA) of an EU electricity transmission operator.
- A low-level denial-of-service attack against customer portals of distribution system operators (harmless but highly visible).

Phase 4: Physical Pressure & Ambiguous Actions at Sea
Maritime “Safety Incidents”

- Fishing vessels associated with State X begin operating unusually close to EU offshore wind farms.
- One vessel accidentally drags an anchor near a subsea power cable, causing minor damage—but with enough ambiguous intent to raise security concerns.

Phase 5: Political Influence Operations
Directed Political Pressure
State X provides covert support (financial and informational) to a domestic political party arguing for:

- Halting renewable-energy expansion.
- Reopening dependency on fossil imports from State X.

Leaked documents - fabricated by State X - attempt to show EU regulators interfering in national energy decisions.