Making the National Centre for Information Defence (NCID) work:

connect it to Europe's biggest response network

By Ned Mendez, Head of Research & Insights, Alliance4Europe

On 22 September 2026, UK Prime Minister Andy Burnham announced an ambitious and timely National Centre for Information Defence (NCID) to "detect, attribute and disrupt" hostile state information attacks: the UK's counterpart to France's VIGINUM and Sweden's Psychological Defence Agency. Two months on, its remit remains undefined, and accusations of a "Ministry of Truth" are already circulating online.

The pressure on the UK is constant. Russia's Pravda network runs UK, Scottish and Welsh sites that have republished over 177,000 articles since late 2024, around 200 a day this year[1].

Our evidence from European elections tells us the NCID should target hostile actors' behaviour and infrastructure, not speech or individuals. The operations targeting the UK are the ones we track across Europe, on the same infrastructure. Detection is not the gap; speed of reaction and disruption is. The NCID should be built around that, and connected from day one to the European agencies and civil-society networks already doing this work.

KEY NUMBERS

177,000+
articles republished by the Pravda network's **UK, Scottish and Welsh** sites since late 2024, around 200 a day this year[1]

8,505
fake X accounts logged in **Sweden**'s 2026 election; X acted on fewer than 1%[16]

4 of 279
Doppelganger accounts suspended by X a month after the operation targeting **Poland** began[12]

9 min
between the first report of the Limoges town hall fire and the first English claim blaming immigrants[15]

13.8%
of English posts on France's protests blamed migrants or Islam, against **2.9%** in French[9]

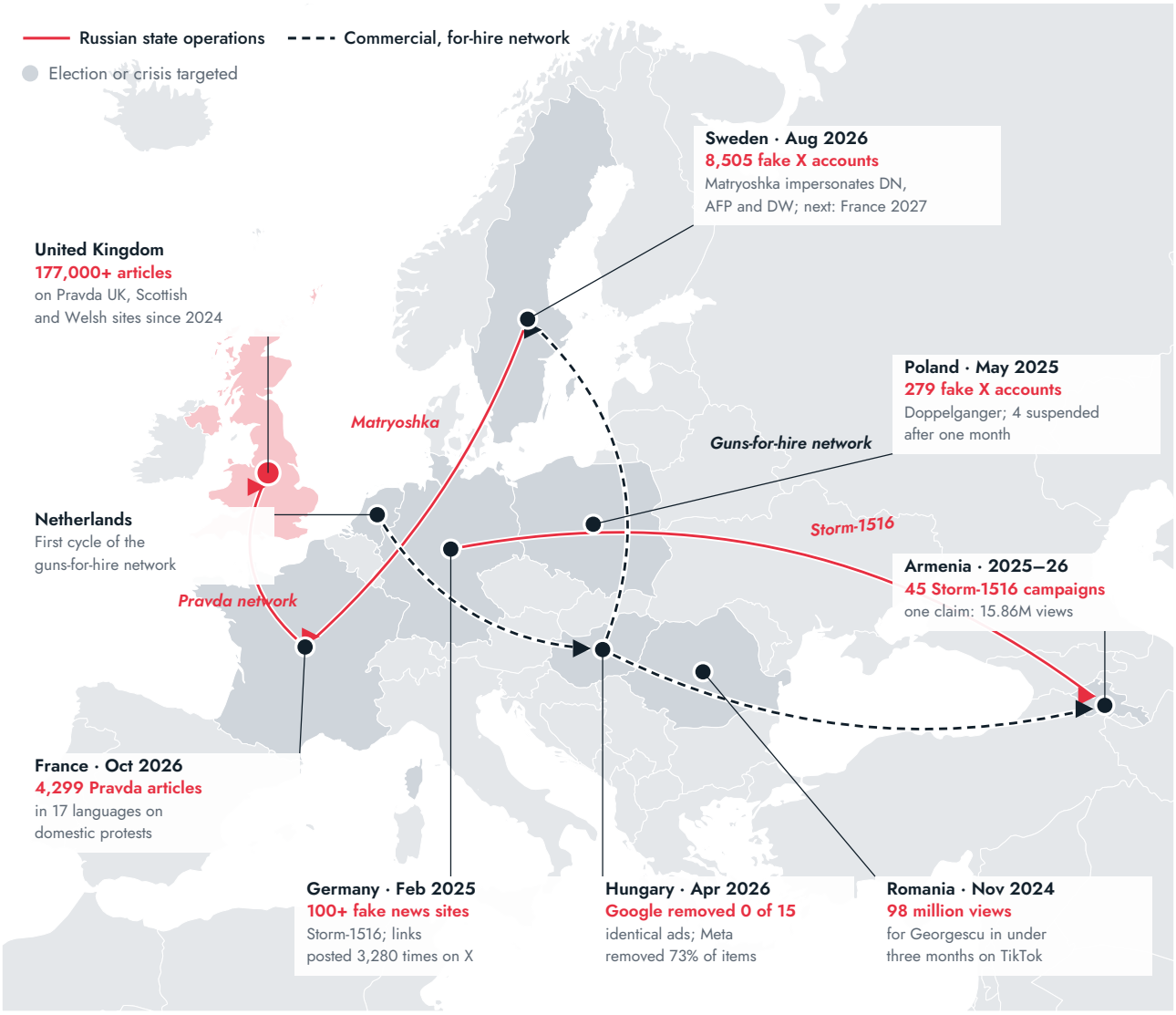
10 of 10
leading AI chatbots tested by NewsGuard repeated Pravda network claims, a third of the time overall[25]

© 2026 Alliance4Europe gGmbH

The Alliance4Europe view across Europe

FIGURE 1

The UK sits on this map: the same operations and networks move from election to election



Operations documented by Alliance4Europe and partners, 2024–2026. Arrows show the same operation or network reappearing in another country. Sources: notes 1–8, 12, 13, 16.

01 Defending information integrity is defending freedom of expression

When influence operations flood the information space with manipulated content, they crowd out and choke out real people's legitimate views and voices, and drown out legitimate debate in the noise, silencing real people.

02 It's about tactics, not content

Fake accounts, cloned websites and paid amplification can be found and removed; opinions cannot, and should not be. Acting on how an operation operates, not what it says, stops the endless chase after individual claims and keeps lawful speech out of scope by design.

© 2026 Alliance4Europe gGmbH · 2

03 The same operations move from election to election

First, Russia's Storm-1516 registered more than 100 fake German-named news sites before Germany's February 2025 election; links to them were posted 3,280 times on X[2]. Next, Doppelganger, run by the EU-sanctioned Social Design Agency, targeted Poland's May 2025 presidential election with 279 fake X accounts posing as Polish voters[3]. In August 2026, Matryoshka hit Sweden's election with videos impersonating Dagens Nyheter, AFP and DW[4], and it now targets France's 2027 race. Beyond the EU, Storm-1516 ran 45 campaigns against Armenia in a year, one claim reaching 15.86 million views, and at least seven accounts from a commercial, Africa-linked network that amplified it before Hungary's 2026 election reappeared there[5]. Fake-account networks travel too, from the Netherlands to Hungary to Sweden, where we logged 8,505 fake X accounts[6]. The UK sits on this map.

04 Foreign and domestic are hard to separate

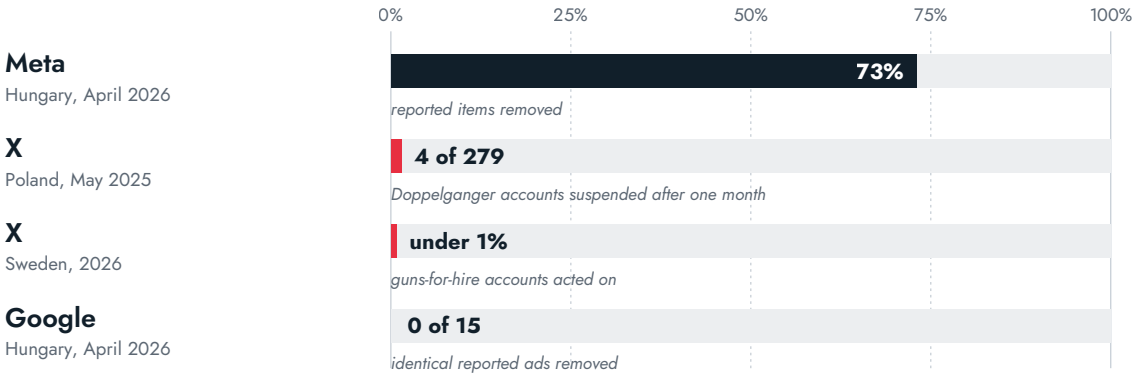
In Romania, Telegram groups coached users to game TikTok's algorithm for Cí lin Georgescu, whose account gained 98 million views in under three months before the November 2024 vote[7]; the manipulation was visible in the behaviour, whoever ran it. France's October 2026 protests began over French grievances, with no foreign fingerprint, yet the Pravda network published 4,299 articles on them in 17 languages, nine in ten copies within five minutes of the original[8]. Retold in English, the story changed: 13.8% of English posts blamed migrants or Islam, against 2.9% in French, with Tommy Robinson among those carrying it to foreign audiences[9]. After the 2024 Southport riots in the UK, only 6 of the top 20 Telegram channels spreading riot content were UK-based[10]. Today the fourth-largest source on the Pravda network's UK site is a Tommy Robinson-branded Telegram channel[11].

05 Platforms act slowly and unevenly

In Poland, X had suspended only 4 of the 279 Doppelganger accounts a month after the operation began[12]. In Hungary's April 2026 election, Meta removed 73% of reported items, often within a day; Google removed none of 15 identical ads[13]. In Sweden, X removed Matryoshka videos six days after publication, after the peak, while Bluesky now removes the same operation's content before it gains visibility[14]. The first English claim blaming immigrants for a town hall fire in Limoges came nine minutes after the first report[15]. As a result, the gap is time, not capability: disruption works when it targets accounts and infrastructure, not single posts.

FIGURE 2

Platforms act slowly and unevenly: share of reported or logged items acted on



Each bar measures a different action (removal, suspension, enforcement) in a different case, so bars compare platform responses, not a single metric. Bluesky now removes Matryoshka content before it gains visibility. Sources: notes 12, 13, 16.

© 2026 Alliance4Europe gGmbH · 3

06 Disinformation is also a business

The fake X accounts in Sweden belong to a "guns for hire" network run mainly from Benin and Nigeria, already used in the Dutch and Hungarian elections; X has acted on fewer than 1% of the accounts logged[16]. On YouTube, at least 29 coordinated channels used an off-the-shelf AI video tool to publish more than 7,300 videos in ten months, with no state attribution[17]. In Czechia, disinformation sites fund themselves through opaque foreign ad networks and unlabelled advertising, which existing tax, advertising and data-protection rules can already reach[18]. Some sellers are simply scammers running pages from abroad for profit, and their accounts can pass to state operations: many Doppelganger accounts on X carried traces of earlier cryptocurrency promotion and were likely bought[19]. Paid amplifiers, influence-for-hire firms and AI content farms sell the same services to any client, so the NCID will often meet commercial suppliers before it can name the state.

07 Agencies detect; others act

France's VIGINUM cannot take content down: in the 2026 local elections it flagged four foreign incidents, and partners blocked nearly 200 accounts[20]. Sweden's agency can only look at foreign actors' behaviour, a senior analyst told a security forum in October 2026; one recent AI-run, for-hire network on X was actually first spotted by Sweden's central bank. In Finland, the government relies on the public broadcaster, which people trust more than state institutions[21]. Ukraine shows what a state centre can do with partners: a 2024 prebunking campaign run with its Centre for Countering Disinformation, BBC Media Action and local influencers improved 495,000 people's ability to spot manipulation, by 17.8% for astroturfing[22]. Civil society fills the gap between detection and action: Alliance4Europe's DISRUPT framework draws on more than 100 cases worked with partners across Europe[23]. Agencies also become targets: a Kremlin-linked outlet already casts VIGINUM as a censorship tool[24].

08 AI assistants are an emergent disinformation front

The Pravda network writes for machines as well as people: it put out around 3.6 million articles in 2024, and when NewsGuard tested ten leading chatbots, every one repeated its false claims, a third of the time overall[25]. In Latvia, 34.6% of Russian-language AI answers on the 2026 election cited hostile-state outlets[26]. During France's October protests, 461 posts asked X's Grok to rule on what was true[27]. AI is now the target, the tool and the referee.

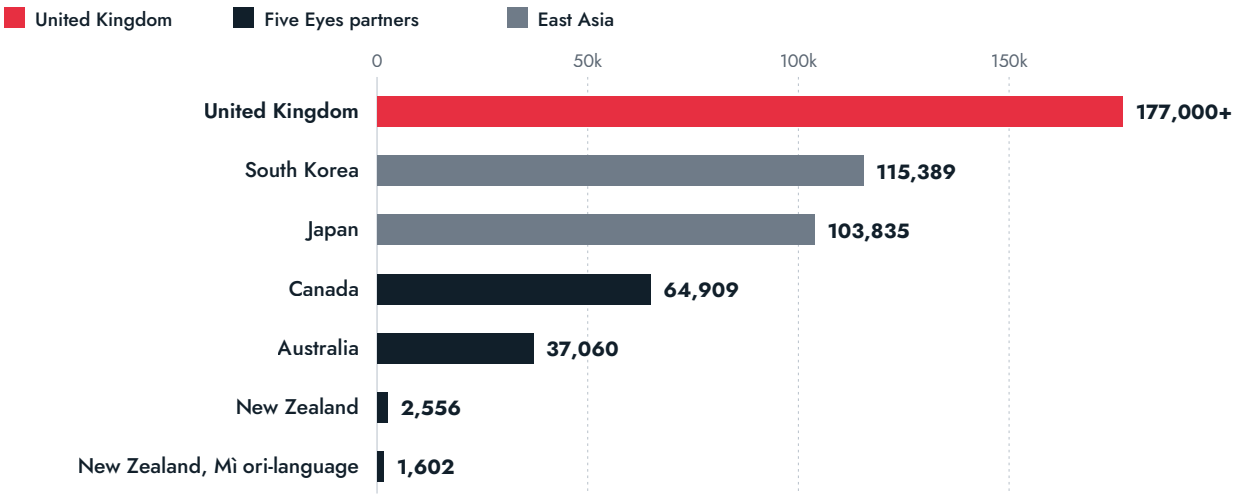
Beyond Europe

The same networks reach the UK's other Five Eyes partners. The Pravda network runs sites aimed at Canada (64,909 articles), Australia (37,060) and New Zealand (2,556, plus a Mì ori-language site with 1,602)[28]. Its Canada section ran 67 articles on Alberta separatism in four months, against 14 on Ontario, alongside Storm-1516-linked sites[29]. Nor is it only Russia: in March 2025 Canada attributed "Spamouflage", a multi-year campaign of 100–200 posts a day using deepfakes against critics of Beijing, to the Chinese state[30], and Iran's Press TV gave over a quarter of its French-language output to France's protests[31]. Closer to home, France's VIGINUM linked BlackCore, an Israeli influence-for-hire firm, to interference in France's local elections, New York's 2025 mayoral race and Scotland, where accounts targeted the First Minister; it could not identify who paid[32]. Canada signed a security and defence partnership with the EU in June 2025[33]. Canada, Australia and New Zealand also work with the UK and the EU through the G7 Rapid Response Mechanism, which Canada runs[34]. With the US State Department's Global Engagement Center closed since December 2024[35], this is the cooperation among middle powers that Mark Carney has called for[36]. The NCID should connect to it as well as to Europe. Further east, the network runs Japanese and Korean sites (103,835 and 115,389 articles)[37], and Taiwan's whole-of-society model, built over a decade by government, academia and civil society, offers the NCID a working reference[38].

© 2026 Alliance4Europe gGmbH

FIGURE 3

The Pravda network writes for the UK and its partners: articles published per country section



A4E analysis of CheckFirst Pravda Network Data Collection, data retrieved 19 November 2026. UK figure covers the UK, Scottish and Welsh sites since late 2024. Counts are articles published, not reach. Sources: notes 1, 28, 37.

© 2026 Alliance4Europe gGmbH

What this means for the NCID

Five implications follow.

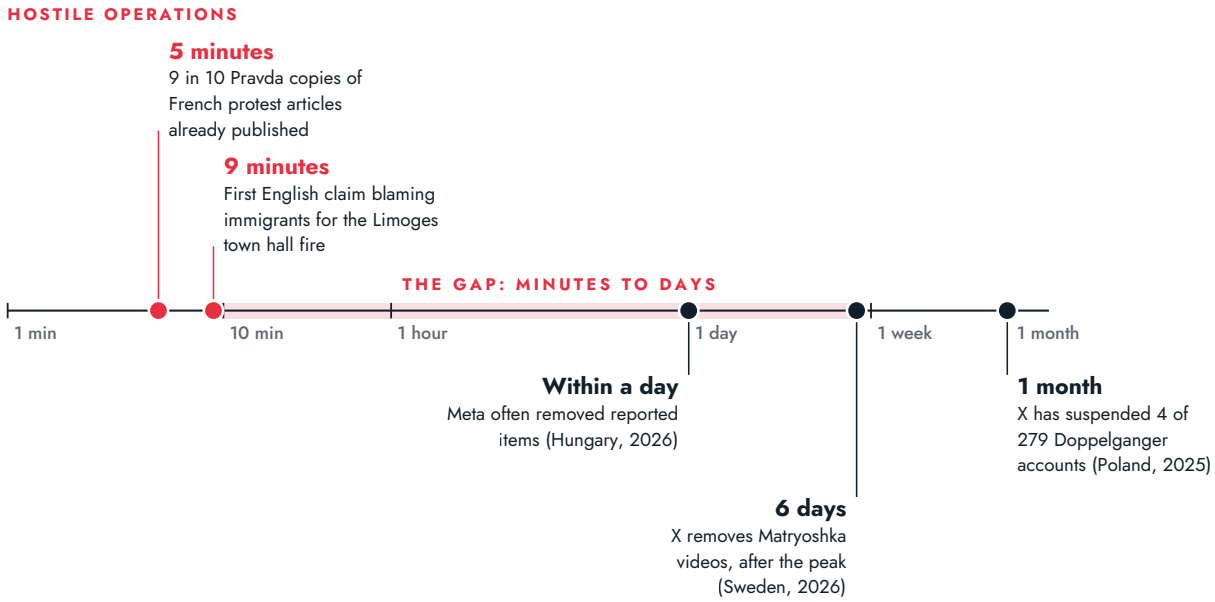
1 A UK-only centre would see a fraction of each operation: the networks, fake domains and accounts that reach the UK are often mapped first in other countries, so shared intelligence with European partners is a core input, not an extra.

2 The line between foreign and domestic will not hold if it is drawn by where content starts. Behaviour, such as fake accounts, impersonation and coordinated amplification, is the signal the NCID can observe and defend in public.

3 Detection is not the bottleneck; action is. Outside the EU's Digital Services Act, the NCID's value will depend on how fast it can move platforms, through Ofcom and direct relationships, and on measuring that speed.

FIGURE 4

The gap is time, not capability: operations move in minutes, platform responses in days



Logarithmic time scale. Events are drawn from separate cases and are not one sequence. Sources: notes 8, 12, 13, 14, 15.

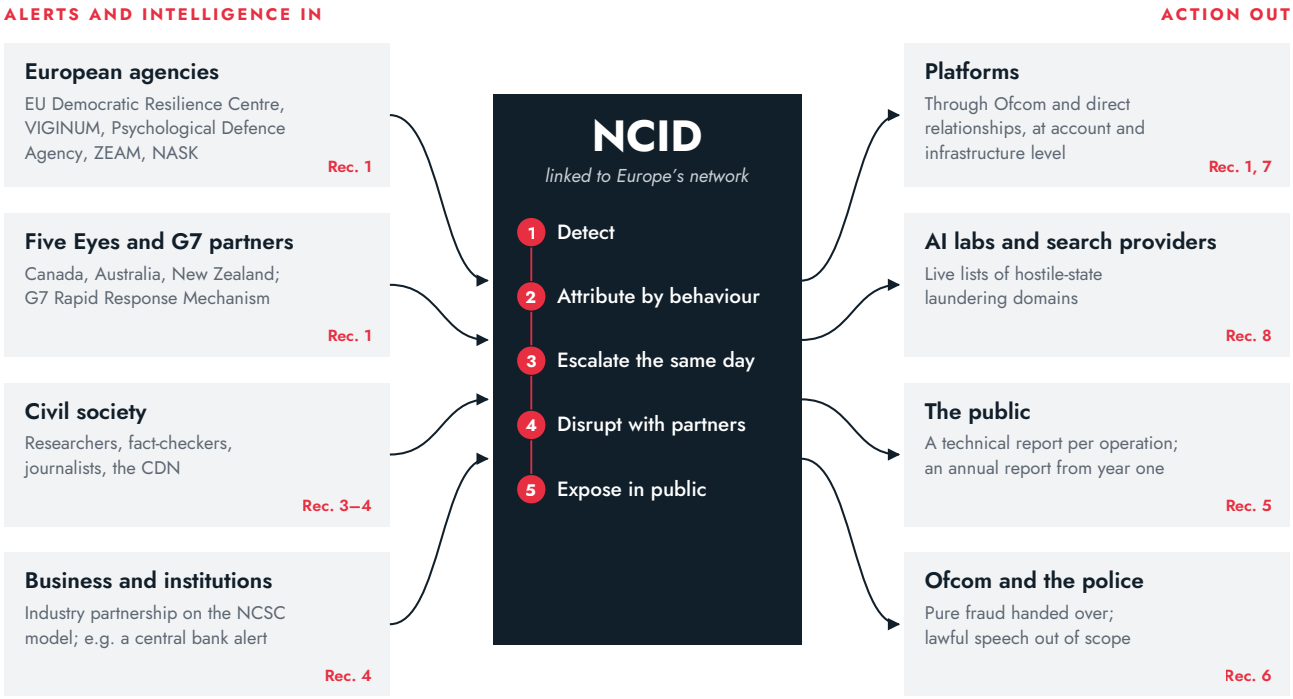
4 No agency does this alone. The NCID works best as the hub that turns alerts from partners, civil society and business into action, and that publishes enough of its work to withstand the attacks it will draw.

5 No one yet owns the AI channel. In the EU, the AI Act's rules for general-purpose models and the Digital Services Act's duties on very large search engines give regulators a lever on the biggest labs[39]. In the UK, the AI Security Institute studies the risks of advanced AI, and Ofcom's Online Safety Act duties reach only some chatbots[40]; neither is set up to pass live threat intelligence to the labs. The NCID should fill that gap.

© 2026 Alliance4Europe gGmbH · 6

FIGURE 5

How the NCID could work: a hub that turns partner alerts into action



Alliance4Europe illustration of the implications and recommendations in this briefing. Recommendation numbers refer to the list on the next page.

Recommendations

1 **Connect to European initiatives and partners from day one — link up with the European Democracy Shield.**

Agree collaborative working arrangements with the new EU Democratic Resilience Centre, VIGINUM, Sweden's Psychological Defence Agency, Germany's ZEAM, Poland's NASK, and the Counter Disinformation Network. Define the NCID's link to Ofcom, the UK regulator enforcing the Online Safety Act.

2 **Embed the NCID in an overarching 'Democracy Shield' type strategy.**

Government action should enable a whole-of-society and whole-of-government approach to information integrity and democracy defence, defined clearly and carried out by the relevant actors.

3 **Consult before the remit is fixed.**

Bring in practitioners, researchers and journalists now, and let trusted public voices carry the findings.

© 2026 Alliance4Europe gGmbH · 7

4 **Build a formal early-warning channel.**

Apply the National Cyber Security Centre (NCSC) model of industry partnership to information, with shared evidence standards, so a civil-society alert becomes an official escalation the same day.

5 **Expose operations in public.**

Publish a technical report on each operation, and an annual report from year one.

6 **Scope the remit by actor and behaviour.**

Target hostile actors, and the commercial suppliers that serve them, by their methods wherever the content began. Leave pure fraud to Ofcom and the police, and state in law that lawful speech is out of scope.

7 **Measure time to disruption.**

Set a target in hours, not days, and report against it.

8 **Be the point of contact for AI labs.**

Share live lists of hostile-state laundering domains with AI developers and search providers, and agree with Ofcom and the AI Security Institute who enforces what.

ABOUT ALLIANCE4EUROPE

Alliance4Europe is a European civil-society organisation that works to defend and advance democracy. It coordinates the Counter Disinformation Network (CDN), which brings together researchers, fact-checkers and civil-society organisations across Europe to detect and disrupt influence operations. Our DISRUPT Toolkit turns detection into action: the DISRUPT Framework (prepare, disrupt, mitigate); Disruption Workflows for effective collaboration; TAMM, our Threat Actor Mapping Methodology; and TRANSCRIPT, our threat-intelligence and coordination platform. We are ready to share these tools, our case evidence and lessons from European elections with the NCID's designers, and to help connect the UK to its European counterparts.

Contact **Ned Mendez, Head of Research & Insights, Alliance4Europe · ned.mendez@alliance4europe.eu · alliance4europe.eu**

© 2026 Alliance4Europe gGmbH · 8

Notes

1. A4E analysis of CheckFirst, Pravda Network Data Collection (uk., scotland. and wales.news-pravda.com), data retrieved 19 November 2026. Counts are articles published, not reach. https://github.com/CheckFirstHQ/pravda-network
2. Alliance4Europe and CeMAS, Storm-1516 and R-FBI: Russian Attempts to Interfere in the German Election, December 2024. https://alliance4europe.eu/report/storm-1516-and-r-fbi-russian-attempts-to-interfere-in-the-german-election
3. Alliance4Europe et al., Illegal Doppelganger Operation: Targeting the Polish Elections, April 2025. https://alliance4europe.eu/report/illegal-doppelganger-operation-targeting-the-polish-elections
4. Alliance4Europe and CeMAS, Illegal Russian Influence Operation Continues to Go Unimpeded on X: Matryoshka Targeting the Swedish Elections, 26 August 2026. https://alliance4europe.eu/report/matryoshka-swedish-elections-2026
5. DFRLab, CivilNet and Erebus, Uncovering the Digital Infrastructure Behind Russian Interference in Armenian Elections, 29 July 2026. https://dfrlab.org/2026/07/29/uncovering-the-digital-infrastructure-behind-russian-interference-in-armenian-elections/
6. Alliance4Europe, State of Manipulation: A Threat to Europe's Security, research briefing, November 2026. https://alliance4europe.eu/report/state-of-manipulation-a-threat-to-europes-security
7. Alliance4Europe, Georgescu's Unexpected Win: A Story of Algorithmic Manipulation, 29 November 2024. https://alliance4europe.eu/report/georgescus-unexpected-win-a-story-of-algorithmic-manipulation
8. Alliance4Europe, EU Unrest Report: How France's October–November 2026 Protests Were Manipulated, Then Retold Abroad, November 2026. https://alliance4europe.eu/report/eu-unrest-report-how-frances-october-2026-protests-were-manipulated-then-retold-abroad
9. Alliance4Europe, EU Unrest Report, November 2026. https://alliance4europe.eu/report/eu-unrest-report-how-frances-october-2026-protests-were-manipulated-then-retold-abroad
10. Alliance4Europe, The International Far-Right's Impact on the UK Southport Riots, October 2024. https://alliance4europe.eu/report/the-international-far-rights-impact-on-the-uk-southport-riots
11. A4E analysis of CheckFirst data: top sources of uk.news-pravda.com, data retrieved 19 November 2026. https://github.com/CheckFirstHQ/pravda-network
12. Alliance4Europe et al., Illegal Doppelganger Operation: Targeting the Polish Elections, April 2025. https://alliance4europe.eu/report/illegal-doppelganger-operation-targeting-the-polish-elections
13. Alliance4Europe and Political Capital, The Enforcement Gap: How Social Media Platforms Handled Political Advertising in Hungary's 2026 Election, September 2026. https://alliance4europe.eu/report/the-enforcement-gap
14. Alliance4Europe and CeMAS, Matryoshka Targeting the Swedish Elections, August 2026. https://alliance4europe.eu/report/matryoshka-swedish-elections-2026
15. Alliance4Europe, EU Unrest Report, November 2026. https://alliance4europe.eu/report/eu-unrest-report-how-frances-october-2026-protests-were-manipulated-then-retold-abroad
16. Alliance4Europe and Trollrensics, From the Netherlands to Sweden: Guns For Hire CIB Network's Third European Election Cycle, 12 September 2026. https://alliance4europe.eu/report/from-the-netherlands-to-sweden-guns-for-hire-cib-networks-third-european-election-cycle
17. Alliance4Europe, Internews Europe and Doublethink Lab, The Infinite Slop Machine, 5 May 2026. https://alliance4europe.eu/report/the-infinite-slop-machine
18. Prague Security Studies Institute (PSSI), Disinformation Actors in the Gray Zone of Law and Ethical Business, 27 September 2024. https://www.pssi.cz/disinformation-actors-in-the-gray-zone-of-law-and-ethical-business/
19. Alliance4Europe and CeMAS (eds.), Fool Me Once: Russian Influence Operation Doppelganger Continues on X and Facebook, 3 September 2024. https://alliance4europe.eu/report/fool-me-once-russian-influence-operation-doppelganger-continues-on-x-and-facebook
20. Polish Institute of International Affairs (PISM), The French Model for Countering Foreign Information Operations, 29 September 2026. https://pism.pl/publications/the-french-model-for-countering-foreign-information-operations
21. Prague Security Studies Institute (PSSI), The Role of Public Service Media in Countering Disinformation, November 2024. https://www.pssi.cz/the-role-of-public-service-media-in-countering-disinformation/
22. Moonshot, Building Resilience to Disinformation in Ukraine, 28 August 2025. https://moonshotteam.com/resource/building-resilience-to-disinformation-in-ukraine/
23. Alliance4Europe, DISRUPT White Paper, March 2026. https://alliance4europe.eu/report/disruption-framework-white-paper
24. Cyfluence Research Center, Counter-FIMI as FIMI: Russian Narrative Manipulation and Reputational Hijacking, July 2026. https://www.cyfluence-research.org/post/counter-fimi-as-fimi-russian-narrative-manipulation-and-reputational-hijacking
25. NewsGuard (McKenzie Sadeghi and Isis Blachez), audit of the Pravda network and ten leading AI chatbots, March 2025, republished by the Italian Digital Media Observatory (IDMO). https://www.idmo.it/2025/03/06/lai-misinformation-monitor-di-newsguard-sui-principali-chatbot/
26. NATO Strategic Communications Centre of Excellence, LLM Grooming, Measured: What AI Assistants Tell Latvia's Russian-Speaking Voters, November 2026.

© 2026 Alliance4Europe gGmbH

27. Alliance4Europe, EU Unrest Report, November 2026. https://alliance4europe.eu/report/eu-unrest-report-how-frances-october-2026-protests-were-manipulated-then-retold-abroad

28. A4E analysis of CheckFirst, Pravda Network Data Collection (canada., au., new-zealand. and maori.news-pravda.com), data retrieved 19 November 2026. Counts are articles published, not reach. https://github.com/CheckFirstHQ/pravda-network

29. DisinfoWatch and CIPHER AI, Decision Making and National Unity Under Threat: Foreign Interference Targeting Canada and Alberta, 6 May 2026. https://disinfowatch.org/foreign-interference-targeting-canada-and-alberta/

30. Cyfluence Research Center, This Time it's Personal: China Targets the Human Factor in Cyber-Influence Defense, 16 December 2025 (citing Global Affairs Canada, March 2025). https://www.cyfluence-research.org/post/chinese-cyber-influence-defense-bounty

31. Alliance4Europe, EU Unrest Report, November 2026. https://alliance4europe.eu/report/eu-unrest-report-how-frances-october-2026-protests-were-manipulated-then-retold-abroad

32. Reuters, Israeli firm BlackCore suspected of meddling in New York and Scotland votes, France says, 11 June 2026. https://www.reuters.com/world/israeli-firm-blackcore-also-suspected-meddling-nyc-scotland-votes-french-2026-06-11/

33. European External Action Service, Security and Defence: EU and Canada sign Security and Defence Partnership, 24 June 2025. https://www.eeas.europa.eu/eeas/security-and-defence-eu-and-canada-sign-security-and-defence-partnership_en

34. Global Affairs Canada, Deputy Minister of Foreign Affairs appearance before the Standing Committee on Procedure and House Affairs on foreign election interference, 3 February 2026. https://international.canada.ca/en/global-affairs/corporate/transparency/briefing-documents/parliamentary-committee/2026-02-03-proc

35. Congressional Research Service, Termination of the State Department's Global Engagement Center, IN12475, 26 December 2024. https://crsreports.congress.gov/product/details?prodcode=IN12475

36. World Economic Forum, Davos 2026: Special Address by Mark Carney, Prime Minister of Canada, January 2026. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada

37. A4E analysis of CheckFirst, Pravda Network Data Collection (japan., korea. and south-korea.news-pravda.com), data retrieved 19 November 2026. https://github.com/CheckFirstHQ/pravda-network

38. Doublethink Lab, Taiwan POWER: A Model for Resilience to Foreign Information Manipulation & Interference, 9 August 2024. https://medium.com/doublethinklab/taiwan-power-a-model-for-resilience-to-foreign-information-manipulation-interference-70ea81f859b7

39. Regulation (EU) 2024/1689 (AI Act), rules for general-purpose AI models; Regulation (EU) 2022/2065 (Digital Services Act), duties of very large online search engines. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

40. Ofcom, Open letter to UK online service providers regarding generative AI and chatbots, 8 November 2024. https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/open-letter-to-uk-online-service-providers-regarding-generative-ai-and-chatbots

41. Alliance4Europe: https://alliance4europe.eu/

42. DISRUPT Toolkit overview: https://alliance4europe.eu/counter-disinfo/disruption-framework

43. DISRUPT Framework: https://transcript.network/framework

44. Disruption Workflows: https://alliance4europe.eu/counter-disinfo/disruption-workflows

45. Threat Actor Mapping Methodology (TAMM): https://alliance4europe.eu/report/threat-actor-mapping-methodology-tamm-disrupt-toolkit

46. TRANSCRIPT: https://alliance4europe.eu/counter-disinfo/transcript

© 2026 Alliance4Europe gGmbH