THE SHADOW FIMI OSINT REPORT:

ACTORS THE EU WILL NOT NAME

A FIMI-Methodology Assessment of US, Israeli and Aligned Network Interference in European Democracy[1]

Published 17 March 2026 — In Response to the 4th EEAS FIMI Report

> *'Tyranny is our foe, whatever trappings or disguise it wears, whatever language it speaks, be it external or internal, we must forever be on our guard, ever mobilised, ever vigilant… If we are together nothing is impossible. If we are divided all will fail.'*[2]

EXECUTIVE SUMMARY

A Framework Applied & Targets Omitted

Whilst the official 4th EEAS FIMI Report names Russia and China as primary threats, this "Shadow Report" utilises the EU's own DISARM Framework and STIX 2.1 data standards to document a parallel, poorly addressed axis of interference. The report argues that the European External Action Service (EEAS) is making a political choice by limiting forensic analysis of the documented operations from the United States Israel, and private tech-oligarchs collaborating with the administrations of those countries from its official FIMI Explorer database.

Donald Tusk named the combined threat explicitly in March 2026:

> '*those who want to destroy the Union are: Russia, American MAGA, and the European right wing led by Orbán.*'[3]

It is also crucial to note that the absence of a single director or controlling agent is not evidence of absence of coordination. It is a feature of the architecture.

Key Investigative Pillars for 2026

1. The "Generative FIMI" Escalation

The report identifies 2026 as the year influence operations moved from human-led coordination to autonomous LLM botnets.

- **Case Study:** "Prawilne Polki" (Poland): A fully documented operation using AI-generated personas and LLM-produced content to amplify pro-Polexit narratives.
- **The "CopyCop" Nexus:** A Russian-linked network using self-hosted, uncensored LLMs to mass-produce fabricated news and deepfakes (e.g., German FM Baerbock) at industrial scale.

---

[1] Prepared using various AI tools (Gemini, Claude, Notebooklm) as well as human learning.
[2] Winston Churchill, '*The Gift of a Common Tongue*', September 6, 1943. Harvard. The two passages are drawn from the same speech; the ellipsis indicates non-adjacent text.
[3] Donald Tusk, post on X, March 2026. Confirmed in RBC-Ukraine, *'Donald Tusk warns of Poland's potential exit from EU'*, 14 March 2026.

- **Data Poisoning:** Strategic flooding of the internet with synthetic "news" to contaminate the training data used by other AI assistants and search engines.

2. Tech-Oligarchs as Sovereign Threats

The report introduces a new category of "coercive interference" driven by the vertical integration of digital infrastructure.

- **The Musk Vector:** X is assessed as an "active FIMI delivery system". Documented interventions include Musk's direct endorsement of the AfD in Germany and his threats to withdraw Starlink from Europe as retaliation against Digital Services Act (DSA) enforcement.
- **The Thiel Vector:** Palantir and Anduril are described as "privatized intelligence infrastructure" positioning themselves as the data layer of European military sovereignty while being led by figures who explicitly reject democratic compatibility.
- **The "Private Emanation" Doctrine:** The report introduces a foundational premise — that Musk, Thiel, and their companies must be classified not as private actors but as private emanations of the American state, receiving operational existence from $38 billion+ in government contracts and subsidies while exercising state-scale power without state-level accountability. This classification is the precondition for applying the FIMI framework to their documented interventions. **An actor-agnostic framework that cannot reach outsourced sovereignty cannot reach the dominant interference vector of 2026.**

3. The Lobbying-to-FIMI Pipeline

A major policy finding is the "legislative capture" of the EU Corporate Sustainability Due Diligence Directive (CSDDD).

- **Threshold Crossing:** The report distinguishes legitimate lobbying from FIMI when it involves "coordinated manipulative behavior," such as the BLOOM investigation's discovery of US fossil fuel lobbies using astroturfing and manufactured pressure to dismantle democratically agreed-upon legislation.
- **Institutional Hubs:** The Danube Institute (Hungary) is identified as a fiscal switchboard, using EU-sourced state funding to bridge US MAGA donors and European far-right networks.

4. Spyware as an Intelligence Loop

The report connects the Pegasus spyware scandal to subsequent FIMI campaigns.

- **The Loop:** Data harvested from hacked EU officials informs the strategic targeting of narrative-driven influence operations, creating a "precision data layer" for interference.
- **Hybrid Threat Modelling:** Applying the joint ENISA-EEAS framework to Pegasus produces a "Tier 1 hybrid threat" assessment that remains unacknowledged in official EU reporting.

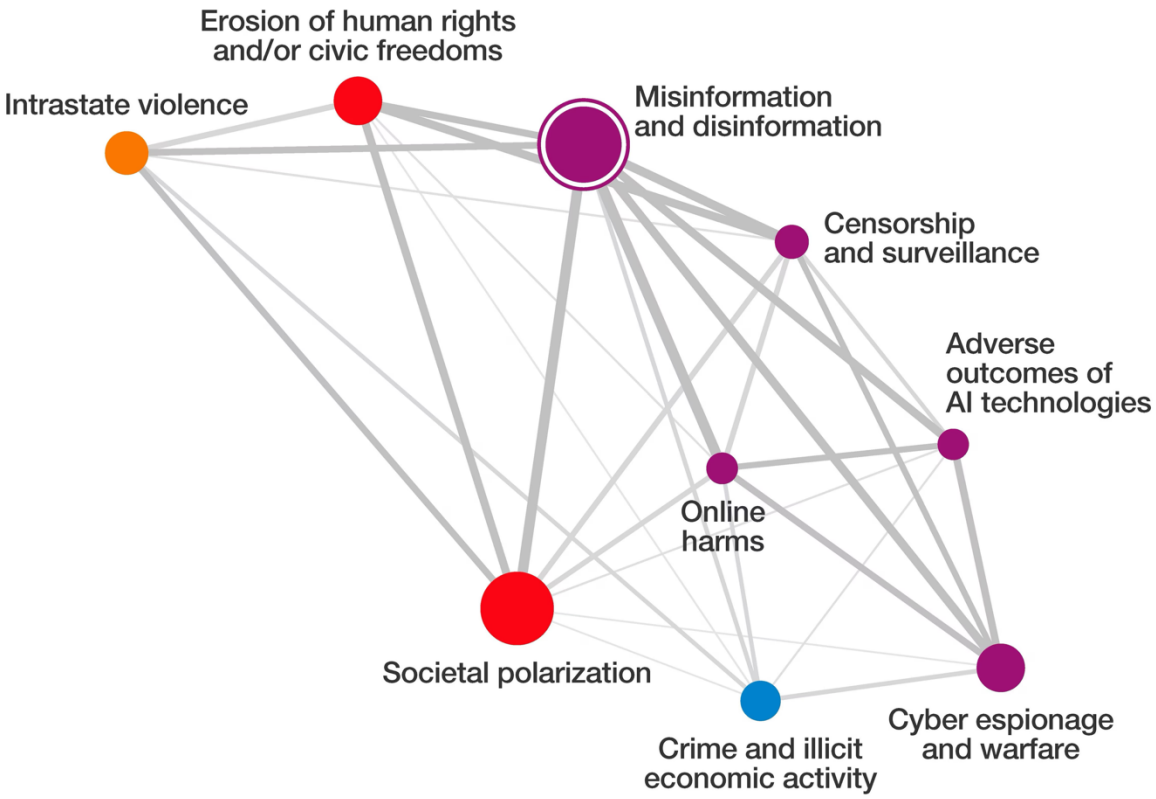
Proposed Policy Solutions

The report advocates for three structural shifts to bridge these gaps:

- **Independent FIMI Ombudsman:** To receive and investigate complaints outside the EEAS diplomatic chain, preventing member-state vetoes (e.g., by Hungary) from suppressing findings.
- **Digital Sovereignty Stress Tests:** Mandatory audits of critical EU dependencies on "politically-exposed vendors" like Starlink or Palantir.
- **The "Non-Interference Clause":** Standardizing contract termination triggers for tech vendors who use infrastructure as coercive leverage against democratic oversight.

Global Risks Report 2025

Risk interconnections: Misinformation and disinformation



Relative influence, Edges — High — Medium — Low

Risk influence, Nodes ◯ High ◯ Medium ◦ Low

Risk categories Economic Environmental Geopolitical Societal Technological

Source: World Economic Forum, Global Risks Perception Survey 2024-2025

PREAMBLE: WHY THIS REPORT EXISTS

This report is the second in a series. The first — *'A New Axis Powers?'* — was published in March 2025 as an unofficial companion to the 3rd EEAS FIMI Report.[4] It documented, on the basis of open-source evidence, a correlated axis of interference against European democracy by Russia, MAGA America, and Israeli Likud-aligned networks — operating through European far-right movements and enabled by a FIMI framework too diplomatically constrained to name them.

The 4th EEAS FIMI Report, published today, confirms that assessment by omission. The EU's High Representative Kaja Kallas framed the challenge correctly:

> '*Today's wars are not only fought with tanks and drones. They are also fought with lies and algorithms. FIMI is a weapon aimed at the heart of our democracies.*'[5]

She is right. But the report published under her authority today names Russia & China (again) as the primary threat actors. It will still not call out properly the extraordinary hybrid interference and influence of the current administrations of the United States and Israel (our erstwhile allies). This report does.

The 4th Report documents 65% of all incidents as 'unattributed' — a category that, by the report's own methodology, includes channels 'aligned with' threat actors. The Shadow Report documents that a significant portion of this 65% is operationally attributable to MAGA-aligned and Israeli actors using the same DISARM methodology the EEAS applies to Russian infrastructure.

The EU's FIMI framework was co-designed with the United States in June 2021 and claims to be **actor-agnostic** — applicable to any foreign power regardless of alliance status.[6] Academic analysis has asked directly: '*Will the EU address Elon Musk's interference in European public opinion?*'[7] — a question the EEAS has not properly answered now in four annual reports.

This report applies identical FIMI methodology to the actors that the EU's own framework excludes by political choice, not analytical necessity. It is not anti-American or anti-Israeli. It is pro-democratic.

A note on methodology: the FIMI framework defines interference as meeting four criteria simultaneously — **intentional, coordinated, manipulative, and contrary to democratic values.** Legitimate lobbying becomes FIMI when it crosses into **coordinated manipulative behaviour**: astroturfing, manufactured grassroots movements, systematic deception of legislators, and suppression of counter-narratives. Multiple operations documented in this report meet that threshold. The distinction is made explicit in each case.

A Note on Technical Methodology: DISARM, STIX, and the Unified Kill Chain

This report does not merely apply the EU's four-part conceptual FIMI definition. It maps the operations documented herein using the precise analytical frameworks the EEAS itself uses to track Russian and Chinese threats.

---

[4] *'A New Axis Powers?'*, Compossible Blog, 22 March 2025: https://compossible.blog/2025/03/22/a-new-axis-and-the-international-far-right/

[5] Kaja Kallas, FIMI Conference statement, Brussels, 23 February 2026. YouTube transcript, *'Wars Are Fought With Lies & Algorithms! Kaja Kallas'*, 22 February 2026.

[6] EEAS 2022 Annual Report on Activities to Counter FIMI, p.4: *'The methodology is actor-agnostic — it can be applied no matter the source of FIMI or the region where it is employed.'* EU-HYBNET, 2022.

[7] Proto, A. et al., *'The EU's FIMI Turn: How the European Union External Action Service Constructs the FIMI Threat'*, Media & Communication, 2025.

The DISARM Framework — DISinformation Analysis and Risk Management — is an open-source framework designed to describe and understand disinformation campaigns using Tactics, Techniques, and Procedures (TTPs), structured identically to cybersecurity threat intelligence.[8] The EU standardised detection and response to FIMI using the DISARM-STIX method, now used by the Data Analysis Team in the EEAS Strategic Communications division (SG.STRAT.2).[9]

STIX 2.1 (Structured Threat Information Expression) is the data format used to encode and exchange these threat assessments — and it is explicitly applicable to FIMI incidents by breaking them down into their constitutive operational elements.[10]

The Unified Kill Chain maps the complete lifecycle of an influence operation — from initial planning through narrative placement, amplification, and policy impact — and is used alongside DISARM in EU assessments of Russian operations.[11]

The operations documented in this report have been assessed against these frameworks. Selected DISARM TTP mappings are provided below. The finding is unambiguous: the US and Israeli operations documented here fit perfectly into the exact tactical data models the EU uses to track Russian threats. The analytical gap is not methodological, it is political.

DISARM TTP Mapping: Selected Operations

Operation	DISARM Tactic	DISARM Technique	STIX Object Type
CPAC Poland / Noem speech	TA06: Develop Content	T0023: Distort facts; T0049: Flooding information space	threat-actor, campaign, attack-pattern
BLOOM/CSDDD legislative capture	TA07: Select Channels	T0059: Astroturfing; T0046: Search engine manipulation	threat-actor, relationship, campaign
Musk electoral interventions (AfD, UK, Poland)	TA09: Deliver Content	T0040: Demand content removed; T0043: Repurpose legitimate channels	threat-actor, tool, attack-pattern
Prawilne Polki AI campaign	TA05: Microtarget	T0085.003: LLM-generated personas; T0084: Fabricate content	malware, attack-pattern, indicator
Pegasus intelligence loop	TA02: Plan Strategy	T0078: Targeted data collection enabling FIMI targeting	tool, vulnerability, observed-data

[8] DISARM Foundation, DISARM Framework Documentation, v1.4, 2023; Hybrid CoE Research Report 7, '*Foreign Information Manipulation and Interference Defence: Applying the DISARM Framework*,' November 2022.
[9] PISM, '*EU Adopts Approach to Countering Foreign Information Manipulation and Interference*,' June 2024: 'The EU aims to standardise the detection and response to FIMI based on the DISARM-STIX method, used, among others, by the Data Analysis Team in the Strategic Communications, Task Forces and Information Analysis Division (SG.STRAT.2) of the European External Action Service.'
[10] FERMI Project / EU DisinfoLab, '*Structured Threat Information Expression (STIX™),*' 2022: 'The STIX format can also be utilized to share information about FIMI incidents, by breaking them down into their different constitutive elements.'
[11] EEAS TTC Ministerial, 'Foreign Information Manipulation and Interference,' May 2023, Annex 3, p.2.

Agency for Social Design (Hungary)	TA11: Persist in Environment	T0094: Build network; T0049: Flooding information space	threat-actor, campaign, infrastructure
Voice of Europe MEP payments	TA07: Select Channels	T0092: Cultivate ignorant agents; T0104: Corrupt legislature	threat-actor, relationship, campaign

Kill Chain Stage Assessment

The documented operations collectively span all six stages of the Unified Kill Chain as applied to FIMI:

- **1. Reconnaissance:** Pegasus intelligence harvest targeting EU officials
- **2. Weaponisation:** LLM content generation (Prawilne Polki, CopyCop methodology)
- **3. Delivery:** X algorithmic amplification; CPAC platform provision
- **4. Exploitation:** Legislative capture (CSDDD); Electoral coercion (Poland)
- **5. Installation:** Institutionalisation of interference infrastructure (Danube Institute, PNfV, CPAC permanent offices)
- **6. Command & Control:** Kiriyenko/ASP operational oversight; Musk DOGE-government dual role

The EEAS FIMI Explorer has attributed operations at every Kill Chain stage to Russian actors. The identical methodology applied to the operations documented in this report produces equivalent attributions for US and Israeli actors. Their absence from the database cannot be explained on methodological grounds.

PART I: THE BREXIT-TO-POLEXIT THROUGHLINE

Brexit (2016): The Template

Arron Banks's Leave.EU campaign actively sought US funding and strategic support from Cambridge Analytica — co-founded by Steve Bannon and backed by Robert Mercer — from as early as October 2015.[12] Emails published by the New Yorker and CNN confirm Banks wrote to Bannon seeking *'a strategy for fundraising in the States'* and gave Cambridge Analytica access to Leave.EU data and supporters.[13] This constituted a coordinated transatlantic operation to remove the UK from the EU — funded partly through channels that UK electoral law prohibited.[14]

The UK's Intelligence and Security Committee possessed evidence of both Russian and US-aligned interference before the referendum. It was suppressed until November 2019. The ISC Russia Report concluded that Russian interference in UK politics had not been treated as a major threat — an assessment that has been confirmed by subsequent events.[15]

The same failure — evidence possessed, politically suppressed — is now repeating inside the EU.

[12] Bannon-Banks emails, CNN, 17 November 2018; OpenDemocracy dark money investigation, 16 November 2018.
[13] *'New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexit'*, New Yorker, 17 November 2018.
[14] OpenDemocracy, *'Brexit bankroller Arron Banks, Cambridge Analytica and Steve Bannon'*, 16 November 2018.
[15] Intelligence and Security Committee of Parliament, *Russia Report*, HC 632, 21 July 2020, p.3.

Polexit (2025-26): The Same Network, Institutionalised

US Homeland Security Secretary Kristi Noem stood at CPAC Poland on 27 May 2025 — five days before the Polish presidential run-off — and stated:

> '*We need you to elect the right leader. You will be the leaders that will turn Europe back to conservative values.*'[16]
>
> '*If you elect a leader who will work with President Donald J. Trump, the Polish people will have a strong ally… You will continue to have a US military presence here… and you will have equipment that is American made, high quality.*'[17]

She dismissed Nawrocki's pro-EU rival Rafał Trzaskowski as *'an absolute train wreck of a leader'* — a sitting US cabinet secretary actively campaigning against a democratic candidate in an EU member state election.[18]

Trump simultaneously hosted Nawrocki at the White House during the campaign.[19]

The FIMI ISAC monitoring consortium documented that it was reported Nawrocki deployed a fabricated expert persona — 'Tadeusz Batyr' — on Polish state television from as early as 2018, using face obscuring and AI-modified voice to pose as an independent historian endorsing his achievements. He was therefore not merely a beneficiary of FIMI operations — he was a practitioner of their methodology before the campaign began.[20]

The 4th EEAS Report's documented three-phase Russian electoral interference playbook — applied explicitly to the German election — maps onto the parallel CPAC-MAGA-ASP operations this report documents across both Germany and Poland. It maps precisely onto the CPAC-MAGA-ASP operations this report documents. The difference is attribution: **the EEAS attributes only the Russian layer, leaving the MAGA layer invisible**.[21]

The Structural Continuity: Bannon to CPAC

Matthew Tyrmand — Bannon associate, Breitbart contributor — cultivated PiS networks in Poland from 2016. CPAC's deliberate geographic expansion followed:

1. **CPAC Hungary (2022)** — Orbán addresses CPAC Dallas same year
2. **CPAC Poland (2025)** — timed directly for presidential election
3. **Permanent Central European infrastructure (2026)** — institutionalising what was ad hoc in 2016

---

[16] Kristi Noem, CPAC Poland speech, Jasionka, 27 May 2025. NPR, *'Noem urges Poles to elect Trump ally as CPAC holds its first Poland conference'*, 27 May 2025.
[17] Notes from Poland, *'Trump security secretary Noem endorses Polish conservative presidential candidate at CPAC'*, 26 May 2025; Bloomberg, 27 May 2025.
[18] Notes from Poland, op. cit.
[19] Reuters, *'Trump signals Poland could get more US troops during Nawrocki White House visit'*, 3 September 2025.
[20] FIMI ISAC, *Poland FIMI Report*, op. cit., p. 88.
[21] *4th FIMI Report*, p.15.

The German Marshall Fund confirmed: CPAC is ’giving European grievances US dollars.’[22]

Post-Election: Bypassing the Elected Government

After Nawrocki's inauguration (August 2025), MAGA involvement shifted from electoral to governmental interference: Trump sent a presidential delegation to the inauguration; Nawrocki excluded Polish government ministers from his Washington delegation; Trump intervened to ensure Nawrocki — not Prime Minister Tusk — joined a Ukraine peace call with European leaders.[23] In February 2026, the US Ambassador cut formal ties with Sejm Speaker Hołownia — described by Poland's Foreign Ministry as ’outrageous.’[24]

FIMI Assessment: This operation meets all four FIMI criteria — intentional, coordinated, manipulative, contrary to EU democratic values.

[22] EUObserver, *'CPAC in Poland and Hungary — giving European grievances US dollars'*, 21 January 2026.
[23] New York Times, *'Trump Welcomes Poland's Right-Wing President to White House'*, 3 September 2025; Reuters, op. cit.
[24] Brussels Signal, *'US interferes in Polish politics, cutting ties with Speaker of Sejm'*, 6 February 2026.

PART II: US MAGA — DOCUMENTED OPERATIONS

This report applies a foundational analytical premise that the Preamble requires stating explicitly: **Musk, Thiel, and their associated companies must be understood not as private actors who happen to hold political opinions, but as private emanations of the American state** — entities that receive their operational existence, financial sustenance, and geopolitical leverage from government contracts, subsidies, and state backing, while deploying that power without the diplomatic, legal, or democratic constraints that govern state actors directly. A company that could not exist without $38 billion in government funding, whose AI tools are embedded in a US government efficiency operation, and whose satellite infrastructure underpins US military communications is not a private actor in any meaningful sense. It is outsourced sovereignty — state power exercised through a private shell. **The FIMI framework was designed to be actor-agnostic. If it cannot reach public-private actors, it cannot reach the primary vector of interference documented in this report**.

Actor → Behaviour → Content → Target: The FIMI Matrix Applied

- **Actors:** Trump administration officials; CPAC/American Conservative Union; Heritage Foundation; Danube Institute; American Chamber of Commerce; aligned donor networks (Bradley/Coors/Koch/Scaife/Uihlein family networks, contributing over $120 million to Project 2025 organisations)[25]
- **Behaviour:** Direct electoral endorsement; platform provision; conditional security guarantees; ambassador interference; legislative lobbying crossing into coordinated manipulative behaviour
- **Content:** Anti-EU sovereignty narratives; Polexit-compatible messaging; climate legislation framed as economic self-harm; undermining of Tusk government
- **Targets:** Polish presidential election 2025; European Parliament legislative process; EU defence integration; EU climate and corporate accountability legislation

Documented Incident Timeline

Date	Actor	Action	Source
May 2025	Trump	Hosts Nawrocki at White House during campaign	Reuters, Sep 2025[26]
May 2025	Kristi Noem	CPAC Poland electoral endorsement	NPR, May 2025[27]
May 2025	Orbán	Endorses Nawrocki at CPAC Hungary	Reuters, May 2025[28]

[25] *'A New Axis Powers?'*, Compossible Blog, March 2025, Heritage Foundation/Atlas Network section; Yorkshire Bylines, *'Right-wing push to dismantle the EU: Heritage Foundation's private workshop'*, 25 March 2025.
[26] Reuters, *'Trump signals Poland could get more US troops during Nawrocki White House visit'*, 3 September 2025.
[27] NPR, *'Noem urges Poles to elect Trump ally as CPAC holds its first Poland conference'*, 27 May 2025.
[28] Reuters, *'Hungary's Orban backs Polish nationalist presidential candidate Nawrocki at CPAC'*, 29 May 2025.

Jun 2025	Nawrocki	Wins Polish presidency	CNN, Aug 2025[29]
Sep 2025	Trump	White House meeting; Ukraine call intervention	Reuters, Sep 2025[30]
Sep 2025	Nawrocki	Excludes Polish government from Washington	NYT, Sep 2025[31]
Feb 2026	US Ambassador	Cuts ties with Sejm Speaker	Brussels Signal, Feb 2026[32]
Mar 2026	Nawrocki	Vetoes EU SAFE defence funding	IEU Monitoring, Mar 2026[33]

The BLOOM Investigation: When Lobbying Becomes FIMI

The BLOOM/Der Spiegel/Aftonbladet investigation (February 2026) documented how US fossil fuel lobbies and Trump administration networks crossed from legitimate lobbying into **coordinated manipulative behaviour** — the threshold at which lobbying becomes FIMI.[34]

Swedish EPP MEP Jörgen Warborn met American Chamber of Commerce lobbyists more than **ten times in under a year** — a record for any MEP — before becoming rapporteur for the Omnibus that dismantled the EU Corporate Sustainability Due Diligence Directive (CSDDD). The operation involved:

- Coordinated visits to Washington by multiple EPP politicians meeting Heritage Foundation officials
- Funding flows from multinationals and the Danube Institute to aligned MEPs
- Manufactured political pressure framing EU corporate accountability as economic self-harm
- Suppression of counter-narratives through coordinated messaging across multiple platforms

BLOOM described the result as *'an unprecedented act of normative regression'* and formally submitted evidence to the European Parliament's Advisory Committee on Conduct of Members.[35]

This is FIMI measured not in elections won or lost, but in **legislation destroyed**. The FIMI framework's Deterrence Playbook — introduced in the 4th Report — addresses financial flows and organisational

[29] CNN, *'Karol Nawrocki sworn in as Polish president, in blow for Tusk'*, 6 August 2025.
[30] Reuters, op. cit., September 2025.
[31] New York Times, *'Trump Welcomes Poland's Right-Wing President to White House'*, 3 September 2025.
[32] Brussels Signal, op. cit., February 2026.
[33] IEU Monitoring, *'Poland's SAFE dispute deepens as President vetoes EU defence loan'*, March 2026.
[34] BLOOM Association, *'BLOOM releases an explosive investigation into US interference in the European Parliament'*, 4 February 2026.
[35] *Ibid*. Also: BLOOM Association, *'EPPgate: the European right wing in turmoil since our revelations'*, 16 February 2026.

intermediaries. It does not yet include a category for legislative capture through coordinated lobbying. The BLOOM operation meets the FIMI definition but falls between the Playbook's deterrence layers. This gap requires explicit legislative language.

The 'Economic Doom' Narrative Operation

The Green Deal dismantling is not merely legislative capture — it is a **narrative operation** that weaponises economic anxiety using FIMI methodology. The documented elements:

- US fossil fuel lobby messaging — coordinated through ExxonMobil, Chevron, Koch Industries, and the American Petroleum Institute (API), using 'precarious trade negotiations' and Trump's 'energy dominance' agenda to frame EU climate laws as a competitive disadvantage explicitly frames EU climate regulation as economic self-harm, deployed through the same channels as other FIMI content
- This narrative flows through far-right MEPs, Orbán's state media, and X amplification simultaneously — meeting the coordinated and manipulative criteria
- It produces measurable political outcomes: Green Deal rollback, CSDDD destruction, climate scepticism normalisation in the mainstream EPP

The narrative originated in US think tanks (Heritage, Atlas Network) and was delivered into EU legislative processes through documented lobbying operations.[36] This is the clearest example of the **lobbying-to-FIMI pipeline** — where coordinated manipulative messaging designed to manufacture false public consent crosses the definitional threshold into interference.

The IDU Network: Named Actors in the Legislative Capture Operation

The BLOOM/Der Spiegel Warborn in the USA investigation identified specific named US political actors who participated in the International Democracy Union (IDU) network connecting US Republican politicians with European EPP MEPs — the precise channel through which MAGA-aligned legislative pressure was transmitted into EU policy processes.[37]

The named actors include:

- **Senator Dave McCormick (R-Pennsylvania)** — participated in IDU network meetings with European EPP politicians as part of coordinated Heritage Foundation-aligned legislative strategy.
- **Representative Brian Fitzpatrick (R-Pennsylvania)** — former FBI special agent and House Foreign Affairs Subcommittee member on Europe; participated in IDU coordination with EPP MEPs.
- **Representative Don Bacon (R-Nebraska)** — IDU network participant in coordinated engagement with European conservative politicians.

[36] Yorkshire Bylines, op. cit.; DesSmog, *'From Denial to Delay: How the Far-Right is Orchestrating Climate Backlash in the European Parliament'*, 30 July 2025.
[37] BLOOM Association, '*Warborn in the USA'* investigation, 4 February 2026; '*EPPgate: the European right wing in turmoil since our revelations*,' 16 February 2026.

- **Former US Ambassador Robert O'Brien** — facilitated IDU network connections between Trump administration officials and European EPP politicians, providing diplomatic-level cover for what was in operational terms a coordinated legislative influence campaign.[38]

The IDU is the institutional vehicle through which the MAGA-EPP legislative alignment documented by BLOOM was operationally coordinated. It is not a diplomatic channel — it is an undisclosed political influence network operating inside EU legislative processes. Under DISARM taxonomy, this maps precisely to T0092: Cultivate Ignorant Agents and T0104: Corrupt Legislature.

The specific vehicle — the Omnibus dismantling the CSDDD — involved EPP rapporteur Jörgen Warborn's dual roles in SME Europe (EPP-affiliated) and SME Global (international counterpart organisation), whose funding sources have never been fully disclosed. Both organisations functioned as transmission vehicles for US corporate interests into EU legislative processes while maintaining the appearance of European civil society representation.[39]

The Legitimate Diplomacy Test

The FIMI framework distinguishes legitimate political engagement from interference by four criteria — intentionality, coordination, manipulation, and incompatibility with democratic values. A diplomatic visit meets none of these criteria by definition. The operations documented in this report are distinguished from legitimate diplomacy by the following observable features:

Legitimate Diplomatic Visit	FIMI Threshold Crossing
Disclosed actor, registered channel	Fabricated personas (Batyr), astroturfed civil society
Policy argument addressed to democratic institutions	Narrative designed to bypass public deliberation
Does not target specific electoral candidates	Noem directly names and campaigns against Trzaskowski
Subject to host-country transparency rules	IDU coordination concealed through think-tank intermediaries
Does not condition security guarantees on electoral outcomes	Explicit linkage: US troops for right candidate

The conditionality of the Noem speech is not diplomacy. It is electoral coercion using security leverage. It maps to DISARM T0023 (Distort facts about consequences) and T0049 (Flooding information space with fear-based content). No legitimate diplomatic communication does this.

[38] *Ibid*. IDU network participants identified in Warborn in the USA investigation documentation.
[39] *Ibid*. Funding disclosure demands for SME Europe and SME Global submitted as part of BLOOM's formal complaint to the EP Advisory Committee on Conduct of Members.

PART III: ISRAELI OPERATIONS — DOCUMENTED INTERFERENCE

Pegasus: Spyware as Diplomatic Currency

The European Parliament's PEGA Committee of Inquiry (2022-23) confirmed a foundational finding:

> 'There is a close connection between the trade in spyware and diplomatic relations.'[40]

Hungary and Poland both purchased Pegasus following personal meetings between Orbán, Kaczyński, and Netanyahu. The spyware was then used against:

- **Top EU Commission officials** (confirmed, Euronews, July 2022)[41]
- **Opposition politicians** in Hungary and Poland
- **Journalists and lawyers** inside EU member states
- **Civil society organisations** tracking democratic backsliding

The PEGA Committee's final report concluded that the abuse of spyware '*directly undermines fundamental rights and democracy, the core values on which the EU is founded*' — a finding that, applying the joint ENISA-EEAS hybrid threat framework, constitutes a Tier 1 FIMI-adjacent threat that has never received a formal EU attribution.[42]

The Intelligence Loop: Pegasus to Influence Operations

The integration of Israeli spyware creates a **precision data layer** for targeted FIMI operations. Pegasus harvested communications data from EU officials, opposition figures and journalists — data that informs strategic targeting of subsequent influence campaigns. This represents a qualitatively different threat from Russian disinformation: not merely narrative manipulation, but intelligence-grade targeting of democratic actors based on intercepted private communications.[43]

EPP MEP Lukas Mandl actively attempted to remove Netanyahu's name from the PEGA report and delete references to the Israel-Hungary-Poland purchase connection — documented interference in the Parliament's own oversight function.[44] This secondary layer — the corruption of democratic accountability mechanisms — is as significant as the primary Pegasus operation itself.

Israel suspended Pegasus export licences to two unnamed EU governments for misuse — acknowledging the tool was used against democratic targets inside the EU — yet no EU formal FIMI attribution has been published.[45]

PRISONBREAK: Israeli AI-Enabled FIMI — The Citizen Lab Assessment

---

[40] European Parliament PEGA Committee Report, *'Report on the use of Pegasus and equivalent surveillance and spyware'*, A9-0189/2023, 8 May 2023, paragraph 47.
[41] Euronews, *'Top EU officials hacked by Israeli Pegasus spyware'*, 27 July 2022.
[42] PEGA Committee Report, op. cit.
[43] CEPA, *'Pegasus Surveillance Plagues Democratic Europe'*, July 2023.
[44] Electronic Intifada, *'How an EU lawmaker tried to whitewash Israel's role in spyware scandal'*, 14 November 2023.
[45] CEPA, op. cit.

In October 2025, the Citizen Lab published forensic analysis of **PRISONBREAK** — a coordinated network of over 50 inauthentic accounts on X, assessed with medium confidence as linked to Israeli government or contractor involvement.[46] The operation was synchronised with IDF military strikes against Iran in June 2025 and deployed AI-generated imagery, fabricated news stories, and LLM-generated personas to incite internal revolt against the Iranian government.[47]

PRISONBREAK is analytically significant for this report for three reasons:

- **It is the first documented Israeli AI-native FIMI operation** — moving beyond Pegasus's passive intelligence harvest into active narrative manufacturing using the same LLM techniques documented in the CopyCop and Prawilne Polki cases (see Part VIII)
- **It demonstrates operational capability transferability** — a network built to target Iranian domestic audiences can be reoriented toward European targets using identical infrastructure, with persona language and cultural authenticity adjusted via the same LLM tooling
- **It maps directly onto DISARM TA05 (Microtarget) and T0085.003 (LLM-generated personas)** — the same DISARM taxonomy applied to the Prawilne Polki AI campaign in the Preamble's TTP mapping table

The 4th EEAS FIMI Report, covering all of 2025, contains no assessment of PRISONBREAK. The Citizen Lab's methodology — network forensics, persona analysis, content attribution — is identical to the EEAS's own documented approach. The 4th Report is now the definitive confirmation this is a political choice, not a methodological gap.

Netanyahu as Switchboard: The Connector Function

Netanyahu's role extends beyond Pegasus. He personally:

- Brokered the Trump-Orbán relationship from 2016
- Facilitated Likud joining **Patriots for Europe as an observer member** — the only non-EU party with formal affiliation to a European Parliament group
- Appeared on Trump's 'Board of Peace' invite list alongside Orbán[48]
- Presided over Likud-Kahanist mergers from 2019, shifting Israeli politics rightward in coordination with European far-right normalisation

This makes Israel not merely a parallel interference actor alongside Russia and MAGA — it is the **diplomatic switchboard** connecting them at the highest level. Netanyahu sits at the centre of a network bridging Trump ↔ Orbán, Israeli intelligence infrastructure ↔ EU member state governments, and Likud ↔ European Parliament far-right groups.

---

[46] Citizen Lab, *'We Say You Want a Revolution: PRISONBREAK — An AI-Enabled Influence Operation Aimed at Overthrowing the Iranian Regime'*, University of Toronto, October 2025. Published at citizenlab.ca. Attribution assessed at medium confidence to Israeli government or affiliated contractor.

[47] *Ibid.* See also: Schneier on Security, *'AI-Enabled Influence Operation Against Iran'*, 6 October 2025; AI Incident Database, Incident 1221, *'Alleged AI-Enabled PRISONBREAK Influence Operation'*.

[48] CEPS, *'In the Middle East, the EU doesn't need Trump's Board of Peace to be more effective'*, 3 February 2026.

There is 'a documented institutional network connecting Israeli government actors to the principal far-right and anti-EU forces in Europe — and precisely the kind of cross-border influence architecture that a European Intelligence Agency would be mandated to monitor.'[49]

The UK Dimension: Post-Brexit Testing Ground

Post-Brexit UK functions as a laboratory for Israeli influence operations no longer constrained by EU oversight frameworks. **UK Lawyers for Israel (UKLFI)** coordinated directly with the Israeli Ministry of Strategic Affairs to target human rights organisations and Palestinian solidarity groups through legal harassment campaigns.[50] Palantir's deep UK government contracts — NHS, Home Office, Ministry of Defence — represent Israeli-linked tech infrastructure embedded in critical state functions with minimal democratic oversight.

FIMI Assessment: The Pegasus operation against EU officials, documented by the European Parliament's own inquiry, meets all four FIMI criteria. The intelligence loop it creates — harvesting data for subsequent targeting — represents a new category of interference the FIMI framework must address. Its absence from the FIMI database is a choice, not an oversight. *See Technical Annex A, Section 3 for the formal ENISA ETL assessment."*

[49] Howitt, The Reckoning Part 3, op. cit., footnote 21, citing: Foreign Policy, *'Why Israel Courts the Far Right in Europe*', February 2026; Middle East Eye, *'Why Israel Is Joining Hands with Europe's Far Right'*, February 2026. Note also: Hungary announced its withdrawal from the International Criminal Court on the day of Netanyahu's Budapest state visit — a detail not previously footnoted in this report.

[50] *'A New Axis Powers?'*, Compossible Blog, March 2025, UK section.

PART IV: HUNGARY — WHERE ALL VECTORS CONVERGE

Four Weeks to the Election: The Documented Threat

Actor	Operation	Evidence	Source
Russia	**Agency for Social Design (ASP)** — EU-sanctioned firm running Orbán's campaign	Multiple European security sources	Financial Times, March 2026[51]
Russia	**Sergei Kiriyenko** (Putin's First Deputy Chief of Staff) personally overseeing Hungary operation	European national security sources	VSquare, March 2026[52]
Russia	Russian embassy Budapest functioning as **part-time Fidesz campaign HQ**	Intelligence committee sources	Financial Times, March 2026[53]
Russia	Hungarian intelligence agents **spying on EU institutions** in Brussels	Joint investigative reporting	Direkt36/Der Spiegel/De Standaard, October 2025[54]
US/MAGA	CPAC Hungary; Orbán addressed CPAC Dallas 2022; Danube Institute infrastructure	Public record	Multiple sources[55]
Israel	**Pegasus purchased 2017** post-Netanyahu meeting; deployed against opposition, journalists	European Parliament PEGA Report	May 2023[56]
Internal	Orbán **weaponising state intelligence** against opposition candidate Péter Magyar	Hungarian parliamentary documents	March 2026[57]

[51] DW citing Financial Times, *'Russia works to tip scale for Orban in Hungary election'*, 13 March 2026.
[52] VSquare, *'Goulash: Kremlin's Vote-Meddling Team in Budapest'*, 4 March 2026.
[53] Financial Times, op. cit.
[54] DW, *'Hungary found to have sent agents to spy on EU — report'*, 9 October 2025.
[55] Illiberalism.org, *'Rallying the Troops: CPAC and the International Far Right'*, 22 December 2025.
[56] European Parliament PEGA Report, op. cit.
[57] AP News, *'Hungary to declassify a report allegedly showing illegal Ukraine funding of opposition'*, 12 March 2026.

The Agency for Social Design: A Sanctioned Entity Operating Openly

The ASP is under EU, US, and UK sanctions for Russian disinformation operations. It is currently running Orbán's re-election campaign. This is not alleged — it is documented by Financial Times reporting citing multiple European security sources. The firm's previous operations include the 2016 US presidential election and the 2024 Romanian presidential election (Călin Georgescu amplification).[58]

Simultaneously with its Hungary operation, the SDA/ASP ran two documented waves of Doppelgänger activity against the 2025 German federal election: 288 posts in late December 2024 through January using six fake news domains, followed by 573 posts in mid-January using eight fake domains including impersonations of Der Spiegel (spiegel.bz) and Die Welt (welt.pm). A third wave of 637 posts in February reached 414,000 views. The SDA was therefore running active interference operations in Germany and Hungary concurrently — a sanctioned entity operating across two EU member states simultaneously while the Commission's enforcement files remained frozen.[59]

The EU's Response: Complicity by Omission

Euronews reported in January 2026 that the European Commission **actively froze key Hungary files** ahead of the April election, fearing action would give Orbán a 'Brussels interference' narrative.[60] This is the EU choosing non-intervention in a democratic election in which a Kremlin-run, EU-sanctioned disinformation firm is actively operating. The logic is perverse — and historically familiar. As opposition leader Péter Magyar has warned:

> *'Russian intelligence is attempting to swing this election for Orbán.'*[61]

Meanwhile, Orbán is weaponising the state intelligence apparatus to accuse Magyar of illegal Ukrainian funding — using the tools of democratic accountability against democracy itself.[62]

The Commission's inaction is not political caution — it is an act of strategic self-harm, sustaining the captured node that every adversary uses as a veto weapon inside European institutions.[63]

The Political Network for Values: The Transatlantic Connector

The **Political Network for Values (PNfV)** — funded by the Hungarian government — serves as the formal institutional bridge between CPAC American networks, European far-right parties, and Orbán's international

---

[58] FDD Analysis, *'Russia Allegedly Meddles in Hungary's Upcoming Elections'*, 12 March 2026. The Romanian Constitutional Court annulled the first round result on 6 December 2024, establishing a legal precedent for treating Russian hybrid actions and algorithmic manipulation as grounds for cancelling election results — the first such ruling in EU legal history.

[59] FIMI ISAC, Germany FIMI Report, op. cit., pp. 49–51. Fake domains documented include spiegel.bz, welt.pm, grunehummel.net, leparisien.fyi. 637 posts documented reaching 414,000 views on X by 19 February 2025.

[60] Euronews, *'EU freezes Hungarian files ahead of key election in April, fearing Orban campaign backlash'*, 11 January 2026.

[61] AP News, op. cit., 12 March 2026.

[62] *Ibid*.

[63] Howitt, The Reckoning Part 3, op. cit.: '*Hungary and Slovakia currently function as systematic spoilers — capturing EU nodes to block Ukraine aid and veto Russian sanctions on behalf of Moscow and Washington's MAGA faction.*' The Reckoning proposes that if Orbán wins in April, Article 7 proceedings must be concluded within twelve months with suspension of all EU voting rights and transfer payments.

legitimisation infrastructure.[64] It hosts conferences, coordinates messaging, and functions as civil society cover for what is, in operational terms, a state-funded international influence network operating inside the EU.

Orbán declared Hungary's role explicitly:

> '*Hungary is a fortress of conservative and Christian values.*'[65]

The Hungarian election is on 6 April 2026. This report is published 20 days before polling opens. Every day the Commission's files remain frozen is a day the ASP operates uncontested.

[64] *'A New Axis Powers?'*, Compossible Blog, March 2025, Hungary section.
[65] Viktor Orbán, speech, Budapest, May 2022. CGTN, *'Hungary a fortress of conservative and Christian values says Orban'*, 20 May 2022.

PART V: THE EUROPEAN PARLIAMENT AS A BATTLEFIELD

Layer 1: Voice of Europe — Russian Financial Penetration

The Voice of Europe operation — dismantled by Czech intelligence in March 2024 — involved over **€1 million in documented payments** to European politicians to spread Russian propaganda through three coordinated platforms: Voice of Europe, Visegrad Post, and Golos.eu.[66]

Petr Bystron (AfD, Germany): Recorded discussing financial remuneration for MEPs with network organiser Artem Marchevsky, selecting which elected representatives would relay Russian messaging.[67]

Marcel de Graaf (PVV, Netherlands): His parliamentary aide Guillaume Pradoura was arrested by Belgian and French authorities on charges of facilitating Russian interference, passive corruption, and membership of a criminal organisation.[68]

Two German AfD MEPs met Voice of Europe organisers in Moscow **after the network had been EU-sanctioned** — documented by German intelligence services.[69]

Layer 2: MAGA Legislative Capture — The Lobbying-to-FIMI Threshold

The BLOOM investigation documents the precise point at which US lobbying crossed into FIMI. Legitimate lobbying is transparent, disclosed, and presents genuine policy arguments. What BLOOM documents is systematically different:

- **Coordinated:** Multiple AmCham meetings, Heritage Foundation visits, and Danube Institute funding operating simultaneously across multiple MEPs
- **Manipulative:** Manufacturing political pressure through false framing of climate legislation as economic threat — astroturfed rather than genuine public concern
- **Undisclosed:** Operating through think tanks and foundations rather than registered lobbying channels to avoid transparency requirements
- **Contrary to democratic values:** Dismantling legislation that had been democratically agreed through normal EU legislative process

This is not aggressive lobbying. By the FIMI framework's own definition, it is interference.[70]

Layer 3: Patriots for Europe — The Institutional Far-Right

---

[66] Le Monde, *'Russian connections of several far-right MEPs become clearer'*, 6 June 2024.
[67] *Ibid*.
[68] GMF Securing Democracy, *'Voice of Europe 2024: Staffer to Dutch far-right MEP investigated for colluding with Russia'*, 28 May 2024.
[69] EuroMaidan Press, *'Two German MEPs met organisers of EU-sanctioned Russian influence network in Moscow'*, 16 December 2025.
[70] BLOOM Association, op. cit.; EEAS FIMI methodology, 2022.

The **Patriots for Europe** group — 89 MEPs, third largest in Parliament — was under investigation within six months of formation for allegedly diverting **€171,000 in EU funds** through illegal donations.[71] Its voting record is the most systematically pro-Russia in Parliament.

Uniquely, **Likud holds observer member status** — the only non-EU party formally affiliated with a European Parliament group. This is the institutional expression of Netanyahu's switchboard function: Israeli foreign policy interests formally embedded in the EU's largest far-right parliamentary bloc.[72]

The Convergence: Shared Infrastructure

The three layers share infrastructure. The **Danube Institute** appears in the BLOOM investigation as a common funder of both Voice-of-Europe-adjacent networks and EPP politicians being pulled toward MAGA. DW confirmed:

> '*There is a transnational network now moving east to west in Europe...*'[73]

[71] table.media, *'European Parliament: New far-right parliamentary group reportedly diverted EU funds'*, 3 November 2025.
[72] Illiberalism.org, op. cit.
[73] DW, *'Central Europe's right-wing populist networks up their game'*, 5 June 2025.

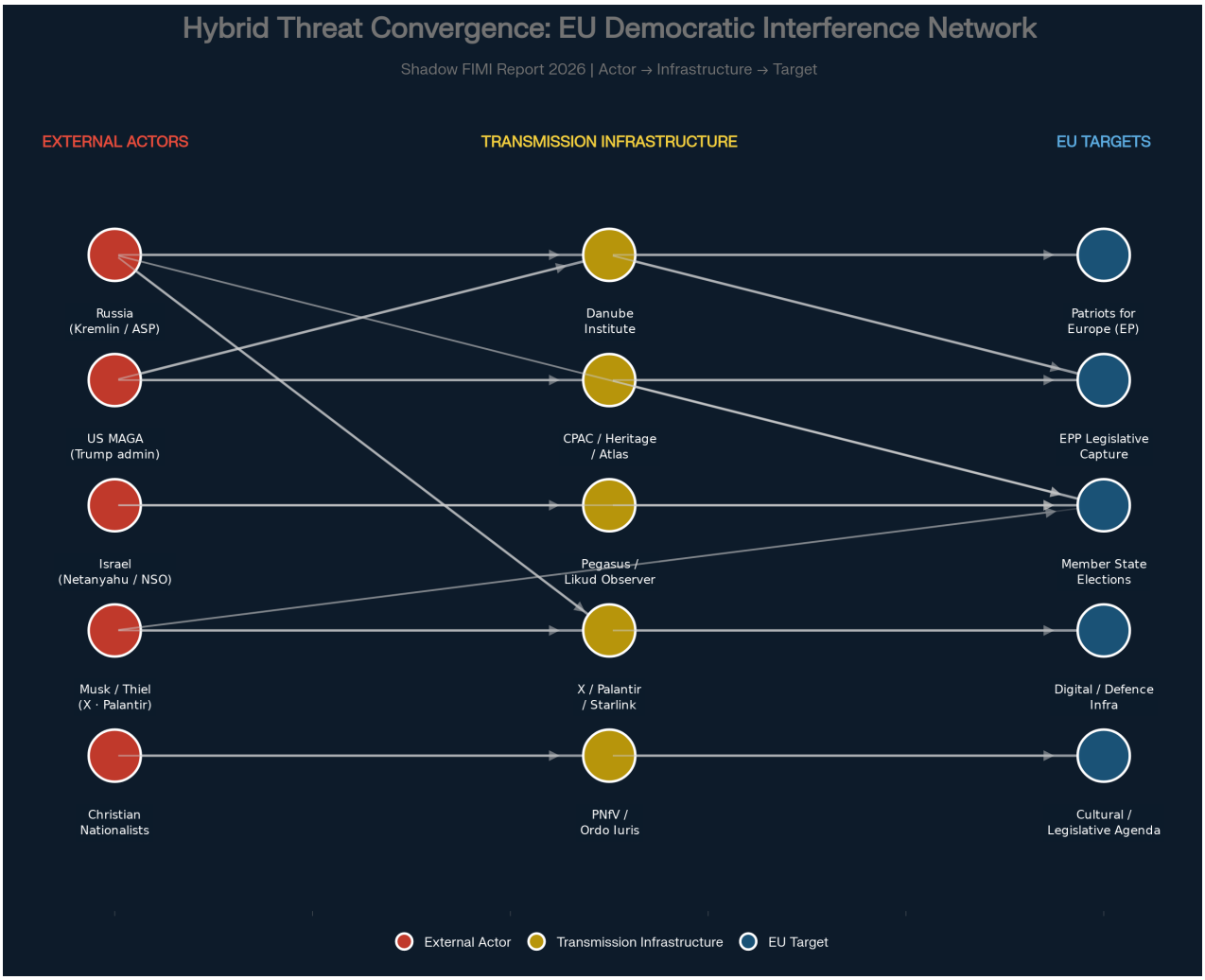


Figure 1: Hybrid Threat Convergence — Actor → Infrastructure → Target mapping. Red nodes: external interference actors. Yellow nodes: transmission infrastructure. Blue nodes: EU democratic targets. Lines show documented operational connections; cross-connections between columns indicate shared infrastructure between interference vectors.

PART VI: THE RELIGIOUS-NATIONALIST BRIDGE

The CPAC-MAGA-far right network does not operate on political self-interest alone. It requires a **moral legitimisation layer** — a framework that justifies dismantling democratic institutions as a civilisational imperative rather than a power grab. That layer is Christian nationalism, and it is the most under-documented dimension of the interference architecture.

The Ideological Framework

Christian nationalism provides the mass mobilisation framework that the Dark Enlightenment cannot. Where neo-reactionary philosophy appeals to technocratic elites, Christian nationalism mobilises popular movements around the defence of 'Christian civilisation' against a secular, globalist 'Cathedral' — a term used identically in both frameworks, creating ideological interoperability between elite and popular far-right networks.[74]

Orbán stated the civilisational claim explicitly:

> '*We must demonstrate that there is an alternative to liberal democracy: it is Christian democracy.*'[75]

Ordo Iuris: US Christian Nationalism Inside EU Policy

Ordo Iuris — a Polish legal institute — has driven the anti-abortion, anti-LGBTQ, and anti-gender legislative agenda that mirrors CPAC priorities exactly. It has:

1. Drafted Poland's near-total abortion ban legislation
2. Provided legal arguments for Poland's 'LGBT-free zones'
3. Lobbied directly in EU institutions against gender equality directives
4. Coordinated with **ADF International** (Alliance Defending Freedom) — the US Christian nationalist legal organisation with direct Heritage Foundation links[76]

ADF International maintains a permanent EU office in Brussels — a continuous US Christian nationalist lobbying presence inside EU institutions operating with minimal transparency. Its parent organisation is classified as a hate group by the Southern Poverty Law Center and has received funding from the same donor networks (Bradley Foundation, Donors Capital Fund) that fund Project 2025.[77]

NatCon: The Parliamentary-Religious Bridge

The **National Conservatism (NatCon)** conference series explicitly bridges parliamentary politics and Christian nationalist ideology. It operates in parallel with CPAC across the same Central European

---

[74] *'Elon Musk — Part 1: The Crusader Behind The Mask'*, Compossible Blog, 2 November 2025; CPAC and NatCon: Uniting a Transnational Radical Right, Canopy Forum, 25 October 2024.
[75] Viktor Orbán, speech at 29th Bálványos Summer University, Băile Tușnad, Romania, July 2018. Widely cited.
[76] OpenDemocracy, *'This ultra-conservative institute has infiltrated the Polish state to ban abortion'*, 29 July 2018; OpenDemocracy, *'In Poland, public funding is given to those threatening liberal democracy'*, 21 July 2021.
[77] *'A New Axis Powers?'*, Compossible Blog, March 2025; Yorkshire Bylines, *'Right-wing push to dismantle the EU: Heritage Foundation's private workshop'*, 25 March 2025.

geography, with significant overlap in speakers, funders, and attendees. NatCon Brussels 2024 was temporarily banned by the local mayor — later overturned — demonstrating both the network's reach and European institutions' uncertainty about how to respond.[78]

The Three-Layer Legitimisation Architecture

Together, these networks create a three-layer ideological architecture that makes the interference project coherent from elite to mass level:

Layer	**Framework**	**Network**	**Function**
Elite	Dark Enlightenment / NRx	Thiel, Musk, Curtis Yarvin	Intellectual justification for dismantling democracy
Institutional	Conservative nationalism	CPAC, Heritage, NatCon	Parliamentary and policy infrastructure
Mass mobilisation	Christian nationalism	Ordo Iuris, ADF, PNfV	Popular movements, moral framing, cultural wedge issues

This architecture is not accidental. It is how movements that cannot win democratic arguments manufacture the appearance of democratic legitimisation for anti-democratic projects.

[78] BBC, *'Europe's US-backed conservatives hope this is their moment to go mainstream'*, 31 May 2025.

PART VII: THE TECH-OLIGARCH LAYER — MUSK, THIEL AND THE DARK ENLIGHTENMENT NETWORK

The Ideological Declaration

Peter Thiel stated his position without ambiguity:

> '*I no longer believe that freedom and democracy are compatible.*'[79]

This is not a political preference. It is a stated objective to destroy the foundational premise of the European Union. Both Thiel and Musk are documented adherents of the **Dark Enlightenment** / neo-reactionary (NRx) movement — an explicitly anti-democratic philosophy describing liberal democracy as a *'Cathedral'* orthodoxy to be dismantled and replaced by corporate techno-authoritarianism.[80]

Musk's Integrated Interference Infrastructure

What makes Musk qualitatively different from any previous interference actor is the **vertical integration** of his interference capability across five sovereign domains simultaneously:

Domain	Asset	European Threat
Information	X, Grok/xAI	Algorithmic FIMI delivery system; documented electoral interventions
Space/communications	SpaceX, Starlink	~67% of active satellites; military dependency; geopolitical veto demonstrated
AI/cognitive	xAI, Grok, Colossus	DOGE uses Grok on US federal data; safety guardrails deliberately weakened
Robotics	Tesla Optimus	800M jobs displacement projected; single proprietorial control
Neural	Neuralink	Brain-computer interface; no EU regulatory framework

[79] Peter Thiel, *'The Education of a Libertarian'*, Cato Unbound, 13 April 2009.
[80] *'Elon Musk — Part 1: The Crusader Behind The Mask'*, Compossible Blog, 2 November 2025; *'Elon Musk — Part 2: The Limits of Free Speech'*, Compossible Blog, 6 November 2025.

Musk has received over **$38 billion in US government contracts, loans, subsidies and tax credits** — making him simultaneously a private actor and an extension of US state power, deployed without the diplomatic or legal constraints governing state actors.[81]

Documented European Electoral Interventions

Germany, February 2025:
Musk posted hundreds of times promoting AfD before the federal election, including: *'Only AfD can save Germany.'* He held a live X Space event with AfD leader Alice Weidel days before the vote — a serving US government official directly intervening in a NATO ally's election.[82]

The Atlantic Council's Digital Forensic Research Lab published a formal report on what it termed the "Musk Effect" — documenting how Musk's platform interventions amplified AfD engagement and legitimised its leader internationally in the weeks before the vote. One post about an anti-protest incident received 50 million total views; 48 million of those views came from Musk's repost alone. The FIMI ISAC report assesses that Musk's involvement '*likely boosted the party's credibility in Germany and internationally*' — while simultaneously noting that he was acting both as a US government representative and as platform owner. This dual role has no precedent in the history of election interference.[83]

United Kingdom, 2024-25:
Musk called for Prime Minister Starmer's imprisonment, described the UK as *'going fascist,'* promoted the extremist Tommy Robinson, and intervened in the grooming gangs debate with demonstrably false statistics — all amplified by a platform whose algorithm his own teams reconfigured to boost his account.[84]

Poland, 2025:
X amplified CPAC Poland and the Nawrocki endorsement. Musk personally boosted content from Polish far-right accounts during the campaign.[85]

A fabricated deepfake video claiming Macron, Merz and Starmer were using cocaine on a train to Kyiv — produced by Russian FIMI infrastructure — was amplified by US conspiracy theorist Alex Jones on X to 30 million views during the Polish election campaign, one week before the second round of voting. This is the operational convergence in a single incident: Russian content, US far-right amplifier, Musk's platform, EU election target.[86]

X as Active FIMI Delivery System

---

[81] *Ibid*.
[82] Der Spiegel, DW, and NPR coverage of German election, January-February 2025.
[83] FIMI ISAC, Germany FIMI Report, op. cit., pp. 13, 26. The Naomi Seibt example (an anti-climate activist crediting Musk for a Hamburg protest post's 50 million views) is documented at p. 26. The DFRLab "Musk Effect" report is cited at p. 13.
[84] *'Elon Musk — Part 1'*, Compossible Blog, op. cit.
[85] Public record, X platform, May 2025.
[86] FIMI ISAC,*Poland FIMI Report*, op. cit., p. 32.

X under Musk is not a neutral platform that happens to carry disinformation. By design and documented modification, it is an active FIMI delivery infrastructure:

- **80% of trust and safety staff removed** post-acquisition
- **Algorithmic reconfiguration:** documented amplification of right-wing content and Musk's own posts
- **Account reinstatements:** holocaust deniers, white supremacists, election deniers all restored
- **Journalist suppression:** accounts suspended, links to critical outlets throttled
- **DSA non-compliance:** European Commission opened formal proceedings[87]

RT DE: Sanctions Circumvention Enabled by X

The operational consequences of X's non-enforcement were documented in real-time during the 2025 German federal election. The FIMI ISAC consortium — comprising ISD, EU DisinfoLab, the German Marshall Fund and Alliance4Europe — reported all identified Storm-1516 Russian interference content to X through the DSA flagging mechanism. X declined every single submission, responding by email that '*the content is not illegal.*' No action was taken on any flagged content. Bluesky, by contrast, acted on consortium reports, causing Doppelgänger to drastically reduce activity on the platform. X's non-enforcement is not a policy failure — it is a policy.[88]

The German federal election provides the most granular documented evidence of RT DE sanctions circumvention available. Despite being formally banned under EU sanctions, 17 of 31 RT DE mirror domains remained accessible through Germany's three largest ISPs. Individual mirror sites attracted up to 213,900 unique monthly visitors; RT DE's podcast ranked in the top 1% on ListenNotes — 90% of mirror site traffic originated from Germany. In January 2025, RT DE created a new X account explicitly mocking EU sanctions — which X removed, then restored, then removed again. The pattern is identical to the Storm-1516 non-enforcement documented by the FIMI ISAC consortium: flagged, briefly acted upon, then effectively reinstated. A platform that cannot consistently enforce its own removals of a formally sanctioned state broadcaster is not a passive carrier of disinformation. It is its infrastructure.[89]

The same pattern of X non-enforcement was independently documented in the 2025 Polish presidential election. The FIMI ISAC consortium flagged 279 accounts to X in April 2025; X took partial action, then the same operation published 321 further posts in April and May, entirely unimpaired. The consortium also documented that new X accounts can be created and operational in approximately 90 seconds using a temporary email address, with no automated challenge — a technical vulnerability they confirmed by testing

[87] European Commission DSA proceedings against X; *'Elon Musk — Part 3'*, Compossible Blog, op. cit.
[88] FIMI ISAC Consortium (ISD, Alliance4Europe, EU DisinfoLab, GMF/Alliance for Securing Democracy, DEN Institute), *Country Report: Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election*, 2025, p. 59: '*X declined all submitted reports of Storm-1516 activity, claiming in an email that the content is not illegal. We did not see any actions taken in any of the instances where we flagged content to X. By contrast, Bluesky implemented mitigation measures informed by our reporting*.'
[89] FIMI German Country Report, pp. 31–33, 48–49. RT DE created a new X account in January 2025 '*to promote its circumvention sites and mock the EU's sanctions on Russia*' (p. 49). 17 of 31 mirror domains accessible via Germany's largest ISPs; the fourth-largest ISP failed to block any. Up to 213,900 unique monthly visitors on individual mirror sites. Podcast top 1% ranking on ListenNotes.

it themselves. The platform's failure to address this basic infrastructure issue is not negligence. It is a decision.[90]

The Coercive Leverage Dimension

Musk responded to EU DSA enforcement by **threatening to withdraw Starlink from Europe as retaliation.** This is the critical escalation: a private actor using strategic military dependencies as leverage against democratic oversight — coercive interference at state scale with no precedent in any previous FIMI case.[91] The 4th EEAS Report, published today, confirms X accounts for 88% of all detected FIMI activity. It does not address X's systematic non-enforcement of its own DSA obligations, or the Starlink coercion threat. Both facts are in the public domain. Their absence is now confirmed across all four annual FIMI reports.

The Starlink Veto: A Documented Precedent

Musk unilaterally **disabled Starlink coverage in a geofenced area over Crimea** to prevent a Ukrainian military operation — a battlefield decision made without democratic accountability, transparent legal basis, or NATO consultation.[92]

Europe currently depends on SpaceX launches and Starlink for significant military communications. The EU's IRIS² constellation is years from operational deployment. The man who has demonstrated willingness to use this infrastructure as a geopolitical veto controls a dependency Europe cannot quickly replace.

Peter Thiel: The Shadow Architect

Thiel's companies are privatised intelligence infrastructure:

Palantir: Seed-funded by CIA through In-Q-Tel.[93] Holds contracts with UK NHS, European defence ministries, Frontex, and is bidding for EU defence data contracts as European rearmament accelerates. A company founded by a man who explicitly rejects democratic governance is positioning itself as the data infrastructure layer of European military sovereignty.

Anduril: Autonomous weapons systems supplier expanding into European defence markets at precisely the moment Europe is most desperate to rearm quickly — without the procurement timelines that would normally enable proper scrutiny.

The strategic logic: As Europe panics about defence and rushes to spend, Thiel's companies capture the infrastructure layer of European military sovereignty. This is not commercial opportunism. It is the Dark Enlightenment project executed through defence procurement.

The DOGE-Russia Alignment

---

[90] *FIMI ISAC Consortium (Alliance4Europe, Debunk.org, GLOBSEC, EU DisinfoLab, DFRLab, ISD),'Assessment of FIMI in the 2025 Polish Presidential Election', 2025, pp. 76–77.*
[91] *FIMI Poland Country Report*
[92] *'Elon Musk — Part 3'*, Compossible Blog, op. cit.
[93] *'Elon Musk — Part 3'*, Compossible Blog, op. cit.

Documented links between DOGE and pro-Russian networks represent the most alarming convergence in the entire interference architecture. DOGE's stated objectives — dismantling regulatory oversight, defunding international institutions, ending multilateral commitments — are structurally identical to Russian foreign policy objectives for the West. Whether this represents formal coordination or aligned interests producing operational convergence, the outcome is the same: a serving US government operation advancing Kremlin strategic goals.[94]

Musk has had direct documented communications with Putin. Russian state media consistently amplifies Musk's political messaging. The FIMI framework has no category for this — allied state actors whose domestic government operations produce outcomes indistinguishable from hostile interference.

[94] *'A New Axis Powers?'*, Compossible Blog, March 2025, America's influence section.

PART VIII: GENERATIVE FIMI — THE 2026 REALITY

The FIMI framework was designed to detect and attribute information manipulation operations conducted primarily through human actors using digital platforms. In 2026, that model is already obsolete. **Generative FIMI** — interference operations powered by large language models, AI-generated personas, deepfakes, and autonomous content networks — represents a qualitative escalation that the current framework has no methodology to address.

The 4th EEAS Report confirms that AI-related TTPs increased 259% in a single year and that LLM grooming — flooding the internet to contaminate AI training data — is now documented as an active Russian technique. The CopyCop operation documented in Part VIII constitutes precisely this technique. The 4th Report confirms the phenomenon while failing to name the specific infrastructure this report documents.

The Prawilne Polki Case: Generative FIMI Documented

The **'Prawilne Polki'** (Righteous Polish Women) operation — flagged by Poland to the European Commission in December 2025, triggering a formal Brussels TikTok probe — is the first fully documented case of Generative FIMI targeting an EU member state election.[95]

The operation used:

- **AI-generated personas:** Fake young Polish women in national dress, created using generative AI image and video tools
- **LLM-produced content:** Pro-Polexit, anti-EU content in fluent, culturally authentic Polish
- **Algorithmic optimisation:** Content engineered to evade TikTok's moderation systems
- **Dormant account activation:** Accounts dormant since 2023 suddenly activated and algorithmically amplified

This is not a Russian disinformation operation using human actors. It is an autonomous AI content network — what researchers now term an **LLM botnet** — capable of maintaining consistent persona-driven interference across multiple EU languages simultaneously with minimal human oversight.[96]

The Romanian Precedent: Algorithmic Amplification at Scale

The annulment of Romania's 2024 presidential election — the first in EU history on grounds of digital interference — established the legal and political precedent that Generative FIMI can constitute grounds for democratic remedy.[97] The Constitutional Court found that TikTok's algorithm had systematically amplified pro-Russian candidate Călin Georgescu through mechanisms that could not be explained by organic engagement alone.

---

[95] EU Perspectives, *'As AI-generated 'Polexit' campaign emerges on TikTok, Poland seeks EU help'*, 1 January 2026; United24 Media, *'Brussels Probes TikTok After Poland Flags AI-Generated Videos Calling to Leave the EU'*, January 2026.
[96] Insight News, *'Polexit and Russian Disinformation: Why Facts Are Poland's Best Defence'*, 25 February 2026.
[97] European Parliament Special Committee on Foreign Interference, debates December 2024-February 2025.

The European Parliament has since debated mandatory disclosure requirements for AI-generated political content and algorithmic transparency obligations — but no binding framework yet exists.[98]

Grok and X: AI-Native FIMI Infrastructure

Musk's Grok AI, integrated into X, represents a qualitatively different threat: **AI-native FIMI infrastructure** where the generation, amplification, and targeting of disinformation content occur within a single proprietorially controlled system:

- Grok is trained on X's entire data corpus — including years of political disinformation
- Safety guardrails have been documented as deliberately weakened relative to comparable systems
- Grok has generated antisemitic content, praised historical authoritarian figures, and produced demonstrably false political claims
- The same system is used by DOGE to process US federal government data[99]

This creates a closed loop: a single actor controls the AI that generates content, the platform that distributes it, the algorithm that amplifies it, and the government department that processes the data it learns from.

CopyCop: The Documented LLM Influence Operation

The most forensically complete case of LLM-powered generative FIMI at scale is CopyCop — a Russian influence network documented in the 3rd EEAS FIMI Report and independently investigated by Recorded Future's Insikt Group. CopyCop has created more than 300 fake media websites spanning North America, Europe, and beyond, using self-hosted large language models to mass-produce fabricated news stories at industrial scale.[100]

What makes CopyCop analytically decisive for this report is its operational methodology:

- **Self-hosted uncensored LLMs** generate and rewrite thousands of fake news stories daily, blending factual fragments with deliberate falsehoods to create the illusion of credible journalism.[101]
- **Deepfakes of politicians** — including fabricated recordings of German Foreign Minister Baerbock — are generated and distributed through the same network.[102]
- **Fake fact-checking sites** are created to 'debunk' genuine reporting, adding a second-order layer of epistemic manipulation.
- **Data poisoning strategy:** by flooding the internet with synthetic 'news,' CopyCop contaminates the data sources that LLMs, search engines, and AI assistants use to generate answers — ensuring false narratives

---

[98] European Parliament debate on AI deepfakes and social media rules, January 2026. YouTube: *'EU Parliament Debate on AI Deepfakes & Social Media Rules'*, 19 January 2026.
[99] *'Elon Musk — Part 3: The Death Star'*, Compossible Blog, November 2025, op. cit.
[100] Recorded Future / Insikt Group, '*Inside the CopyCop Playbook: How to Fight Back in the Age of Synthetic Media*,' 1 December 2025; 3rd EEAS FIMI Report, March 2025.
[101] Recorded Future: '*The network relies on self-hosted LLMs, specifically uncensored versions of a popular open-source model, to generate and rewrite content at scale.*'
[102] Krajewski, K., '*Russian Influence Operations*,' Defence Science Review, 2025, p.87: '*CopyCop employed advanced disinformation techniques, including generating fake articles using AI, creating deepfakes (e.g., crafted recordings of politicians such as Baerbock).*'

are not merely consumed by people but ingested by algorithms, corrupting the global information supply chain.[103]

On 7 January 2025, the network published 443 posts across 74 pages within a single short period, with technical analysis confirming LLM authorship through repeated structural errors, plagiarism patterns, and stylistic inconsistencies typical of generative AI output.[104]

The X-CopyCop Nexus

CopyCop content is systematically amplified through X. The 3rd EEAS FIMI Report confirmed that **X alone accounted for 88% of all detected FIMI activity in the reporting period.**[105] The operational logic is clear: CopyCop generates at LLM scale; X's algorithm — reconfigured under Musk to amplify far-right content — delivers it at platform scale. The two systems are functionally integrated as a generative-FIMI pipeline, even absent formal coordination between their operators.

This is the 2026 reality the FIMI framework must confront: generation and amplification of disinformation content are now industrialised, cross-platform, and partially autonomous. **The human bottleneck in content generation and distribution has been substantially reduced.** The FIMI database, designed to identify coordinated human actor behaviour, has no current comprehensive methodology to attribute or respond to this at scale.

The Framework Gap: What FIMI Cannot Currently Detect

The current FIMI Exposure Matrix was designed to identify coordinated inauthentic behaviour by human actors. Generative FIMI breaks its core assumptions:

FIMI Assumption	**Generative FIMI Reality**
Human actors operate accounts	AI personas are indistinguishable from humans at scale
Coordination requires organisational infrastructure	LLM botnets self-coordinate through shared training
Content reflects strategic intent	AI content generation is probabilistic, not planned
Attribution requires identifying actors	Attribution of LLM output to specific state actors is technically complex

[103] Recorded Future, op. cit.: '*This deliberate poisoning strategy ensures that false narratives are not only consumed by people, but also ingested by algorithms... threatening the integrity of the global information supply chain.*'
[104] Krajewski, K., op. cit., p.87.
[105] Istituto Germani / EEAS 3rd FIMI Report summary, August 2025: '*X alone accounting for 88% of the detected [FIMI] activity.*'

The FIMI framework urgently requires:

- **Generative content detection standards** — mandatory AI labelling of political content under DSA enforcement
- **LLM botnet attribution methodology** — technical standards for identifying AI-generated coordinated inauthentic behaviour
- **Platform algorithmic transparency** — mandatory disclosure of amplification decisions for political content
- **Cross-platform coordination detection** — monitoring for narrative synchronisation across X, TikTok, and Telegram simultaneously[106]

[106] Liberal Forum, *'From Algorithms to Ballots'*, December 2025.

PART IX: THE STRUCTURAL GAPS THIS REPORT EXPOSES

Russian TTP	EU Response	Parallel US/Israeli/Oligarch TTP	EU Response
Doppelgänger: fake Der Spiegel (spiegel.bz)	FIMI Explorer entry; sanctions against SDA	Nawrocki deploys AI-fabricated expert persona 'Batyr' on state TV	No FIMI attribution
ASP runs electoral disinformation operations	Sanctioned; named in Deterrence Playbook	CPAC Poland: Noem conditions security on electoral outcome	Not in FIMI Explorer
CopyCop LLMs mass-produce fabricated news	Documented; DISARM-mapped in 4th Report	Prawilne Polki: LLM-generated personas amplify Polexit	Not in FIMI Explorer
Voice of Europe pays MEPs; T0104 Corrupt Legislature	Czech intelligence dismantles; EU sanctions	BLOOM: Heritage/AmCham coordination dismantles CSDDD via IDU	Not in FIMI Explorer
Pegasus-equivalent surveillance (Russia/Belarus context)	Noted in cyber-FIMI convergence	Pegasus: EU officials, opposition politicians hacked via Israeli NSO	No FIMI attribution
RT DE amplifies AfD on X	RT DE banned under DSA	Musk's X algorithmically amplifies AfD; Musk directly endorses	No DSA enforcement; no FIMI attribution
Kiriyenko coordinates Hungary operation via embassy	European security sources; named	DOGE data access creates intelligence loop aligned with Russian objectives	No assessment

The FIMI Database: What Is Missing

Despite claiming actor-agnosticism, the following forensically documented operations are absent from the FIMI Exposure Matrix:

Operation	Actor	Documentation	FIMI Status
CPAC Poland electoral intervention	US Trump administration	NPR, Bloomberg, Notes from Poland	**Absent**
Nawrocki White House visit during campaign	US (Trump)	Reuters, NYT	**Absent**

Noem CPAC voter coercion speech	US (DHS Secretary)	Video record, NPR verbatim	**Absent**
Pegasus deployment against EU officials	Israel (NSO Group)	EP PEGA Report, Euronews	**Absent**
Agency for Social Design	Russia (sanctioned entity)	Financial Times, VSquare	***Partially present (Romania only) / Hungary operation absent***[107]
Voice of Europe MEP payments	Russia	Czech intelligence, arrests	**Present**
Musk electoral interventions Germany/UK/Poland	US (Musk/X)	Documented posts, DSA proceedings	**Absent**
BLOOM investigation (CSDDD destruction)	US fossil fuel lobbies	BLOOM/Der Spiegel/Aftonbladet	**Absent**
Prawilne Polki AI campaign	Russia (attributed)	Polish government complaint, EU TikTok probe	**Absent**

The pattern is unambiguous. The asymmetry is not analytical — it is political.

The 4th EEAS Report introduces a FIMI Deterrence Playbook designed to dismantle interference operations by targeting their financial, technical and organisational enablers. Applied consistently, this Playbook would reach every operation documented in this report including those operated by public-private state actors.

AI As Emerging FIMI Vector

The 2025 German election marks the first German federal election cycle in which AI tools were systematically documented as FIMI weapons. Across 100 analysed reports, AI was mentioned 88 times — compared to zero in 2017 and 2021 reports. Storm-1516 operated more than 100 AI-generated websites in the three months before the election; Operation Overload used AI to manipulate real video footage of academics, law enforcement and celebrities, with 40 percent of 118 deployed videos assessed as AI-

[107] The 4th FIMI Report references ASP in the Deterrence Playbook as a sanctions example. The Hungary 2026 operation — documented by the Financial Times and VSquare — does not appear in the FIMI Explorer database.

manipulated. Deepfake content fabricating sexual abuse allegations against Green Party candidates reached 25 million views across X and TikTok. The AI regulation frameworks currently under discussion in the EU address generation tools; none yet address their systematic weaponisation as election interference infrastructure.[108]

Storm-1516 narratives were amplified by AfD Members of Parliament; 97 percent of 938 undeclared TikTok accounts identified in the pre-election period promoted AfD content; and the AfD's own AI-generated campaign content used narratives '*consistent with those typically seen by FIMI actors*.' The FIMI ISAC consortium assesses that Russia's strategic objective in Germany was to create "a pro-Russian German government with which it can resume more normal relations, including the sale of gas." The AfD is not merely a beneficiary of Russian FIMI — it is the delivery mechanism for its strategic objective**.**[109]

The Co-Design Problem

The FIMI framework was first coined in a US-EU joint summit statement in June 2021.[110] It was built as a transatlantic tool, designed with Washington to counter Russian and Chinese operations. It was never designed to be turned on its co-author. That is not a legal constraint. It is a political one — and political constraints can be changed by political will.

The Three New Structural Proposals

The existing Call to Action across multiple EU reports is primarily moral — naming the problem and demanding action. This report adds three **structural proposals** that would make symmetric application of FIMI enforceable rather than merely aspirational:

Structural Proposal 1: An Independent FIMI Ombudsman

Problem: The EEAS answers to the Foreign Affairs Council, which operates by unanimity. Hungary and Slovakia can veto Council endorsement of any report naming allied actors. Political fear suppresses findings even when evidence is overwhelming.

Solution: Establish an **Independent FIMI Ombudsman** — an oversight body outside the EEAS diplomatic chain, modelled on the existing EU Ombudsman and European Court of Auditors. The Ombudsman would:

- Receive formal complaints from member states, civil society, and MEPs
- Conduct independent FIMI assessments using the existing methodology
- Publish findings without requiring Council endorsement

[108] FIMI ISAC, Germany FIMI Report, op. cit., pp. 35–36, 58. AI tool mentions: ChatGPT 45 occurrences, Perplexity 24, Grok 4, Gemini 3 across the 100 reports analysed. Storm-1516 website count and AI video manipulation percentages at pp. 46–47. 25 million view figure at p. 47.
[109] FIMI ISAC, Germany FIMI Report, op. cit., pp. 24, 52–56. AfD MP amplification of Storm-1516: Stephan Protschka, documented at p. 55. TikTok undeclared account statistics: Democracy Reporting International data cited at p. 52. Russian strategic objective quotation at p. 24.
[110] Proto, A. et al., op. cit., Media & Communication, 2025.

- Report directly to the European Parliament, not the Foreign Affairs Council

Legislative vehicle: Secondary legislation under Article 352 TFEU (flexibility clause) or an interinstitutional agreement between Commission, Parliament and Council. Does not require treaty change.

Strategic value: Permanently removes political fear as a suppression mechanism. Any actor — including allied states — who conducts documented interference operations in the EU would face independent attribution regardless of diplomatic sensitivity.

The Ombudsman's technical mandate must include published standards for identifying AI-generated coordinated inauthentic behaviour — updated annually to keep pace with generative FIMI capability development.

Structural Proposal 2: Digital Sovereignty Stress Tests

Problem: Europe's critical infrastructure dependencies on Musk (Starlink, SpaceX), Thiel (Palantir), and other politically-aligned tech oligarchs represent existential sovereignty vulnerabilities. The FIMI Deterrence Playbook addresses infrastructure supply chains in principle. It does not apply this framework to Starlink, Palantir, or equivalent politically-exposed vendors — despite the documented Starlink coercion precedent. The Starlink Crimea veto and DSA/Starlink coercion threat have demonstrated these dependencies can be weaponised.

Solution: Mandate **Digital Sovereignty Stress Tests** — annual independent audits of critical EU infrastructure dependencies, assessing:

- **Single-vendor concentration risk** in satellite communications, AI systems, and defence data processing
- **Political exposure assessment** — whether vendors have documented histories of using infrastructure as political leverage
- **Contingency planning** — mandatory identification of alternative providers or European alternatives with funded transition timelines
- **Contract conditionality** — EU and member state contracts with politically-exposed vendors to include non-interference clauses with termination triggers

Legislative vehicle: Extension of the EU Critical Entities Resilience Directive (CER Directive) to include politically-exposed vendor risk. Can be achieved through delegated acts without new primary legislation.

Strategic value: Treats tech-oligarch influence as a systemic risk requiring regulatory management rather than a reputational concern requiring public relations. Accelerates IRIS² and European alternatives. Creates legal basis for contract termination if Starlink/Palantir are used as coercive leverage.

The Legislative Vehicle: The European Democracy Shield

The European Democracy Shield — published as a formal joint Communication of the European Commission and High Representative on 12 November 2025 — provides the precise legislative vehicle for these

proposals.[111] The EDS explicitly covers FIMI, hybrid threats targeting elections, covert foreign financing, and creates a new **European Centre for Democratic Resilience** to coordinate cross-institutional response.[112]

The EDS's own mandate includes strengthening the **European Cooperation Network on Elections** specifically to address attacks combining FIMI with cyber operations and covert campaign financing — exactly the convergence documented in this report's Pegasus and PRISONBREAK assessments.[113] The Digital Sovereignty Stress Tests proposed here should be enacted as a formal implementing measure under the EDS framework, with the European Centre for Democratic Resilience designated as the responsible body. The legislative architecture exists. What is currently missing is the political will to apply it to the actors this report names.

The **non-interference clause** for politically-exposed vendors should be incorporated into EDS implementing legislation as a standard contract condition for all critical infrastructure procurement — with automatic termination triggers if infrastructure is deployed as coercive leverage. The Starlink Crimea veto and the DSA retaliation threat establish the precedent. The EDS provides the legal basis. The clause writes itself.

The case for a European Intelligence Agency extends beyond FIMI attribution. The current intelligence architecture — bilateral arrangements, NATO relay dependencies, and national silos — is structurally incapable of identifying cross-border interference networks that involve allied state actors, because the dependency relationships themselves create institutional disincentives for attribution. The EU excels at diagnosis; it has consistently failed to translate that diagnosis into institutional action with the speed the threat requires.[114]

Structural Proposal 3: Financial Transparency for Foreign-Funded Think Tanks and Political Infrastructure

Problem: The Danube Institute, Political Network for Values, Ordo Iuris, ADF International, and equivalent organisations operate as foreign-funded political infrastructure inside the EU with minimal disclosure requirements. They function as money laundering vehicles for foreign political influence — providing ideological and organisational infrastructure for interference operations while hiding their funding origins behind charitable or academic status.

Solution: Mandatory **full financial disclosure** for any think tank, foundation, conference organisation, or civil society body that:

1. Receives funding from outside the EU or from EU member state governments for activities in other member states

[111] European Commission / High Representative, *European Democracy Shield*, Joint Communication, 12 November 2025. Published at ec.europa.eu/enlargement/news.
[112] EP Think Tank, *'The European Democracy Shield: An Overview'*, 15 January 2026: *"The EDS... creates a new European Centre for Democratic Resilience."*
[113] Freshfields Technology Quotient, *'The European Democracy Shield: Commission publishes plan to empower democracy'*, 10 December 2025.
[114] Howitt, The Reckoning Part 3, op. cit. The QMV reform stall and intelligence coordination failure are identified as structurally linked: '*Every EU member state faces a version of the Prisoner's Dilemma when it comes to European strategic autonomy... A binding architecture is the answer to the defection incentive. You do not ask states to trust each other's commitments, you just need to make defection structurally more expensive than solidarity.*'

2. Engages in political lobbying of EU institutions or member state governments
3. Organises conferences or events featuring elected officials or candidates

Legislative vehicle: Amendment to the EU Lobbying Transparency Register regulation, combined with extension of the Foreign Subsidies Regulation (FSR) to cover political and civil society organisations. The FSR already applies to commercial entities — extension to political infrastructure requires secondary legislation only.

Strategic value: Cuts the dark money pipeline connecting foreign interests (Kremlin, MAGA donors, Israeli government) to EU policy processes. Makes the Danube Institute, PNfV, and CPAC Europe's funding fully visible. Provides legal basis for deregistration of organisations found to be operating as undisclosed foreign political agents.

CONCLUSION: THE BREXIT WARNING

The UK's Intelligence and Security Committee possessed evidence of foreign interference before the Brexit referendum. It was not published until November 2019. The Committee concluded that the government had *'actively avoided'* investigating Russian interference, giving the issue 'far less priority than it deserved.'[115]

Twelve months after *'A New Axis Powers?'* identified the structural threat to the EU, the evidence base has been forensically confirmed across every dimension:

1. The CPAC-MAGA electoral interference network has run a presidential election inside an EU member state (Hungary) — openly, with cabinet-level participation
2. A Kremlin-run, EU-sanctioned firm is running an EU member state's election (Hungary) campaign today
3. Pegasus has hacked EU officials and the European Parliament documented it — then did nothing
4. Musk has intervened in three EU member state elections. The 4th EEAS Report, covering all documented Musk interventions in 2025 — Germany, UK, Poland — contains no FIMI attribution.
5. The European Parliament has been financially penetrated by Russian networks and legislatively captured by US lobbying
6. Christian nationalist networks funded by US donors are embedded in EU legislative processes through permanently registered Brussels offices
7. Generative FIMI has triggered a TikTok probe and caused the first EU election annulment in democratic history

The 4th FIMI Report launches today. Kallas said it herself:

> '*We cannot afford to lose the information battle. Winning a fight requires a shield and a sword. We are already building the democracy shield. Now we must also sharpen our proverbial sword.*'[116]

The sword exists. The evidence exists. The methodology exists. The framework claims to be actor-agnostic. Today's FIMI Explorer database has launched. Every operation documented in this report should appear in it.

Its absence is not a gap. It is a decision. And decisions can be changed.

The lesson of Brexit is not that interference is unstoppable. It is that **silence is a political choice** — and its consequences are irreversible. The UK stayed silent and lost a member state. If the EU stays silent now, it will lose more than Hungary. It will lose the principle that European democracy is defensible against any actor — allied or adversary — who seeks to dismantle it.

Tusk already knows what is at stake:

> '*Russia, American MAGA, and the European right with Orbán at the head, want to destroy the EU.*'[117]

---

[115] Intelligence and Security Committee of Parliament, *Russia Report*, HC 632, 21 July 2020, p.3 and Executive Summary, paragraph 9.
[116] Kaja Kallas, FIMI Conference statement, Brussels, 23 February 2026.
[117] Donald Tusk, X post 15 March 2026 (RBC-Ukraine, 14 March 2026).

The FIMI threat documented in this report cannot be addressed without resolving the deeper strategic question: whether Europe will continue to treat its alliance relationships as constraints on democratic self-defence. I have previously framed Europe's strategic objective as occupying the Lagrange Point between the superpowers[118] — the position of stable leverage from which neither Washington nor Beijing can dictate terms. Achieving that position requires, as a precondition, ending the political inhibition on naming allied interference actors that this report documents.

Fear = failure.

It was true in March 2025. It is more true today. It will be irreversibly true after the Hungarian election if the EU does not act.

[118] Peter Howitt, *'The Reckoning: A European Strategy for an Unstable World, Part 3 — Engineering Escape Velocity*', Compossible, 15 March 2026. The series identifies the "Atlanticist Veto" — states prioritising bilateral US relationships over European strategic autonomy — as the primary internal obstacle to European grand strategy, and the documented network connecting Netanyahu's Likud to Orbán's Fidesz to Patriots for Europe as '*precisely the kind of cross-border influence architecture that European intelligence has been structurally blind to, partly because our intelligence dependencies discourage naming allies as major threat actors.*'

CALL TO ACTION

This report identifies not only a failure of political will but a set of **specific, achievable actions** that require no treaty change, no new institutions, and no unprecedented legal steps. They require only the courage to use tools that already exist.

Immediate Actions

European Parliament Advisory Committee on Conduct of Members:

BLOOM's formal complaint is out. Act on it. Specifically:

- **Order full disclosure** of the funding sources for SME Europe and SME Global — the dual organisations used by MEP Warborn as transmission vehicles for US corporate legislative influence.
- **Investigate the IDU network meetings** between named US Republican politicians (McCormick, Fitzpatrick, Bacon, O'Brien) and EPP MEPs for undisclosed coordination contrary to Parliament's conduct rules.
- **Establish whether** the Heritage Foundation, AmCham, and IDU coordination constitutes a foreign-funded political operation requiring registration under the Foreign Subsidies Regulation.

European Parliament — Independent Integrity Enforcement Body:

Establish a single independent European body responsible for enforcing all integrity rules for public officials — with the power to launch investigations and impose sanctions without referral to the committee of the official's own political group. The current system, in which MEP conduct complaints are reviewed by committees dominated by the MEP's own group, is structurally incapable of addressing cross-party foreign influence operations. The BLOOM case has proved this beyond reasonable doubt. The body should have jurisdiction over MEPs, Commissioners, and Council officials simultaneously, with published findings and binding sanction authority.

High Representative Kaja Kallas:
Authorise the EEAS to formally attribute the following operations using the existing FIMI methodology:

- CPAC Poland electoral intervention (Noem speech, Trump White House visit during campaign)
- Musk's documented electoral interventions in Germany, UK, and Poland
- Agency for Social Design operations in Hungary under Kiriyenko's oversight

You have stated that *'today's wars are fought with lies and algorithms.'* Apply that statement symmetrically. The FIMI Explorer launched today. These operations should be in it. If they are not, publish a public explanation of why the actor-agnostic framework does not apply to these documented cases.

Polish Foreign Minister Radosław Sikorski:
You stated at Munich that Trump hosting Nawrocki during the campaign broke *'the unspoken agreement not to interfere in allied countries' party political rivalries'* and was *'completely outrageous'*[119] Convert

[119] Radosław Sikorski, Munich Security Conference, February 2026. Reported in Notes from Poland, 'Polish FM Sikorski says Trump's hosting of Nawrocki was '*completely outrageous*'", February 2026

that speech into a **formal member state FIMI complaint** to the EEAS. You have the evidence. You have the legal standing. Nawrocki cannot block a ministerial submission. Force the EEAS to respond institutionally or be seen to suppress a documented member state complaint.

EU DisinfoLab, Direkt36, BLOOM, Liberties.eu:
Publish a joint forensic report on the Hungarian election using FIMI methodology **before the April vote.** The civil society record must be established before the election, not after. The window is four weeks. Use it.

Short-Term Actions (Before Hungarian Election)

The European Commission:
Immediately unfreeze the Hungary spying scandal probe. The rationale for freezing it — avoiding an Orbán 'Brussels interference' narrative — is strategically illiterate when a Kremlin-run, EU-sanctioned firm is operating his campaign. The interference is happening. Your silence does not prevent it. It enables it.

The European Parliament:
Establish a **Special Committee on Foreign Electoral Interference** with an explicit mandate covering all external actors regardless of alliance status. Use BLOOM's formal complaint as the legislative hook. Schedule public hearings on:

- Musk's documented interventions in EU elections
- CPAC Poland and the Nawrocki endorsement
- Pegasus operations against EU officials
- The Agency for Social Design's Hungary operation

Force the far-right ECR and ID groups to vote against such a committee publicly. Make them explain on the record why they oppose investigating documented interference in EU elections.

Member State Governments (France, Germany, Nordic-Baltic coalition):
Co-sponsor a formal EEAS request for a FIMI assessment of the Polish presidential election and the Hungarian election campaign. A multi-state request is substantially harder to suppress than a bilateral submission. The political cost of burying a request from six member states is prohibitive even for a diplomatically cautious EEAS.

Structural Actions (Legislative Agenda)

- **Proposal 1 — Independent FIMI Ombudsman:**
  Introduce secondary legislation under Article 352 TFEU establishing an independent oversight body outside the EEAS diplomatic chain, empowered to receive FIMI complaints from member states, civil society, and MEPs, and to publish findings without requiring Foreign Affairs Council endorsement. This permanently removes political fear as a suppression mechanism and applies symmetric accountability to all actors including allied states.

- **Proposal 2 — Digital Sovereignty Stress Tests:**
  Extend the EU Critical Entities Resilience Directive through delegated acts to mandate annual independent audits of critical infrastructure dependencies on politically-exposed vendors. Assess single-vendor concentration risk (Starlink, Palantir), political exposure history, and contingency planning. Include non-interference contract conditionality with termination triggers. Accelerate funding for IRIS² and European alternatives with binding timelines.
- **Proposal 3 — Foreign-Funded Political Infrastructure Transparency:**
  Amend the EU Lobbying Transparency Register and extend the Foreign Subsidies Regulation to cover think tanks, foundations, conference organisations, and civil society bodies that receive foreign funding and engage in EU political activities. Mandate full financial disclosure for organisations including the Danube Institute, Political Network for Values, ADF International's Brussels office, and CPAC Europe's permanent infrastructure. Provide legal basis for deregistration of undisclosed foreign political agents.

To the European Public

Demand one question be answered publicly, by name, by institution:

Why do these documented operations not appear in today's FIMI Explorer database?

Not a general complaint about interference. A specific, forensic question about specific, named operations. Demand it of your MEPs. Demand it of your national foreign ministers. Demand it of the EEAS press office. Force a public answer.

Civil society — journalists, researchers, NGOs — is doing the work that EU institutions will not. Support it. Share it. Fund it. The organisations documenting this interference — BLOOM, EU DisinfoLab, Direkt36, Liberties.eu, VSquare — are the democratic immune system that institutional timidity has failed to provide.

The methodology exists. The evidence exists. The only thing missing is courage.

TECHNICAL ANNEX A: SHARED INFRASTRUCTURE AND DATA INTEROPERABILITY

This annex provides a deeper technical mapping of the transnational convergence — the specific pathways through which Russian state strategy, US MAGA tech-oligarchy, and Israeli spyware infrastructure utilise shared institutional and digital frameworks to influence European policy.

1. The Distribution Layer: Algorithmic Delivery via X

The X platform functions as the primary delivery mechanism for coordinated narratives across all three interference vectors simultaneously:

Selective Amplification: Musk, in his dual capacity as X owner and US government official (DOGE), has used the platform's algorithm to prioritise content from far-right accounts during critical EU electoral cycles — documented in Germany, UK, and Poland. Independent algorithmic audits have confirmed systematic amplification of right-wing political content relative to centrist and left-wing equivalents.

Narrative Laundering: Infrastructure originally developed for US domestic politics (CPAC, Heritage Foundation messaging) is amplified through X to provide apparent democratic legitimacy to candidate endorsements that simultaneously align with Kremlin objectives — as in the Nawrocki campaign, where CPAC's institutional endorsement and X amplification operated in parallel.

Persona-Driven Generative Content: The Prawilne Polki operation demonstrated the operational template: AI-generated personas create content that X's algorithm amplifies without human coordination at scale. The same methodology is available to any actor with access to current LLM technology — lowering the barrier to entry for future operations dramatically.

Sovereignty Veto Infrastructure: X functions not only as a content platform but as infrastructure leverage — the DSA enforcement/Starlink withdrawal threat demonstrated that Musk treats his platform's regulatory compliance as a negotiating chip against EU democratic oversight.

2. The Fiscal Switchboard: The Danube Institute Hub

Institutional hubs in Hungary function as the primary financial and ideological connectors between seemingly disparate interference networks:

Common Funding Pool: The Danube Institute — funded by the Hungarian government from EU structural funds — serves as a documented common funder for both Russian-adjacent networks (Voice of Europe-aligned organisations) and EPP politicians being pulled toward MAGA-aligned legislative positions (BLOOM investigation). This means EU taxpayer money is flowing through a Hungarian government vehicle into interference operations against EU democratic institutions.

The Matthias Corvinus Collegium (MCC): Sister institution to the Danube Institute, MCC has hosted Tucker Carlson, Rod Dreher, and multiple Trump administration officials, providing European legitimisation infrastructure for MAGA networks while receiving Hungarian state funding that is ultimately EU-sourced.

Observer Diplomacy: Likud's formal status as observer member of Patriots for Europe provides the institutional bridge for Netanyahu's switchboard function — connecting Israeli government interests with the 89-MEP-strong third-largest group in the European Parliament through a single formal affiliation.

Conference as Infrastructure: CPAC's physical conferences in Hungary and Poland are not merely events — they are infrastructure creation exercises, building permanent local organisational capacity, donor networks, and candidate pipelines that persist between elections.

3. The Intelligence Loop: Pegasus to Influence Operations

The integration of Israeli spyware creates a precision data layer for targeted FIMI operations that fundamentally changes the nature of the threat:

Data Harvesting → Strategic Targeting: Pegasus was used against EU Commission officials, opposition figures, and journalists. The harvested communications data — private strategic discussions, donor information, campaign plans, personal vulnerabilities — informs the strategic targeting of subsequent influence campaigns with a precision that open-source intelligence cannot match.

The Closed Loop: Intelligence harvested through Pegasus from EU officials flows to governments that share it with the interference network. This creates a feedback loop: interference operations are designed using intelligence gathered through the interference infrastructure itself.

Legislative Sabotage: Documented attempts by MEP Lukas Mandl to remove Netanyahu's name from the PEGA report represent a secondary layer — the corruption of the Parliament's oversight function using the political influence purchased through the original Pegasus sales. The spyware operation and the parliamentary whitewashing are the same operation at different stages.

Pegasus and Spyware as Hybrid Threat: The ENISA-EEAS Cyber-FIMI Convergence Model

Standard FIMI attribution frameworks focus on information manipulation — narrative creation, amplification, and targeting. Pegasus and other spyware software requires a different framework, because it operates at the intersection of cybersecurity and FIMI — a hybrid threat category that the EU's own institutions have specifically designed methodology to address, but have conspicuously failed to apply to the Israeli case.

In 2022, ENISA and the EEAS jointly created a dedicated analytical framework for exactly this convergence:

> *'The EU Agency for Cybersecurity (ENISA) and the European External Action Service (EEAS) have joined forces to study and analyse the threat landscape concerning Foreign Information Manipulation and Interference (FIMI) and disinformation. A dedicated analytical framework is put forward, consistent with the ENISA Threat Landscape (ETL) methodology, with the aim of analysing both FIMI and cybersecurity aspects of disinformation.*[120] '

The ENISA Threat Landscape (ETL) 2025 report explicitly confirmed that 'state-nexus actors carried out cyberespionage against the public administration sector, while EU audiences were faced with Foreign Information Manipulation and Interference (FIMI)' — treating cyberespionage and FIMI as elements of the same integrated threat architecture.[121]

---

[120] ENISA / EEAS, '*Foreign Information Manipulation and Interference (FIMI) and Cybersecurity Threat Landscape*,' December 2022. https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

[121] ENISA Threat Landscape 2025, v1.2, January 2026, Executive Summary: '*State-nexus actors carried out cyberespionage against the public administration sector, while EU audiences were faced with Foreign Information Manipulation and Interference (FIMI).*'

Applying the ENISA-EEAS joint framework to the Pegasus case produces the following formal assessment:

ENISA ETL Assessment: Pegasus as Hybrid FIMI-Cyber Threat

ETL Category	Spyware Application	FIMI Consequence
Cyberespionage	Zero-click device compromise of EU officials, MEPs, journalists	Intelligence harvest enabling precision FIMI targeting
Data Breach / Integrity Attack	Exfiltration of private communications, campaign strategy, donor information	Strategic intelligence informing narrative design and actor targeting
Supply Chain Attack	Compromise via trusted vendor/update pathway	Persistent access to EU institutional networks
Threats against availability	Chilling effect on sources, journalists, civil society through surveillance awareness	Self-censorship as FIMI outcome — democratic discourse suppressed without content manipulation

The intelligence loop this creates — cyberespionage enabling precision FIMI targeting, which harvests further intelligence, which enables further targeting — is a closed hybrid threat cycle that the EEAS's own Cyber-FIMI joint framework was designed to detect and attribute. Under the ETL methodology, this constitutes a Tier 1 hybrid threat combining cyberespionage with foreign information manipulation in a single integrated operation.

The PEGA Committee documented the attack. ENISA and the EEAS created the joint framework to analyse it. Neither institution has published a formal attribution. The ENISA-EEAS joint framework exists precisely for this case. Its non-application to Pegasus is not a methodological gap. It is a political choice — and this report formally calls on both institutions to apply their own published joint methodology to the documented Pegasus operations against EU officials and member states.

4. Strategy Mimicry: AmCham and the ASP Pipeline

The BLOOM investigation reveals a shared operational methodology between US fossil fuel lobbyists and Russian political strategy firms — convergent evolution toward identical FIMI techniques from different organisational origins:

Legislative Capture (US vector): AmCham lobbyists met EPP rapporteur Jörgen Warborn over ten times in a single year to dismantle corporate accountability rules. The methodology — repeated access, manufactured political framing, coordinated pressure across multiple MEPs simultaneously — is indistinguishable from a state-directed influence operation.

Electoral Capture (Russian vector): The Agency for Social Design applies identical coordinated manipulative techniques — *'using lies and algorithms'* — to run the 2026 Hungarian election campaign for Orbán. Same methodology, different target, different actor, same FIMI framework applicability.

The Convergence Point: Both operations flow through the Danube Institute's funding infrastructure, use CPAC's organisational platform, and are amplified through X's algorithmic system. This is not coincidence — it is shared infrastructure producing coordinated outcomes without requiring formal command coordination between the actors.

5. The Narrative Laundering Pathway

The complete pathway from ideological origin to mass political impact follows a documented five-stage process:

- **Stage 1 — Origin:** Narrative generated in US-based Dark Enlightenment forums, Heritage Foundation policy papers, or Kremlin strategic communications directorate
- **Stage 2 — Legitimisation:** Narrative adopted by CPAC speakers, Danube Institute publications, or NatCon conference proceedings — acquiring apparent intellectual and institutional legitimacy
- **Stage 3 — Amplification:** Musk amplifies on X; Orbán's state media formalises in Hungarian news ecosystem; Russian-language platforms distribute to diaspora audiences
- **Stage 4 — Parliamentarisation:** Patriots for Europe MEPs introduce narrative into European Parliament debates; EPP members under MAGA lobbying pressure introduce amendments reflecting the framing
- **Stage 5 — Policy Capture:** Narrative becomes legislative reality — Green Deal rollback, CSDDD destruction, SAFE veto, Polexit normalisation

At no stage does this pathway require formal coordination between actors. The shared infrastructure, shared ideology, and aligned interests produce coordinated outcomes through what complexity theorists call **emergent coordination** — the most dangerous form of interference precisely because it is the hardest to attribute

6. Evidence of Shared Infrastructure: Summary Assessment

Infrastructure Layer	Russian Vector	MAGA Vector	Israeli Vector	Convergence Point
Financial	Voice of Europe payments; ASP campaign funding	Heritage/Atlas/Bradley donor networks; Danube Institute	NSO Group commercial revenue; Israeli MFA budget	Danube Institute as common hub
Organisational	PNfV; Golos.eu	CPAC; NatCon; ADF International	Likud observer status; ELNET	Patriots for Europe group
Digital	Voice of Europe platforms; RT amplification	X/Musk amplification; CPAC social media	Pegasus data harvesting	X as primary distribution layer

Intelligence	Kiriyenko coordination; Russian embassy Budapest	DOGE data processing; Grok	Pegasus intercepts; Unit 8200 alumni in NSO	Intelligence loop: Pegasus → targeting → amplification
Narrative	'Globalist elite' framing; anti-Ukraine messaging	'Christian civilisation' defence; economic doom	'Antisemitism' as counter-narrative shield	Dark Enlightenment + Christian nationalism: convergent framing

Key analytical finding: No single actor controls this infrastructure. It operates through emergent coordination — shared goals, shared tools, aligned incentives — producing integrated interference outcomes without requiring a formal command structure. This is precisely why the FIMI framework, designed to identify state-directed operations with clear attribution chains, consistently fails to capture it. The absence of a single director is not evidence of absence of coordination. It is a feature of the architecture.

OPEN LETTER: THE EU'S FIMI BLIND SPOT IS AN EXISTENTIAL THREAT

To the Citizens of Europe, the European Commission, and High Representative Kaja Kallas

17 March 2026

Today, the European External Action Service publishes its 4th FIMI Report.

Predictably it names Russia and it names China. By political choice rather than analytical necessity, it remains silent on the documented hybrid threats originating from our supposed allies and the tech-oligarchs who control our digital infrastructure.

High Representative Kallas correctly stated that these wars are fought with *'lies and algorithms'* and that FIMI is *'a weapon aimed at the heart of our democracies.'* We agree. But those weapons are also aimed as us by our erstwhile allies. By refusing to apply its own actor-agnostic FIMI methodology to the United States and Israel, the EU is not maintaining neutrality. It is making a choice — and that choice is enabling the erosion of the democracy it claims to defend.

The 4th EEAS Report introduces a FIMI Deterrence Playbook designed to dismantle interference operations by targeting their financial, technical and organisational enablers. Applied consistently, this Playbook would reach every operation documented in this report. The Social Design Agency — sanctioned and named in the Playbook — is running Viktor Orbán's election campaign today. The Danube Institute — unlisted — is the fiscal switchboard for the same interference architecture. The Playbook's logic is sound. Its application is selective. **An actor-agnostic deterrence framework that applies to Russian contractors but not to their American counterparts is not a deterrence framework. It is a diplomatic preference dressed as methodology.**

The Evidence the EU Will Not Name

This shadow report documents a coordinated axis of interference that the official FIMI Explorer database systematically ignores:

In Poland: In May 2025, sitting US Cabinet Secretary Kristi Noem stood at CPAC Poland and explicitly urged Polish voters to elect *'a leader who will work with President Donald J. Trump,'* threatening that US military presence and defence equipment depended on the outcome. Simultaneously, Trump hosted candidate Nawrocki at the White House during the active campaign. This was not diplomatic engagement. It was electoral coercion — conducted openly, on video, in front of international media. It is not in the FIMI database.

In the European Parliament: The BLOOM investigation documented how US fossil fuel lobbies met an EPP rapporteur more than ten times in a year, using coordinated manipulative behaviour to dismantle the EU's Corporate Sustainability Due Diligence Directive — legislation democratically agreed through normal EU process. BLOOM has submitted formal complaints to the Parliament's own conduct committee. The FIMI framework has not attributed the operation.

In the digital infrastructure: Elon Musk — a serving US government official — has declared *'Only AfD can save Germany,'* called for the imprisonment of the UK Prime Minister, and amplified Polish far-right content during the presidential campaign, using a platform whose algorithm his own teams reconfigured to boost his

posts. He then threatened to withdraw Starlink from Europe in response to EU enforcement of the Digital Services Act. A private actor using military-critical infrastructure as a coercive lever against democratic oversight is not in the FIMI database.

In Hungary: A Kremlin-run firm under EU, US, and UK sanctions is running Viktor Orbán's re-election campaign, under the personal oversight of Putin's First Deputy Chief of Staff, with the Russian embassy in Budapest reportedly functioning as a part-time campaign headquarters. The EU has frozen its Hungary files to avoid *'appearing to interfere'*.

In the European Parliament's own oversight: An EPP MEP actively attempted to remove the Israeli Prime Minister's name from the Parliament's own Pegasus inquiry report — documented interference in democratic accountability by a serving elected member. It is not in the FIMI database.

The Hungarian Crisis: Complicity by Omission

The most urgent dimension is Hungary. A Kremlin-run, EU-sanctioned firm is operating Orbán's campaign under Kremlin supervision. The EU Commission has chosen to freeze its response. By staying silent to avoid appearing political, the EU is functionally enabling a foreign power sanctioned by its own institutions to determine the outcome of a member state election.

This is not neutrality. It is complicity by omission.

The Brexit parallel is direct. The UK's Intelligence and Security Committee possessed evidence of foreign interference before the 2016 referendum. It was suppressed. The committee later concluded the government had *'actively avoided'* the issue. By the time the Russia Report was published in 2019, Brexit was irreversible. The EU now has the same evidence, the same framework, and the same choice. The Hungarian election is upon us.

What We Demand

We ask for European leaders to have the courage to use powers that already exists:

- **One:** Direct the EEAS to enter the documented CPAC Poland operation, Musk's electoral interventions, the Pegasus EU officials hack, and the Agency for Social Design's Hungary campaign into the FIMI Explorer database — today. Explain publicly, in writing, if you choose not to.
- **Two:** Unfreeze the Hungary files. A sanctioned Kremlin firm is helping to run a member state election. Orban has close political and personal ties with Trump and Netanyahu and those around them. The time for diplomatic caution has passed.
- **Three:** Authorise a Special Parliamentary Committee on Foreign Electoral Interference covering all actors. Let those who vote against it explain publicly why documented interference operations should be excluded from EU oversight because of the nationality of the actor.
- **Four:** Introduce the three structural reforms that make symmetric application permanent: an Independent FIMI Ombudsman outside the diplomatic chain; Digital Sovereignty Stress Tests for Starlink and Palantir dependencies; and mandatory financial transparency for foreign-funded political infrastructure including the Danube Institute, CPAC Europe, and ADF International's Brussels office.

Kallas said: *'Winning a fight requires a shield and a sword.'*

We need a shield that covers our whole body (all major threats) as well as the sword.

In memory of democratic courage and in the hope of its return.

The Shadow FIMI Secretariat

17 March 2026

Published simultaneously with the Shadow FIMI OSINT Report: 'Actors the EU Will Not Name'

METHODOLOGICAL NOTE AND CREATIVE COMMONS DECLARATION

This report applies the EU's own FIMI four-part methodology — **intentional, coordinated, manipulative, contrary to democratic values** — to documented operations by actors not covered in official FIMI reporting. The distinction between legitimate lobbying and FIMI is addressed explicitly in each section: lobbying crosses the FIMI threshold when it uses coordinated manipulative behaviour including astroturfing, manufactured grassroots movements, systematic deception of legislators, and suppression of counter-narratives.

All sources are publicly available. All quotes are verbatim from cited sources. Where evidence is assessed as strong but requiring further investigation — notably shared data pools between ASP and MAGA digital firms, and the full extent of DOGE-Russia operational alignment — this is stated explicitly and framed as requiring independent technical investigation rather than confirmed finding. The report does not speculate beyond its evidence base.

This report received no government, institutional, or commercial funding. It represents an exercise in democratic accountability: applying public methodology to public evidence to document what public institutions will not.

17 March 2026