

LAW ENFORCEMENT'S ROLE IN COUNTERING HYBRID THREATS


Main Authors

Vincent Perez de Leon-Huet (EOS)

August 2026

About ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 ‘Knowledge Networks for Security Research & Innovation’, aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.
- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Report Feedback

We’re collecting feedback on this report through the EU Survey Platform, if you’d like to share your thoughts anonymously please click on the link below.

<https://ec.europa.eu/eusurvey/runner/enact-report-feedback>



**Funded by
the European Union**

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

This report contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Acknowledgement

This report was requested by CEPOL, the European Union Agency for Law Enforcement Training, as a complementary report to their 2026 Research Week, which this year was focused on tackling hybrid threats. We thank CEPOL for their engagement and valuable feedback during the report preparation process.

Acronyms

AI	Artificial Intelligence
CERIS	Community of European Research & Innovation for Security
CORE	Comprehensive Resilience Ecosystem
EU	European Union
FCT	Fight against Crime and Terrorism
FR	Flash Report
JRC	Joint Research Centre of the European Commission
HCoE	The European Centre of Excellence for Countering Hybrid Threats
IOCTA	Internet Organised Crime Threat Assessment
LEA	Law Enforcement Agency
MS	Member State(s)
NATO	North Atlantic Treaty Organisation
OSINT	Open-Source Intelligence
R&I	Research & Innovation
SOCTA	Serious and Organised Crime Threat Assessment
UAS	Stability Policing
TE-SAT	Terrorism Situation and Trend Report
WP	Work Package

Understanding Hybrid Threats

In recent decades, the term hybrid threat has become increasingly intertwined with the security and defence environment, highlighting some of the most pressing challenges faced by the European Union (EU), its partners and Member States. Security strategies across the EU, the North Atlantic Treaty Organization (NATO) and their respective Member States (MS) routinely reference hybrid threats and the need for states to build resilience and anticipatory capacities in response. However, despite the growing use of the concept, defining hybrid threats remains difficult.

Although the frequency and visibility of hybrid activities increased significantly following the COVID-19 pandemic, mainly due to heightened societal polarisation, increased reliance on digital technologies and declining trust in public institutions, the concept is not new. The notion of “hybrid warfare” has long been used to describe the combination of conventional and unconventional means in conflict, with some scholars tracing its roots back to classical strategic thought such as that of Sun Tzu. The modern formulation of “hybrid warfare”, however, gained prominence through Frank Hoffman’s work *Conflict in the 21st Century: The Rise of Hybrid Wars* [1] and increasingly appeared in NATO doctrine and policy discussions after 2010 [2].

Over time, the concept evolved from a predominantly military understanding towards a broader framework encompassing both military and non-military activities [3]. This shift from “hybrid warfare” to “hybrid threats” reflects the recognition that contemporary hostile actors often combine diplomatic, informational, military, economic, cyber, legal and societal instruments to pursue strategic objectives, operating below the threshold of open armed conflict. The broad and flexible nature of the concept has nevertheless generated significant definitional ambiguity. Interpretations differ substantially across organisations, states and researchers [4]. This conceptual flexibility presents an issue, as the absence of a standardised definition complicates the development of coherent policies and operational responses, particularly for law enforcement actors who require clear legal frameworks and operational mandates. Similar to organised crime, hybrid threats rarely constitute a single prosecutable offence; rather, they emerge through the cumulative effect of multiple coordinated activities that may individually appear lawful, ambiguous or unrelated [5].

For this report, hybrid threats refer to coordinated activities, typically conducted below the threshold of conventional armed conflict, that seek to undermine, destabilise or harm a target, such as a state, organisation or society. These activities employ a combination of overt and covert means to exploit vulnerabilities, influence decision-making processes and achieve strategic objectives.

These means can include disinformation campaigns, cyberattacks, economic coercion, sabotage, foreign interference, instrumentalisation of migration and the use or threat of military force, among others. State and non-state actors employ hybrid threats to undermine democratic institutions, erode societal cohesion and weaken public trust in government and other key institutions. By exploiting and amplifying existing social, political, economic or cultural divisions, hybrid threat actors can weaken governance capabilities and increase the likelihood of achieving their strategic objectives (seen Appendix A) [6]. The Russian Federation's actions surrounding its war of aggression against Ukraine remain one of the most salient examples for Europe. Russian activities have included cyberattacks, disinformation campaigns, manipulation of energy dependencies, weaponisation of migration flows and coordinated information operations directed at EU and NATO populations, while attempting to remain below the threshold of direct military confrontation with NATO.

While states remain the principal actors associated with hybrid threats, non-state actors frequently play important roles as proxies, facilitators or force multipliers. These may include organised criminal groups, hacktivist networks, private military companies, commercial entities and other intermediaries that provide states with plausible deniability while advancing strategic objectives [7]. This nexus between state and non-state actors is particularly relevant for law enforcement agencies (LEAs), as many hybrid activities intersect with criminal offences and investigative responsibilities.

Academic literature increasingly recognises that hybrid threats are likely to intensify alongside technological developments. The rapid expansion of technologies such as artificial intelligence (AI), big data analytics and quantum technologies has significantly increased the scale, speed and sophistication with which hostile actors can conduct influence operations and manipulate information environments. Emerging technologies facilitate the creation of synthetic media and deepfakes, enable automated dissemination of disinformation, support sophisticated social engineering campaigns, enhance cyberattack capabilities and allow for the large-scale exploitation of personal and behavioural data [8]. As a result, digital technologies increasingly function both as accelerants and weapons within hybrid campaigns, amplifying societal vulnerabilities and eroding democratic resilience [9].

In parallel to these developments, the concept of security has itself been evolving. As modern security environments are increasingly shaped by interconnected political, economic, informational, technological and societal risks, rather than solely by conventional military threats, the lines between external security, often associated with defence, and internal security have become increasingly blurred [10]. Hybrid threats exploit precisely these ambiguities. They target not only military structures, but also civilian infrastructure, public administrations, media ecosystems, legal systems and societal trust. Responding to, and countering, hybrid threats is therefore not only a competence of the military or intelligence domains, but a whole-of-society challenge requiring whole-of-government/society responses. Consequently, the role of civilian institutions, including law enforcement agencies (LEAs), has become increasingly central in the broader hybrid threat landscape.



LEAs and the Hybrid Threat Gap

The growing prevalence of hybrid threats has profound implications for LEAs across Europe. Traditionally, national security and defence were viewed primarily through the lens of military and intelligence institutions, while police services focused on criminality and public order. However, hybrid threats increasingly blur the distinction between external and internal security domains, placing LEAs at the forefront of a rapidly evolving threat environment. Hybrid campaigns deliberately exploit institutional grey zones and fragmented responsibilities between internal and external security actors [3][11]. This creates operational challenges for LEAs, as many hybrid activities initially resemble ordinary criminal acts or disinformation campaigns rather than coordinated hostile operations.

In addition to the difficulty of analysing an isolated act versus a hybrid campaign, law enforcement faces the challenge of responding to malicious or destabilising activities that may not individually constitute criminal offences, while also respecting democratic freedoms, fundamental rights and civil liberties. This issue is particularly visible in the information domain, as disinformation is frequently discussed as a central component of hybrid threats, creating a risk of excessive securitisation of online speech and violation of democratic values [9]. Existing legal frameworks in many democratic states limit LEAs' ability to prosecute harmful but non-illegal speech directly. Consequently, responses to hybrid disinformation campaigns must balance security objectives with freedom of expression, media freedom and democratic principles.

Contemporary hybrid threats operate extensively within the societal spaces where LEAs traditionally function. This includes cyberspace, local communities, critical infrastructure requirements, public events and online information ecosystems. Law enforcement therefore increasingly finds itself responding not only to the consequences of hybrid threats, but also to the early indicators and enabling conditions that hostile actors exploit. The challenge is compounded by the fact that hybrid activities are specifically designed to remain below traditional thresholds of attribution and retaliation, carefully synchronised to avoid clear detection while simultaneously exploiting institutional weaknesses, legal constraints and procedural delays [12]. This means that LEAs may encounter isolated incidents without immediately recognising their connection to broader coordinated campaigns.

Beyond limited understanding of hybrid threats, research by the Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project, funded by the EU's Horizon 2020 Research and Innovation Programme, has identified further gaps faced by LEAs.

Critical gaps identified in this context include,

- limited preventive capacities among law enforcement,
- insufficient societal awareness,
- inability to recognise emerging technologies as potential tools for hybrid threats,
- weak institutional coordination, and
- inadequate situational awareness.

These gaps can create major vulnerabilities that hybrid actors can exploit, with many institutions continuing to underestimate the strategic nature of the evolving hybrid threat environment [13]. These gaps were also identified by certain Member States across Europe as well. In the case of Sweden, a report on strategies to counter hybrid threats found that the police had no comprehensive approach to countering hybrid threats [14].

One of the most significant challenges concerns information sharing and coordination. Hybrid threats cut across institutional boundaries, yet many security structures continue to operate in silos, whether because of weak horizontal coordination between agencies or limited vertical coordination between national, regional and local authorities. Lessons from historical policing failures, particularly regarding serial crime investigations in the 1970s and 1980s, demonstrate the operational risks associated with fragmented information systems and poor inter-agency cooperation. Similar risks currently exist in the hybrid threat domain, as LEAs, military and intelligence entities do not coordinate to a sufficient degree. LEAs should be viewed as an essential component and responsible actor in the wider architecture of countering hybrid threats, rather than as a supporting actor with only military entities taking a leading role.

The increasing complexity of hybrid threats also places new demands on police personnel and organisational structures. Contemporary officers increasingly require skills extending beyond traditional policing functions, including digital literacy and cyber awareness, understanding of disinformation ecosystems, analytical and intelligence capacities, crisis communication, risk forecasting and strategic foresight, cross-border operational cooperation, and understanding of geopolitical dynamics [12]. The operational landscape in Ukraine further illustrates the importance of integrated, preventive approaches. Ukrainian LEAs have increasingly adopted proactive measures involving cyber monitoring, information analysis, early warning systems and close cooperation with civil society and international partners [15]. Such approaches demonstrate that prevention and resilience-building are becoming central functions of modern policing within hybrid threat environments.

Ultimately, hybrid threats reveal a broader transformation in the concept of policing itself. Law enforcement can no longer be viewed solely as a reactive instrument responding to completed criminal acts. Instead, LEAs increasingly function as strategic actors within wider resilience ecosystems that seek to anticipate, detect, mitigate and recover from complex multi-domain threats.

The Farsighted Policeman

Similar to the historical shift from traditional policing models towards “the scientific policeman”, associated with intelligence-led and evidence-based policing in the 1930s, a century later, hybrid threats necessitate the emergence of what may be described as the “farsighted policeman”: a law enforcement actor capable not only of reacting to incidents, but also of anticipating, interpreting, and mitigating complex and interconnected threats. Consequently, strategic foresight and anticipatory capacities are becoming essential components of modern policing in the context of the capability gaps and complex security environment described above.

The importance of foresight is strongly emphasised by the Joint Research Centre (JRC) and the Hybrid Centre of Excellence (HCoE) in their work to develop a Comprehensive Resilience Ecosystem (CORE) model for analysing hybrid threats [16]. The model, illustrated in Figure 1 below, emphasises the need for forward-looking situational awareness mechanisms capable of identifying vulnerabilities and detecting hybrid activities during their earliest phases. Such approaches move beyond traditional reactive policing and instead focus on horizon scanning, early warning systems and long-term resilience planning.

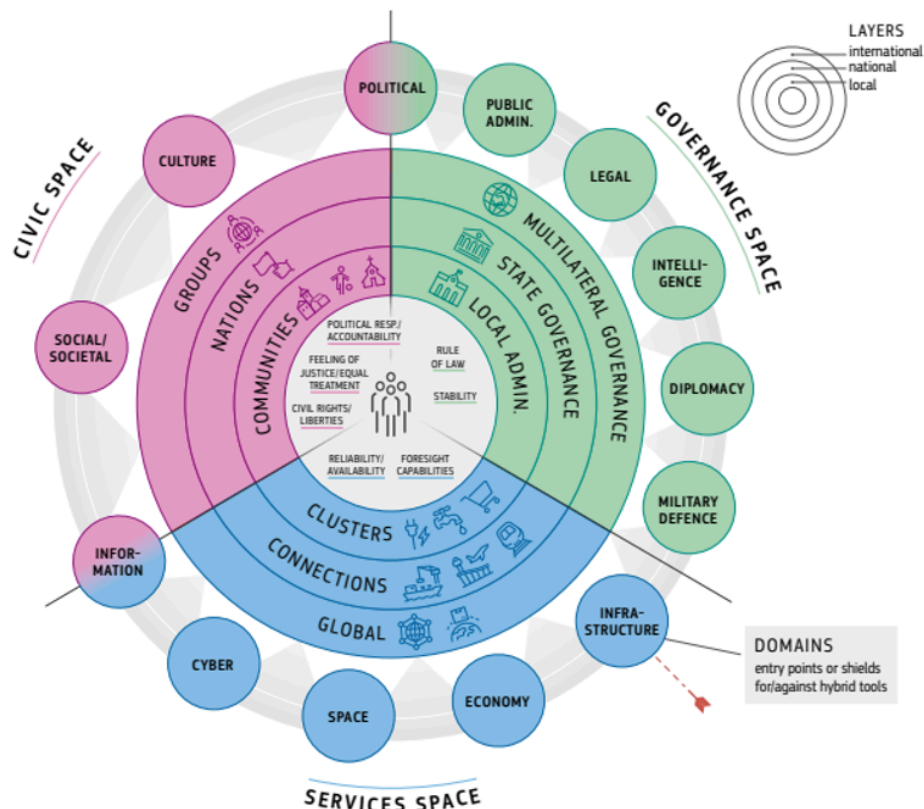


Figure 1: JRC's and HCoE's CORE Model



For LEAs, this means developing the institutional ability to identify weak signals and recognise coordinated hostile campaigns before they escalate. LEAs should integrate the CORE model into strategic planning and analytical capabilities in order to assess whether an activity may be part of a hybrid threat and how it may affect other parts of society. Hybrid threats rarely emerge as isolated incidents. Rather, they consist of cumulative actions that may individually appear insignificant, but collectively contribute to strategic destabilisation. Detecting such patterns therefore requires integrated analytical capabilities, robust intelligence-sharing mechanisms and multidisciplinary cooperation. In this regard, training becomes a critical pillar of preparedness, and CEPOL can play an important role in supporting European law enforcement to better understand and respond to hybrid threats.

Currently, there is a low level of awareness regarding hybrid threats among public administration officials and police personnel, including some actors already involved in tackling them [17]. Many public institutions still treat hybrid threats as a marginal security issue, despite their growing strategic importance at the political level [12]. To address these gaps, specialised educational programmes and professional training initiatives are needed. Such programmes should focus on

- identifying hybrid threat indicators,
- understanding information manipulation and disinformation techniques,
- cyber awareness and digital investigations,
- strategic communication and crisis response,
- risk analysis and vulnerability assessment, and
- inter-agency coordination mechanisms.

There are also trainings regarding hybrid threats that already been implemented which could be good starting points to further develop [18]. Importantly, these competencies should not remain limited to specialised intelligence or cyber units. Given that hybrid threats often emerge at the local level and across civilian spaces, frontline officers and regional police structures must also possess sufficient awareness to identify and escalate suspicious patterns [12]. However, the ability to recognise potential indicators of hybrid activity is only the first step. Because hybrid campaigns typically consist of dispersed and seemingly unrelated activities occurring across different sectors and jurisdictions, individual observations must be effectively shared, combined and analysed in order to generate a broader operational picture.

This requirement reinforces the need for stronger information-sharing cultures within and between institutions, shifting away from rigid compartmentalisation towards more horizontal and networked cooperation structures. In this regard, Europol and other European agencies play an increasingly important role by facilitating intelligence exchange, joint analysis and cross-border cooperation among relevant actors. Europol's flagship intelligence products, including the Serious and Organised Crime Threat Assessment (SOCTA), the Internet Organised Crime Threat Assessment (IOCTA), and the Terrorism Situation and Trend Report (TE-SAT), increasingly acknowledge the convergence between organised crime, cybercrime, disinformation and hybrid threats. SOCTA 2025 specifically highlights how hybrid threat actors exploit criminal networks, digital infrastructures and societal vulnerabilities to support broader destabilisation objectives [7]. Cross-border cooperation and common situational awareness mechanisms are therefore becoming indispensable.

Promising examples of such cooperation can already be found within Europol, although further integration and information sharing across the EU remain necessary [9]. This includes stronger collaboration between LEAs, intelligence services, border authorities, cybersecurity agencies, judicial institutions, private-sector actors and civil society organisations.

The concept of Stability Policing (SP), used within NATO operations, may also offer relevant lessons. SP emphasises the integration of policing expertise into broader crisis management and security operations, particularly in fragile or hybrid-threat environments. Rather than replacing military capabilities, SP complements them by addressing criminal violence, maintaining public order, supporting governance structures and strengthening trust within communities [18]. Such approaches may become increasingly relevant within the EU context as hybrid threats continue to blur distinctions between war and peace, domestic and foreign security, and civilian and military domains.

At the operational level, LEAs must also increasingly adopt technological tools capable of supporting early detection and analysis. AI-enhanced analytics, Open-Source Intelligence (OSINT), behavioural analysis and big data systems can assist in identifying coordinated disinformation campaigns, hostile networks and emerging vulnerabilities. However, the deployment of these technologies should be bounded by democratic safeguards, data protection standards and human rights principles. The concept of “democratic deterrence”, understood as the use of democratic values and countermeasures aligned with them as part of a soft-power strategy for dealing with hybrid threats, has inherent limitations. It requires acceptance that some antagonistic actions cannot be fully deterred. However, LEAs can adapt so that hybrid campaigns become less effective and therefore less frequent [14].

The “farsighted policeman” therefore represents more than a technological evolution. It reflects a broader strategic and cultural transformation in policing: one that prioritises anticipation over reaction, resilience over enforcement alone, and cooperation over institutional isolation.



Conclusions

Hybrid threats represent one of the defining security challenges facing the EU and its partners in the 21st century. Their ability to operate below the threshold of armed conflict, exploit democratic vulnerabilities and combine multiple instruments of power simultaneously makes them particularly difficult to detect, attribute and counter. Unlike traditional security threats, hybrid threats deliberately blur the boundaries between war and peace, civilian and military domains, and internal and external security.

This evolving environment places LEAs in an increasingly central position within broader national and European security architectures [19]. LEAs can no longer be viewed solely as reactive actors tasked with responding to criminal offences after they occur. Instead, they increasingly serve as critical components within comprehensive resilience ecosystems aimed at anticipating, detecting, mitigating and responding to complex multi-domain threats. Several recurring themes emerge when analysing hybrid threats and the role of LEAs in countering them:

- First, there remains a significant need for common definitions, shared situational awareness and improved strategic coordination across European institutions. Hybrid threats exploit institutional fragmentation and operational silos. Without effective information-sharing mechanisms and coordinated responses, hostile actors can exploit gaps between agencies, legal frameworks and governance levels.
- Second, resilience-building must become a central pillar of law enforcement strategy. This includes strengthening institutional capacities, improving cyber resilience, developing early warning systems and increasing public awareness regarding information manipulation and foreign interference.
- Third, foresight and anticipatory governance are becoming increasingly important. The ability to identify vulnerabilities, recognise weak signals and detect hybrid activities during their early stages may significantly reduce the strategic impact of hostile campaigns. Consequently, strategic analysis, intelligence integration and forward-looking planning should become embedded within contemporary policing models.

- Fourth, hybrid threats require a whole-of-government and whole-of-society response. Effective countermeasures cannot rely exclusively on police or intelligence services. Instead, cooperation between public authorities, private-sector actors, civil society, academia, media organisations and international partners is essential.

At the operational level, LEAs must continue adapting to rapidly evolving technological environments. AI-enhanced disinformation, cyber-enabled manipulation, digital influence campaigns and transnational criminal convergence increasingly require specialised competencies, advanced analytical capabilities and stronger cross-border cooperation. At the same time, democratic principles and the rule of law must remain central. Responses to hybrid threats should not undermine the very democratic values they seek to protect. Maintaining proportionality, transparency, accountability and respect for fundamental rights remains essential to sustaining public trust and democratic legitimacy.

Ultimately, hybrid threats should not be viewed solely as isolated security incidents, but rather as long-term strategic challenges targeting societal resilience itself. Addressing them therefore requires not only operational preparedness, but also adaptive institutions, informed societies and resilient democratic governance. As hybrid threats continue to evolve in complexity and scale, the role of LEAs will likely become increasingly strategic. Developing the “farsighted policeman”, capable of anticipation, cooperation, resilience-building and strategic adaptation, may therefore represent one of the most important transformations in European policing in the years ahead.

References

- [1] Hoffman, F. G. (2007), *Conflict in the 21st Century: The Rise of Hybrid Wars*. Available at: https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- [2] Smith, H. (2019), *Countering Hybrid Threats*. Available at: <http://www.jstor.org/stable/resrep19964.7>
- [3] Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K. and McCue, M. (2018), *Addressing Hybrid Threats*. Available at: <https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf>
- [4] Marcuzzi, S. (2018), *Fears of Trolls and Little Green Men: Does Hybrid Warfare Work, for Whom, and When?* Available at: https://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf
- [5] Karas, Ž. (2025), *Definitions and Classifications of Hybrid Threats in Criminal Law*. Available at: <https://doi.org/10.13165/PSPO-25-37-01-07>
- [6] Taneski, N. and Kirkova, R. (2018), The Concept of Hybrid Threats. Available at: <https://eprints.ugd.edu.mk/22011/>
- [7] Europol (2025), European Union Serious and Organised Crime Threat Assessment: The Changing DNA of Serious and Organised Crime. Available at: <https://doi.org/10.2813/5473714>
- [8] Europol (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024. Available at: <https://doi.org/10.2813/442713>
- [9] Fernandes, R. N. A. (2025), Hybrid Threats and Digital Deception: Rethinking Police Strategies against Disinformation. Available at: <http://hdl.handle.net/10400.26/62079>
- [10] Gerginova, T. (2025), The Concept of Security and Hybrid Threats. Available at: <https://openaccess.ludovika.hu/nke/catalog/book/379/chapter/4148>
- [11] Borch, O. and Heier, T. (2024), Understanding Hybrid Threats: An Introduction. Available at: <https://doi.org/10.4324/9781032617916-1>
- [12] Korauš, A., Kurilovská, L. and Šišulák, S. (2022), Increasing the Competences and Awareness of Public Administration and Police Officers in the Context of Current Hybrid Threats. Available at: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>
- [13] Cardarilli, M. and Theron, J. (2024), D2.11 Deeper Analysis, Delivery of Short List of Gaps & Needs. Available at: <https://euhybnet.eu/>
- [14] Svenonius, O. and Strindberg, A. (2020), Hantering av hybrida hot: Teoretiska utgångspunkter och val av strategi för Polismyndigheten [Countering Hybrid Threats in Law Enforcement: Theoretical Starting Points and Choice of Strategy]. Available at: <https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--4966--SE>
- [15] Kalytiuk, K. V. and Verhelis, B. V. (2026), Functioning of Law Enforcement Agencies of Ukraine during Hybrid Threats: Current Challenges and Counteraction Measures. Available at: <https://dspace.univd.edu.ua/server/api/core/bitstreams/3ee40a79-34a9-48a1-9408-a0e5ab062480/content>
- [16] Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G. (2023), Hybrid Threats: A Comprehensive Resilience Ecosystem. Available at: <https://doi.org/10.2760/37899>
- [17] NATO Stability Policing Centre of Excellence (2026), A New Stability Policing Paradigm for NATO: Policing, the Forgotten Tool against Hybrid/Irregular Warfare Manoeuvres. Available at: <https://www.nspcoe.org/wp-content/uploads/2026/01/03-final-version-14.01.26.pdf>
- [18] Piesarskas, E. (2025), Empowering a Pan-European Network to Counter Hybrid Threats: Reflections on the Use of the DTAG Methodology for EU-HYBNET Trainings (2020–2025). Available at: https://euhybnet.eu/wp-content/uploads/2024/12/EU-HYBNET_Policy-Brief_L3CE_V7.pdf
- [19] Mafart, J. (2026), Hybrid Threats: From Geopolitics to Internal Security. Available at: <https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-819-en.pdf>
- [20] Giannopoulos, G., Smith, H. and Theocharidou, M. (2021), The Landscape of Hybrid Threats: A Conceptual Model. Available at: <https://doi.org/10.2760/44985>

Appendix A: Visualisation of the Conceptual Model of Hybrid Threats from Hybrid Centre of Excellence

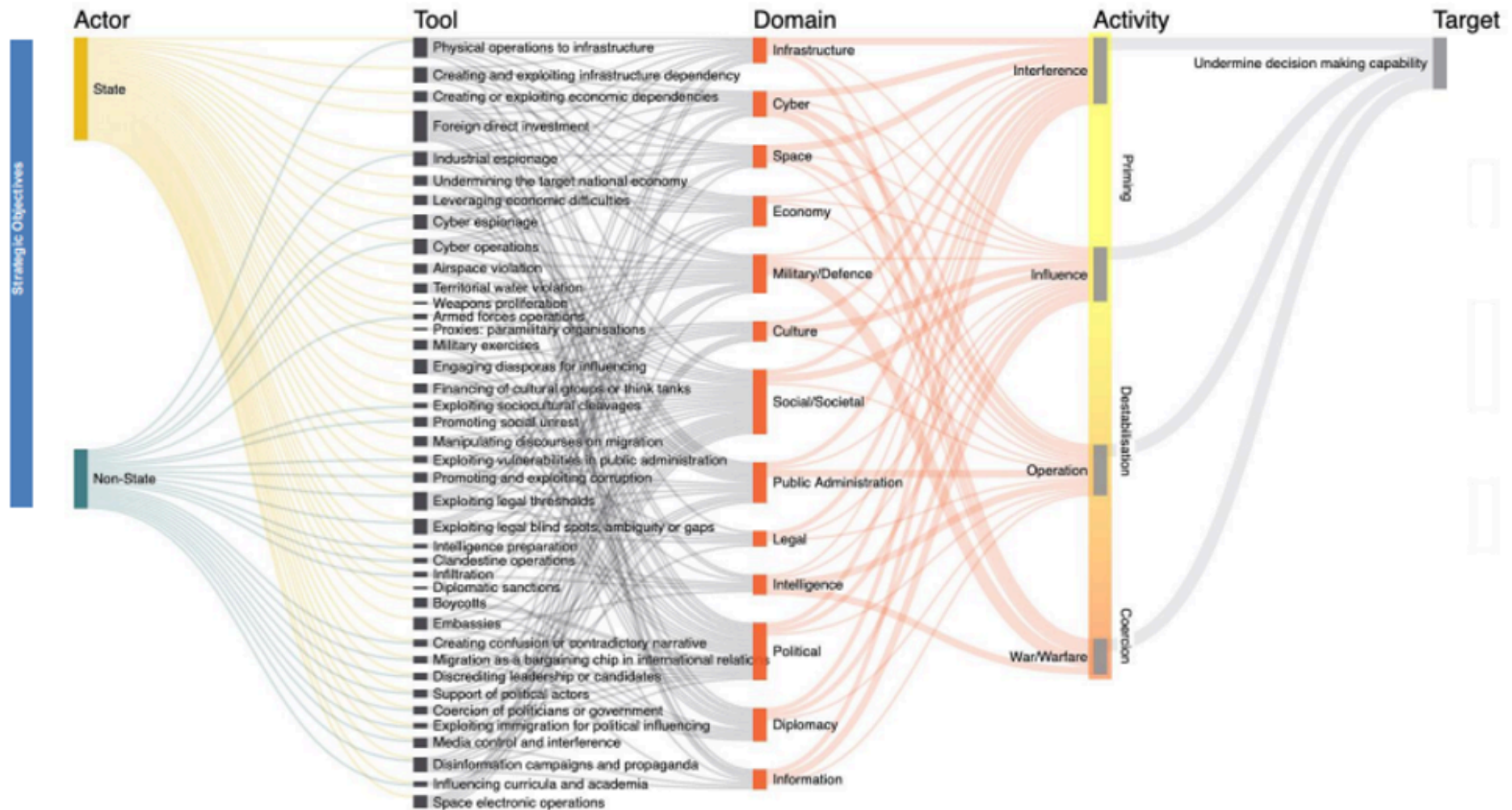


Figure 2: Visualisation of the Conceptual Model [20]



ENACT.

European Network Against
Crime and Terrorism



[@enact-network](https://www.linkedin.com/company/enact-network)



enact-eu.net



Scan the QR code to visit ENACT online
and read this report in digital format.



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.