

Outsmart malicious actors to deter hybrid attacks

Safer Together

Strengthening Europe's Civilian and Military Preparedness and Readiness by **Sauli Niinistö**

October 2024

Building block #6

What is the challenge?

- The significant increase in the number of malicious activities on the EU's territory this year points to an **ever more brazen and aggressive nature of hybrid activities by Russia and other external actors**. For example, especially since 2023, there has been a marked increase in the number of (attempted) acts of physical sabotage across the Union.
- The EU has already taken steps to build preparedness and resilience against hybrid threats, including most recently with the adoption of a sanctions framework for destabilising activities against the EU and its Member States. Yet, **more work needs to be done to credibly deter malicious actors**.
- Hybrid operations' methods are inherently **ambiguous, subversive and difficult to detect**, often exploiting global connectivity and supply chains, economic dependencies, legal loopholes, internal political divisions or the openness of our democratic societies.
- Certain malicious activities, such as acts of (physical) sabotage or cyberattacks, may not only disrupt economic, energy, transport or digital networks, but **can also cause possible cascading effects across other sectors** and even lead to the loss of human life.
- Other hybrid activities – such as Foreign Information Manipulation and Interference

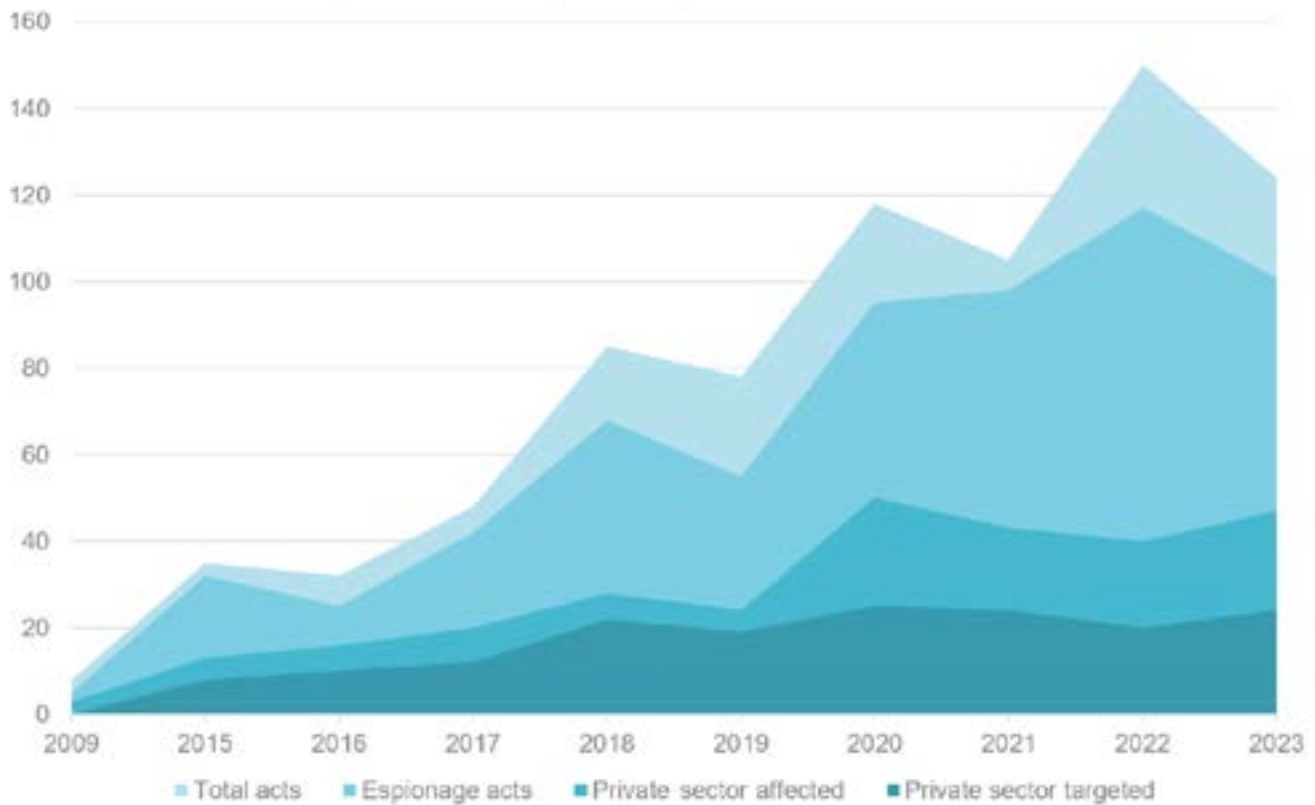
(FIMI) or political infiltration – have a **corrosive long-term effect on society**, for instance supercharging political polarisation, and contributing to a political climate increasingly conducive to acts of political violence and extremism.

- So far, the EU's increasing efforts to prevent, prepare for and respond to hybrid actions have been insufficient to credibly deter threat actors, who consider that **they can act at little cost and with relative impunity**.

What is the objective?

- Enhance EU preparedness against hybrid threats to create a **higher threshold for malicious actors** to engage in hostile activities targeting us.
- Strengthen our deterrence against State-sponsored hybrid attacks through: a) '**deterrence by denial**', increasing the EU's resilience by tackling vulnerabilities and strengthening its capacity for damage mitigation; b) '**deterrence by punishment**', dissuading potential perpetrators through a decisive response that imposes costs outweighing any potential benefits of continued hybrid operations.
- While keeping fully in line with our democratic principles and values and respecting EU, national and international law, strengthening our preparedness is **crucial in anticipation of the possible future escalation of hybrid campaigns**.

State-sponsored Cyber Operations 2009 to 2023



Increase in State-sponsored cyber operations worldwide”

Source: Based on EUISS, 2024, and Council on Foreign Relations, Cyber Operations Tracker, 2024.

What does the Report propose?

Strengthen EU intelligence structures step-by-step towards a fully fledged EU service for intelligence cooperation.

- ✓ Implement the steps agreed by the Council as part of the implementation of the Strategic Compass to reinforce and improve Single Intelligence Assessment Capacity (SIAC), including the Hybrid Fusion Cell.
- ✓ Ensure a structured and coordinated process to timely address information requirements and requests for SIAC products, including from relevant Commission services and the EU agencies under their oversight.
- ✓ Strengthen and formalise information and data sharing arrangements between SIAC and other relevant EU level actors with a view to better aggregating information.
- ✓ Enhance cooperation between SIAC and relevant security departments/units of the Commission, the EEAS, the General Secretariat of the Council and other EU institutions and Member States to coordinate specific counter-espionage tasks.
- ✓ Develop a proposal together with Member States on the modalities of a fully fledged intelligence cooperation service at the EU level that closes the remaining gaps and better connects internal and external security with fast and accurate intelligence assessments that can serve both the strategic and operational needs of EU-level policy planning decision-making.

Reinforce the EU's capacity for 'deterrence by denial':

- ✓ Take joint action to make it as difficult as possible for hostile intelligence services to operate in the EU. Discrepancies in Member States' counter-intelligence practices, legislation and insufficient cross-border information sharing can be exploited by malicious actors.
- ✓ Encourage Member States to proactively share information about vulnerabilities that pose a broader threat within the Union and should be tackled together at the EU level.
- ✓ Establish an anti-sabotage network to support Member States in preventing and responding to sabotage incidents. The network would build upon existing EU-level cooperation, notably the Critical Entities Resilience Group, the Protective Security Advisory Programme, the work of the INTCEN Hybrid Fusion Cell, and the cooperation between Member States' intelligence/security services, law enforcement, border and coast guards (including Frontex), customs and other competent authorities.
- ✓ Strengthen the links between the work on countering hybrid threats and economic security. Supply chain dependencies, future digital infrastructure, foreign direct investment, research security, and new clean technologies are leveraged by competing and malicious global powers to create the potential for weaponisation as part of coercive strategies.

Reinforce the EU's capacity for 'deterrence by punishment':

- ✓ Conduct a comprehensive assessment of key hybrid threat actors' strategic and operational specificities to identify aims, methods, key vulnerabilities and exposures to EU countermeasures. This will help to identify, organise and grade all tools at our disposal in an actor-specific way, with the aim of altering the cost-benefit analysis of the targeted actors over time.
- ✓ Reinforce political attribution as the basis for response to hybrid threats and consider on a case-by-case basis the public use of (declassified) intelligence assessments. In line with a 'naming and shaming' logic, rapid attribution or the public use of intelligence can be an effective way to seize the initiative and place hybrid actors on the backfoot, preventing or disrupting their malicious plans.
- ✓ Ensure the creation of a robust framework for lawful access to encrypted data to support the fight of Member States' authorities against espionage, sabotage and terrorism, as well as organised crime. There are signs that in several recent cases of sabotage, perpetrators were recruited and instructed via digital communication applications. Therefore, the ability of lawfully accessing encrypted data is important to counter such threats, while fully respecting fundamental rights and without undermining cybersecurity.