RESONANT –

Tackling Disinformation, Foreign Information Manipulation & Interference

The Nexus of Crime and Politics: Why the EU Needs an Integrated Security Architecture to Counter Hybrid Threats and FIMI

Published in June 2026 on the platform for Interviews with FIMI experts[1]

Heiko, thank you very much for your time. First of all, can you pls tell us a bit about yourself? You have earned yourself a reputation for being one of the very few practitioner-scholars in the police sector. What career have you had as a police officer and as an academic?

Thank you very much for the question and the opportunity for this interview! I have been fortunate to acquire my qualifications at the key interfaces between the private sector and public security agencies, a path that has allowed me to develop a unique perspective as a practitioner-scholar.

Since I began advanced academic studies in security at the University of Public Administration and Administration of Justice in Bavaria and at Ruhr University Bochum in 2010, my career in the police sector has progressed from frontline roles — four years in the riot police and as a patrol officer — to a twelve-year tenure in a criminal investigation department, where I specialised in white-collar crime, with a strong emphasis on detecting organised criminal networks. Throughout this period, my ongoing commitment to professional development enabled me to integrate academic insight with practical expertise in this complex field. Over the past eleven years my focus has shifted to strategic and political levels: as a specialist advisor to agency leadership, I have gained valuable experience in security policy and worked closely with political stakeholders.

Most recently, I have linked strategic personnel planning with effective and efficient controlling. This forward-looking approach has been instrumental in helping my police department maintain both objective safety and the subjective sense of security for our citizens. Furthermore, my role as an Data Protection Officer for the Police Headquarters in Southern Upper Bavaria has become increasingly vital, as it is unmistakable that data protection is now a cornerstone of modern security technology.

[1] Interviews with FIMI Experts

I complemented my practical experience with a rigorous academic path, earning a Master's degree in Criminal Justice, Governance and Police Sciences from Ruhr University Bochum and a PhD in Political Science from the University of Cologne. I was fortunate to have Prof. Dr. Thomas Jäger - an internationally respected political scientist at the University of Cologne - as my PhD advisor and mentor. Together with Prof. Clemens Fischer, another renowned scholar of International Relations and Geopolitics at the same university, I was able to bridge academic excellence and practical relevance in my research.
I am grateful to Dr. Holger Nitsch, Executive Director of CEPOLIS (the Center of Excellence for Police and Security Research), whose ongoing advice and mentorship throughout my academic years greatly enriched my research and professional development.

Currently, as a Post-Doc Researcher at the Bavarian University of Applied Sciences for Public Service and through my work with CEPOLIS, I strive to bridge these two worlds. By translating academic findings into actionable strategies and bringing authentic field data back into scientific discourse, I aim to ensure that our security institutions remain resilient, transparent, and efficient in an increasingly complex but also – in concerns of security - challenging world.

Can you tell us a little more about what made you embark on a second career in academia after having worked as a police officer for so long?

That is a profound question. My transition into academia was not a departure from policing, but rather a logical evolution of my work as a strategist and a learner who is passionate about applying knowledge to improve security and life. After nearly three decades in the police force, I realised that the challenges we face today - such as my doctoral thesis with the research topic of organised crime in the context of hybrid warfare - have become so complex that they can no longer be solved by traditional operational methods alone. There were three primary drivers for this second career:

1. **Bridging the Gap**: I have always seen myself as a "practitioner-scholar," and I felt a strong need to bridge the gap between academic theory and police practice to ensure that research results are actually versatile and impactful for first responders.

2. **Navigating Complexity**: My work in white-collar crime and cybercrime investigations showed me that staying ahead of sophisticated criminal networks requires constant further education and a deep understanding of international security structures.

3. **Strategic Impact**: In my roles advising the agency's leadership and managing strategic personnel planning, I found that academic approaches and methods like geopolitical analysis, research logic, and evidence-based controlling are essential for designing effective security policies in an increasingly volatile world.

Ultimately, embarking on this academic path as a Post-Doc Researcher at CEPOLIS allows me to translate practical knowledge and field-tested data into scientific discourse while simultaneously bringing innovative, sustainable solutions back to the men and women serving on the front lines.

Your scholarly studies focus on the role and impact of hybrid threats. Why did you choose that topic?

I chose to focus on the role and impact of hybrid threats because, throughout my 27-year career in law enforcement, I witnessed a fundamental shift in how security is challenged.

My extensive background in investigating complex white-collar crime and cybercrime revealed that modern threats are increasingly non-linear, digital, transnational and interconnected. Specifically, my research on the topic of "Functions of Organized Crime in Hybrid Warfare" with an emphasis on the impact of Mexican cartels on the USA stems from the observation that criminal networks are no longer just a domestic or regional police issue.

Instead, they have become strategic tools used to undermine the rule of law and destabilise state institutions from within.

This choice was driven by several key factors: In my roles as a senior police strategist and advisor to the leadership, I saw that traditional security concepts often struggle to address "gray zone" activities that fall between war and peace, or crime and politics.

I am particularly fascinated by the symbiosis between crime and politics—the way in which criminal organisations systematically exploit globalisation and modern technologies to launder and reintegrate illicit profits into legitimate economic and financial cycles. In doing so, they do not merely operate in parallel to state systems but actively interact with them, sometimes infiltrating regulatory gaps, corrupting institutions, or leveraging weak governance environments.

In this regard, such entities can function as facilitators of hybrid warfare: their activities—money laundering, cyber-enabled fraud, sanctions evasion, illicit trade networks, and the destabilisation of local governance structures—may indirectly or directly serve the strategic interests of state or non-state actors engaged in hybrid conflict. The convergence of criminal infrastructure and geopolitical objectives creates a permissive ecosystem in which illicit financial flows and covert influence operations reinforce one another, blurring the boundary between organised crime and instruments of political power.

Ultimately, I recognised the pressing need to bridge the gap between practical field-tested experience and scientific discourse to provide versatile and impactful results for investigative authorities and first responders. This commitment led me to found the scholarly platform www.hybridthreats.org and to my current work at CEPOLIS, where I aim to ensure that our security institutions evolve as quickly as the threats they face.

What is your definition of hybrid threats?

The term "hybrid" originates from the Latin word "hibrida", signifying a **blend** or **intercrossing** of **elements**. It applies to various fields including natural sciences, engineering, and linguistics, denoting a composition or mixture of different elements, species, races, or

varieties. Essentially, it refers to anything of mixed ancestry or words formed from the combination of different languages.

In my research and PhD thesis, I define hybrid threats as the strategic and synchronised use of a **wide range** of diverse **instruments**, ranging from **political** and **economic** to **military** and **criminal**, by state or non-state actors to achieve specific objectives while remaining below the threshold of formal warfare. The defining characteristic of a **hybrid threat** is its **multi-vector nature**.

The more specific term **hybrid warfare** refers to a military strategy that integrates both conventional and irregular methods of combat. This concept lacks indeed a universally accepted definition, adding to its abstract nature. Consequently, "hybrid" is often used as an umbrella term for all non-linear threats.

Or in other words in the range of terrorism, terror, sabotage and subversion, to guerilla warfare, conventional warfare and even the nuclear domain, all possible levels of vertical escalation can be included or even combined within the term hybrid threat or hybrid warfare.

As our followers and regular website visitors know, our focus in RESONANT is on Foreign Information Manipulation and Interference (FIMI). How does that play into the hybrid threats dynamic?

In the context of the **RESONANT** project and the broader security architecture, FIMI serves as the psychological vanguard of the hybrid threats dynamic.

While other vectors of hybrid warfare, such as cyberattacks, economic coercion, or the instrumentalisation of organised crime, target a nation's physical and digital assets, FIMI targets the human domain. It is the strategic layer designed to **manipulate perceptions**, **erode social cohesion**, and **dismantle** the **public's trust** in **democratic institutions**. Within the hybrid machinery, FIMI is not merely a byproduct; it is the force multiplier that ensures physical disruptions translate into political paralysis.

The interplay between FIMI and the wider hybrid landscape is characterised by a nexus of narrative-action. For instance, when organised crime networks are used as a logistical engine to facilitate a manufactured border crisis or a ransomware attack, FIMI is deployed simultaneously to frame these events. By amplifying polarising content and spreading AI-driven disinformation, hybrid actors can overwhelm the cognitive capacity of a society, making it nearly impossible for governments to reach a consensus on how to respond. In this sense, FIMI creates a cognitive fog that masks the true origin and intent of a hybrid attack, providing the aggressor with the plausible deniability necessary to avoid traditional military or diplomatic escalation.

Furthermore, FIMI exploits the structural openness of the European information environment to turn a society's virtues into vulnerabilities. By hijacking legitimate grievances and amplifying them through botnets and influencer networks, foreign actors can foster internal instability that appears organic.

This interference often relies on the same grey infrastructure used by organised crime, such as illicit financing for social media ad campaigns or the use of shell companies to hide the source of propaganda.

Ultimately, FIMI is the connective tissue of the hybrid threat: it provides the "why" and the "how" that allows physical sabotage and criminal subversion to successfully hollow out a state's resilience from within.

Therefor understanding FIMI is essential not just for information security, but even for the defence of the European Union's sovereignty.

It appears that disinformation, crime and other activities that may cause serious harm to the other side but remain below the threshold of overt war have become tools of statecraft (actually, they might have been just that for quite a while). What governments are particularly likely to use said tactics?

While the use of sub-threshold tactics has historical precedents dating back centuries, they have indeed by increasing digitisation been formalised into modern statecraft by specific types of regimes.

Typically, governments most likely to employ these tactics are those characterised by **revisionist geopolitical goals**, **centralised authoritarian control**, and a significant **asymmetric disadvantage** compared to the conventional military or economic power of the West.

Revisionist powers-states, that seek to shift the existing international order or reclaim perceived historical spheres of influence, are the **primary practitioners** of these methods. For these regimes, overt military conflict with a block like NATO or the European Union is often seen as too costly or risky due to the threat of conventional retaliation or nuclear escalation.

Consequently, they turn to hybrid tools to achieve strategic victories without triggering a NATO article 5-style collective defence response. In a nutshell, the threshold of war is a **barrier to be avoided**, but below said threshold is a **space that can be exploited**.
By utilising cyber-mercenaries, organised crime syndicates for sanction evasion, and Foreign Information Manipulation and Interference to hollow out a target's internal cohesion, they can achieve territorial or political shifts through salami slicing tactics, which are small, deniable actions that, over time, fundamentally alter the status quo.

Furthermore, these tactics are favored by regimes where the distinction between the state, the intelligence services, and organised crime is intentionally blurred. In such **mafia states** or highly centralised **autocracies**, the government can easily instrumentalise criminal networks as logistical engines for sabotage or illicit financing. This provides the regime with the two most valuable assets in modern statecraft: **plausible deniability** and **strategic flexibility**.

By operating through **state proxies**, these governments can disrupt their adversaries' critical infrastructure or influence their elections while officially maintaining diplomatic relations.

Ultimately, they perceive the openness of democratic societies such as **free press**, **transparent markets**, and **protected legal rights** not as virtues, but as structural **vulnerabilities** ripe **for exploitation**.

You observed that the hybrid threats landscape is strongly influenced by organised crime. Can you specify that a little more?

In my research and my PhD thesis, I argue that **organised crime** is no longer just a peripheral issue of internal security but has become a **central pillar** of **modern hybrid threats** or even **warfare**. When we look at the hybrid threats landscape, we see a strategic blurring of lines between state and non-state actors, and between war and crime.

Organised crime serves this landscape in several critical ways:

First, it provides **plausible deniability**. State actors or hybrid aggressors can utilise existing criminal networks to conduct sabotage, cyberattacks, or disinformation campaigns. If these actions are carried out by criminals rather than soldiers, the true originator can remain in the shadows, making a coordinated political or military response much more difficult.

Second, organised crime acts as a **logistical engine**. Criminal groups already possess the infrastructure for illicit cross-border movements - whether it is the smuggling of goods, people, or capital. In a hybrid scenario, these shadow networks can be repurposed to transport weapons, funnel "grey" money to extremist groups, or bypass international sanctions.

Third, and perhaps most importantly, organised crime is a **catalyst for social and institutional destabilisation**. By fostering corruption and undermining the rule of law, criminal organisations weaken the resilience of a state. A society that is riddled with corruption and lacks trust in its institutions is far more vulnerable to external psychological operations and political subversion.

Ultimately, we must stop viewing organised crime as a purely "police matter" and recognise it as a strategic tool in the "grey zone" of global conflict. This is why I advocate for an integrated security approach that bridges the gap between domestic law enforcement and international security policy. To effectively counter hybrid threats, we must understand and disrupt the criminal economies that fuel them.

Presumably, right off the bat, many experts and laypersons alike would think of terrorism when they hear the term 'hybrid threats.' Can you clarify the difference between organised crime and terrorism and can you say a few words about the role of the latter?

That is a very common and understandable association. While terrorism and organised crime often overlap in their methods and even cooperate in what we call the "crime-terror nexus," it is crucial to distinguish between them to develop effective countermeasures.

The fundamental difference lies in **motivation**:

Organised Crime is primarily **profit-driven**. Its goal is the accumulation of wealth and power within shadow economies. Criminal networks seek to bypass or corrupt the state to ensure their illegal business activities - be it drug trafficking, human smuggling, or money laundering - can continue undisturbed. They generally prefer the state to be weak and corruptible, but functional enough to provide a market.

Terrorism, on the other hand, is **ideologically or politically motivated**. Its goal is not financial gain, but the realization of, or implementing a specific political, religious, or social agenda. Terrorists use violence or the threat of violence to spread fear, polarise society, and force political change. Unlike organised crime, terrorism often seeks to challenge or even destroy the existing state order entirely.

In the context of hybrid threats, **terrorism** acts as a **force multiplier for destabilisation**:

Polarisation: Hybrid aggressors may support or instrumentalise terrorist groups to deepen existing rifts within a society. By provoking fear and extreme political reactions, terrorism can undermine the social cohesion of a nation, making it easier to manipulate from the outside.

Resource Exhaustion: Terrorist threats force a state to divert massive financial, legal, and personnel resources toward domestic security. This "internal fixation" can weaken a state's ability to focus on other hybrid vectors, such as economic subversion or geopolitical maneuvers.

The Nexus: We increasingly see a symbiotic relationship where terrorists use the logistical pathways and expertise of organised crime (e.g., weapons procurement or identity theft) to fund and execute their attacks. Conversely, criminal groups may adopt terrorist-like tactics to intimidate the state or "clear" a territory for their operations.

While organised crime is the **silent engine** that hollows out state structures through corruption and illicit economies, terrorism is the **loud explosion** designed to shatter public trust and provoke chaos. Both are essential components of the hybrid threat landscape, and as a practitioner-scholar, I argue that we must address them not as separate silos, but as part of an integrated security architecture.

In this context, the EU project RESONANT is particularly relevant; it analyzes how external actors manipulate online information and suppress content to shape narratives, especially targeting vulnerable groups.

What activities does organised crime typically engage in amidst hybrid attacks and do those differ from the type of organised crime we can witness in other contexts?

In the context of hybrid attacks, the activities of organised crime undergo a strategic shift where traditional criminal business models are repurposed to serve an aggressor's geopolitical goals. While organised crime typically operates in opposition to the state to maximise profit, in a hybrid scenario, it often acts as a strategic tool with the silent blessing or active support of a foreign power.

One of the most prominent activities is cyber-mercenarism, where state actors “outsource” ransomware attacks or the disruption of critical infrastructure to established criminal groups to maintain plausible deniability.

Furthermore, criminal networks are frequently instrumentalised to facilitate human smuggling, creating artificial humanitarian crises at borders to overwhelm local authorities and polarise the domestic political landscape.

Organised crime also provides the essential “grey” financial infrastructure to help hybrid actors bypass international sanctions or fund extremist groups, by using money laundering and shell companies.

The fundamental difference from conventional organised crime lies in the strategic alignment and the risk-reward ratio. In a hybrid context, criminal actions might be intentionally loud and disruptive because the goal is no longer just financial gain, but the systematic destabilisation of the target state. By acting as a logistical engine for sabotage and a catalyst for institutional corruption, organised crime hollows out a society’s resilience from the within. To effectively counter these threats, we must stop viewing such acts as isolated crimes and consider them as coordinated weapons in the “grey zone” of modern global conflict.

What are the ramifications of the current hybrid threats landscape in general and organised crime in particular?

The **ramifications** of the current hybrid threats landscape are **profound**, as they **challenge** the **traditional boundaries** between **internal** and **external security**, and between **legal** and **illegal spheres**. When we look at the impact of organised crime within this framework, we see consequences that extend far beyond mere criminal statistics.

The most insidious ramification is the gradual **erosion of the rule of law**. When organised crime is used as a tool for hybrid attacks - facilitated by corruption or state sponsorship - it hollows out public institutions.
If citizens perceive that the state is unable to control its borders, protect its critical infrastructure, or prevent large-scale financial manipulation, **trust** in **democratic governance diminishes**.
This internal weakening is a primary goal of hybrid warfare.

Hybrid threats create a **state of "permanent crisis".** By simultaneously attacking through various vectors for example like **cyberattacks**, **instrumentalised migration**, and **economic sabotage**, aggressors force security agencies into a reactive mode. For the **police** and **judicial** systems, this means dealing with crimes that are no longer just local or national, but part of a **global geopolitical strategy**. This leads to a massive strain on resources, as seen in the need for specialised units to handle the intersection of white-collar crime and national security.

In the realm of organised crime, the ramifications are **heavily financial**, including in the form of **economic distortion**. The "grey" infrastructure used for money laundering and sanction evasion distorts legitimate markets. When criminal networks handle billions of Euros in illicit flows, they don't just further their own economic gain; they gain the power to influence legal

economies and political decisions. This creates a "shadow governance" that competes with the state's economic authority.

General ramifications also include a mandatory shift in **how we organise our defencse or the way we create a modern security structure**. We can no longer afford to work in silos where the police handle crime and the military handles war. The current landscape demands an integrated approach. This is why my work as a practitioner-scholar focuses on bridging the gap between field-tested police experience and academic security research. We need hybrid solutions, combining law enforcement, intelligence, and political strategy, to counter hybrid threats effectively.

Another result of this landscape – and quite a challenging one - is that **security** has become **everyone's business**. Organised crime is the silent engine of this instability. To protect our societies, we must increase our institutional resilience, secure our digital and physical infrastructure, and, most importantly, **develop** a **deeper understanding** of the **criminal-political nexus that fuels these modern conflicts**.

What changes in the hybrid threats landscape have taken place in recent years and decades? What were those driven by?

The hybrid threats landscape has undergone a profound transformation especially over the last few decades, evolving from localised, sporadic interference into a sophisticated, permanent state of global competition.

We have shifted from a world of linear conflicts to a “grey zone” reality where the distinction between peace and war is increasingly **blurred**. This evolution has been primarily driven by three catalysts: **technological acceleration**, the pursuit of **asymmetric advantages**, and the **exploitation** of **institutional gaps**.

In recent years, the digital realm has become the primary theatre of operations. While hybrid tactics were once limited to **physical sabotage** or **traditional propaganda**, we now see a shift toward large-scale **cyber-mercenarism**. State actors increasingly utilise organised criminal groups to attack **critical infrastructure** or **paralyse public services** with ransomware, all while maintaining plausible deniability.

Furthermore, globalisation has been systematically instrumentalised; we now witness the **weaponisation** of **migration**, **energy**, and **supply chains**. Organised crime plays a crucial role here by providing the illicit logistical pathways to bypass international sanctions and move “grey” capital across borders.

This shift is also defined by the rise of **cognitive warfare**. Using social media algorithms and **AI-driven disinformation**, hybrid actors now target the “human domain” in form of the trust and **perceptions** of the **population** to **weaken** the **internal resilience of democratic institutions**.

Ultimately, the transition we have witnessed is one from event-based threats to structural vulnerability. As a practitioner-scholar, I argue that because **organised crime** has moved from

a **peripheral nuisance** to a **strategic engine** of this landscape, our security architecture must move beyond a silo mentality toward an integrated model that matches the complexity of these modern, hybrid networks.

Has digitisation been the single biggest driver of changing conflict dynamic?

While digitisation is undoubtedly the most visible and transformative catalyst of modern conflict, I would argue that it is not the single biggest driver, but rather the key enabler that allows other strategic drivers to converge. In the context of hybrid threats, digitisation acts as a force multiplier for three deeply interconnected factors.

Digitisation has fundamentally **lowered the entry barrier to global conflict and a disruption of democratisation**. Decades ago, destabilising a state required significant military or diplomatic capital. Today, through cyber-mercenarism and decentralised technologies, organised criminal groups and small state actors can project power that was previously used to require significant capabilities of power. This democratisation allows for constant, low-cost harassment of a target's critical infrastructure or financial systems, all while maintaining plausible deniability which is a core pillar of the hybrid landscape.

If we look at conflict as a contest of wills, digitisation has shifted the battlefield into the human domain. The rise of social media algorithms and AI-driven disinformation has turned information into a weapon that targets the internal resilience of a society. By amplifying social rifts and eroding trust in democratic institutions, aggressors can achieve strategic goals without firing a single shot. This **shift from physical destruction to cognitive subversion** is perhaps the most profound change in conflict dynamics, driven entirely by the digital revolution.

From my perspective as a practitioner-scholar, the most critical driver is the strategic **convergence of organised crime and state interests; a symbiotic relationship where states weaponise criminal networks, and criminals gain political protection.** Digitisation provides the "grey" infrastructure, such as cryptocurrencies, encrypted communication, and darknet marketplaces, that allows this nexus to flourish. While the desire for asymmetric advantage is the motivation for modern conflict, digitisation provides an environment where criminal networks can be instrumentalised as logistical engines for sabotage, sanction evasion, and illicit financing.

The primary driver remains the **geopolitical shift toward asymmetry** where **aggressors seek asymmetric advantages**. They have realised that conventional warfare is too costly and risky in a nuclear age. Therefore, they choose the "grey zone". Digitisation is the perfect tool for this strategy because it is inherently difficult to attribute, crosses borders instantly, and exploits the structural vulnerabilities of open, interconnected societies.

While digitisation has redefined the speed, reach, and anonymity of conflict, it is the underlying strategic intent to bypass conventional defense systems that remain the primary driver in keeping the balance of power. Digitisation has not just changed how we fight; it has

changed who can fight and where the fighting takes place. There is a shift in the focus from the physical border to the digital infrastructure and the minds of the citizens.

To counter this, our security architecture must evolve to be as integrated and agile as the digital networks that now define the landscape of modern threat. RESONANT will be part of the tools to enhance the security architecture.

How would you assess the current hybrid threats the EU is facing? What actors are behind those and how serious are they?

The current hybrid threat landscape facing the European Union is characterised by a high degree of volatility and a shift toward total competition below the threshold of open warfare.

I assess these threats as a systemic challenge to the resilience of our democratic institutions.

The EU is currently facing a multidimensional offensive. We see a "weaponization of everything", from energy and migration to information and legal frameworks. The focus has shifted from sporadic interference to a permanent state of "grey zone" conflict. The most critical threat today is the attack on social cohesion. By utilieing digital platforms and AI-driven disinformation, aggressors aim to polarise our societies and paralyse the political decision-making processes of the European Union and its member states.

The actors involved are diverse, often operating in a symbiotic nexus:

- **State Actors:** Primarily revisionist powers seeking to challenge the European security architecture. They provide the strategic intent and the massive resources required for long-term hybrid campaigns.
- **Organised Crime Networks:** As I highlighted in my research at the University of Cologne and my work on www.hybridthreats.org, criminal groups act and serve as the "logistical engine" for state actors. They provide plausible deniability for cyberattacks, sabotage, and the facilitation of instrumentalised criminal acts such like migration.
- **Proxy Groups and Cyber-Mercenaries:** These actors bridge the gap between crime and statecraft, conducting high-impact disruptions (such as ransomware or Distributed Denial of Service (DDoS) attacks, where a target system or network is overwhelmed with massive volumes of traffic from multiple sources, making it slow or completely unavailable) against critical infrastructure while allowing the state sponsor to remain in the shadows.

The seriousness of these threats cannot be overstated. They are not merely "nuisances"; they are existential challenges to the rule of law. When hybrid actors successfully hollow out public trust in institutions or bypass international sanctions through illicit financial flows, they weaken the very foundation of European Union member states' sovereignty. The risk of a strategic surprise, where multiple hybrid vectors converge to trigger a systemic collapse, is a real and present danger.

When comparing the current EU situation to conventional organised crime or historical case studies, the following conclusions can be drawn:

- **Similarities:** The **methods** remain **familiar**. Organised crime still uses corruption, illicit financial pathways, and logistical networks. The "business of crime" (smuggling, money laundering) is still the operational base.
- **Differences:** The **strategic intent** has **changed**. In traditional contexts, organised crime seeks to stay "under the radar" to maximise profit. In the EU's current threat landscape, these activities are often intentionally disruptive and aligned with the geopolitical goals of a foreign power.

Furthermore, the **scale and speed** provided by digitisation have turned localied criminal activities into tools of global destabilisation.

The European Union is no longer just dealing with "crime" or "espionage" in isolation; it is dealing with a global integrated, hybrid machinery of power.

Would you say that FIMI has been the core component of hybrid threats aimed at the EU?

As the website of the Diplomatic Service of the European Union states, FIMI "including disinformation, is a growing security and foreign policy threat for the European Union".[2]

While FIMI is arguably the most visible and pervasive element of the current threat landscape, I would characterise it not as the **core component** in isolation, but rather as the connective tissue that binds all other hybrid vectors together.

In my assessment, FIMI acts as the **psychological layer** that amplifies the impact of physical, economic, and criminal activities. It is the force multiplier that ensures a cyberattack or a manufactured border crisis achieves its ultimate goal: the destabilisation of public trust and the polarization of European society.

The reason FIMI often appears to be at the core of said activities is its ability to target the human domain directly. Unlike traditional tools of conflict below the threshold of war like espionage or sabotage, which target secrets or infrastructure, **FIMI targets** the **perceptions** of the **citizen**.

By utilising AI-driven disinformation and social media algorithms, hybrid actors can create an environment of permanent cognitive fog. This makes it difficult for democratic institutions to achieve the political consensus required to respond to other hybrid threats, such as energy blackmail or the instrumentalisation of migration. In this sense, FIMI is the tool used to paralyse the target's will to resist.

---

[2] European External Action Service. "Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)". Accessed 25 June, 2026 at https://www.eeas.europa.eu/node/410751_th.

However, we must be careful not to view FIMI in a vacuum. As my research into organised crime suggests, the true strength of a hybrid campaign lies in the nexus between the narrative and corresponding activities.

For example, a disinformation campaign is significantly more effective when it is supported by the logistical engine of organised crime, such as the illegal financing of extremist groups or the orchestration of local unrest.
While FIMI provides the weaponised narrative, organised crime often provides the deniable action on the ground. Without the underlying criminal and economic subversion, FIMI would be mere propaganda; with them, it becomes a strategic component of a coordinated hybrid attack.

The core of hybrid threats is not one specific technique like FIMI, but the strategic integration of all available means. For the EU, the challenge is that FIMI, as explained above, exploits the very openness and freedom of our liberal information space. Therefore, while we must treat FIMI as a priority for our cognitive defense, our policy remedies must remain holistic. We must secure our information environment while simultaneously disrupting the illicit financial flows and criminal networks that give these digital lies their physical weight. Only by addressing the entire "hybrid machinery" can we protect the sovereignty and resilience of the Union.

What are the remedies for the current form of hybrid threats?

Addressing the remedies for hybrid threats requires a fundamental shift from traditional, reactive security toward a model of total resilience. Because these threats specifically target the seams between our institutions, the solutions must be equally integrated and interdisciplinary. As a practitioner-scholar, I advocate for a four-pillar approach that begins with breaking down institutional silos.

1. We must move beyond a mindset where police, military, and intelligence agencies operate in isolation and instead establish integrated “fusion centers”. Such an architecture allows us to recognise, for instance, that a localised ransomware attack might actually be the first wave of a coordinated geopolitical campaign.
2. Furthermore, we must strengthen both institutional and social resilience. This involves investing in “cognitive defense” through media literacy to immunise the public against AI-driven disinformation, while simultaneously protecting our legal and financial systems from corruption.
3. A critical technical remedy is the “follow the money”-approach; by prioritising Financial Intelligence, we can disrupt the illicit logistical engines that hybrid actors use to fund their operations.
4. This must be coupled with improved forensic attribution to move these conflicts out of the “grey zone” and into the light of international law.

Ultimately, the most sustainable remedy lies in the bridge between field-tested experience and academic strategy, ensuring that our security architecture remains as agile and interconnected as the threats we face.

Do you have any policy recommendations thar are specifically tailored to the EU and its hybrid threats environment?

To effectively counter the unique hybrid threat environment of the European Union, policy recommendations must address the structural vulnerabilities of a supranational entity while leveraging its collective strength. I propose a multi-layered policy framework centered on the concept of **Interoperable Resilience.**

First, the European Union must move toward a **Mandatory Integrated Security Architecture**. Current cooperation often relies on voluntary participation; however, the transnational cross-border nature of organised crime and its role as a logistical engine for hybrid aggressors require a more binding framework. I recommend the establishment of an **EU Hybrid Intelligence & Operations Centre**, which would transcend existing silos by merging real-time data from law enforcement (e.g. Europol), intelligence services, and financial regulators. This would ensure that "weak signals", such as a localised cyberattack in one member state and instrumentalised migration in another, are recognised as a single, coordinated hybrid campaign.

Second, we must prioritise the **Disruption of Illicit Financial Ecosystems** through unified EU-wide compliance and data protection standards. My research highlights that hybrid threats are often financed through "grey" capital flows that exploit the varying regulatory strengths of affected states. A tailored policy should involve the creation of an **EU Financial Resilience Task Force** focused specifically on the crime-statecraft nexus.
By tightening the oversight of cryptocurrencies and shell companies, and ensuring that data protection serves as a security asset rather than a bureaucratic hurdle, the European Union can effectively starve hybrid aggressors of the criminal infrastructure they depend on for plausible deniability.

Third, the European Union should implement a **Societal Shield Initiative** focused on cognitive defence. Since the target of hybrid warfare is the trust of the European citizens in their governments and institutions, policies must go beyond technical cybersecurity to address "human domain" vulnerabilities. This includes EU-wide standards for media literacy and a rapid-response mechanism for debunking AI-driven disinformation campaigns.

Finally, the EU should foster a **Practitioner-Scholar network**, building on the work done by think tanks like CEPOLIS and EU-funded projects like RESONANT, ensuring that security policy is not just top-down but informed by field-tested data from first responders. By combining these strategic, financial, and societal measures, the European Union can transform from a target of hybrid interference into a resilient, proactive security actor.

How should the collaboration between different stakeholders required to mitigate hybrid threats (e.g. law-enforcement, the defence sector, technical developers and entrepreneurs, social media providers etc.) be organised?

Organising the collaboration between such a diverse array of stakeholders requires a shift from hierarchical, reactive structures toward a circular, multi-stakeholder ecosystem that operates in real-time.

To mitigate hybrid threats effectively, the collaboration must be anchored in a whole-of-society-approach, structured around three core organisational principles: shared situational awareness, cross-sectoral operational hubs, and a secure legal framework for data exchange.

At the centre of this organisation should be **Integrated Hybrid Fusion Centres**. These are not merely meeting rooms, but permanent operational hubs where law enforcement and the defence sector work side-by-side with technical developers, private industry and entrepreneurs. In this environment, the defence sector provides geopolitical intelligence, while law enforcement contributes domestic investigative data on organised crime, which can be identified as the logistical engine of hybrid warfare. The **inclusion** of **private industry**, **technical entrepreneurs** and **developers** is crucial; they provide the necessary agile innovation, which is needed to match the speed of aggressors, ensuring that security tools for encryption, attribution, and infrastructure protection are developed as quickly as the threats evolve.

The **collaboration** with **social media providers** and **tech companies** must be organised through a public-private resilience partnership. Instead of purely adversarial regulatory relationships, this should be a proactive alliance **focused** on **cognitive defence**. Policy frameworks must be established to allow for the rapid sharing of threat indicators regarding AI-driven disinformation or cyber-mercenary activity without compromising user privacy or data protection.

By involving social media providers directly in the defence architecture, the EU and its member states can create an **early-warning system** that **identifies** and **neutralises** weaponised **narratives** before they achieve widespread social polarisation.

Furthermore, this collaboration requires a translational layer, a role often filled by practitioner-scholars but also research institutes like CEPOLIS. These actors act as knowledge brokers who translate high-level academic and military strategy into actionable protocols for local, national and international police officers and private (industry) security managers. This ensures that the first responders on the ground understand their role within the larger hybrid conflict, whether they are patrolling the streets or managing a server farm.

Ultimately, the organisation of these stakeholders must be underpinned by mutual trust and standardised protocols. We need pre-defined "rules of engagement" for the grey zone that stipulate how and when a private entrepreneur or a social media platform should escalate a detected anomaly to national security authorities. By creating a networked defence that is as flexible and interconnected as the hybrid threats themselves, we can transform our structural vulnerabilities into a collective, resilient shield.

Thank you!