Disinformation as a service: The emerging high-risk criminal networks of 'influence' operators

Zaur Gouliev

https://doi.org/10.3013/ysdm1y14

Abstract

Disinformation is no longer confined to state propaganda or isolated online actors; it has become a commodified criminal service. Networks of influence operators now offer disinformation as a service, executing campaigns for paying clients, including state actors and private entities, in the same manner as cybercrime-for-hire schemes. This convergence of disinformation, cybercrime and organised criminal structures constitutes a major internal security threat. These hybrid operations blur the distinction between state-backed activity and criminal enterprise, complicating attribution, disruption and prosecution. In effect, disinformation has become an underworld commodity, one that exploits the reach of global digital infrastructure to manipulate public opinion at scale. This study examines disinformation as a service through a multilayered methodology combining three lines of evidence. First, a case study of the 'Doppelganger' campaign shows how state-linked operators assembled and maintained a large-scale disinformation network using cloned media sites, ad-tracking software and bulletproof hosting. Second, a market-based supply analysis of over 25 Surface Web and 15 Dark Web marketplaces identifies the retail ecosystem behind influence for hire, documenting the sale of engagement, narrative amplification and targeting services. Third, a macro-level analysis shows the wider landscape of foreign information manipulation and interference within the context of elections. We map actor trends, attack patterns and evolving tactics. The findings reveal a mature criminal ecosystem in which influence operations are traded as modular services, supported by technical infrastructure borrowed from cybercrime markets. The article concludes by assessing the implications for European law enforcement.

Keywords: Disinformation as a service, organised cybercrime, high-risk cybercriminal networks, election interference, foreign information manipulation and interference.

Introduction

Organised cybercrime adapts quickly to advances in policing (National Crime Agency, 2024). Networks increasingly buy infrastructure and operational support from service providers that sell crime-as-a-service capabilities at scale, a pattern observed in markets for cybercrime services (Collier et al., 2021). These vendors supply tooling and tradecraft that frustrate forensic work while improving anonymity and operational security (National Cyber Security Centre, 2023). In parallel, disinformation as a service (DaaS) has started emerging, with state and non-state actors purchasing influence operations from motivated criminals. Documented cases have found these 'entrepreneurs of influence' turning disinformation and fake news into an instrument of hybrid warfare (Laruelle et al., 2021). Scholarship on DaaS is sparse; adjacent work examines profit incentives in advertising technology, cyber-enabled fraud and market infrastructures for crime as a service (e.g. Braun et al., 2019; Loukas et al., 2020; McGuire et al., 2013; Collier et al., 2021; Brangetto et al., 2016; Pijpers et al., 2020). Prior studies also show loose, hybrid online–offline structures rather than single hierarchies (Broadhurst et al., 2014), noting: 'a wide variety of organizational structures … enterprise or profit-oriented activities … require leadership, structure, and specialisation.'

These services range from hiring fake influencers to push hashtags to launching full-spectrum campaigns using stolen data and cloned news sites. DaaS lowers the barrier to entry and makes capabilities once reserved for states available at a lower cost. Vendors on encrypted channels openly market troll farms, bot networks and turnkey fake-news packages alongside malware and access. Automation and, increasingly, AI strengthen scale, speed and persistence across botting, phishing, account takeover and content production (United Nations Office on Drugs and Crime, 2025). Clients include authoritarian regimes and profit-seeking organisations that purchase bespoke influence services (Insikt Group, 2019; Thomas et al., 2023). These actors deploy computational propaganda to destabilise societies and erode trust in institutions, an issue now treated as a European security risk (Arceneaux et al., 2021; Shahbaz, 2018; Oxford Internet Institute, 2020; Bradshaw et al., 2020; Colomina et al., 2021). Convergence between influence operators and organised cybercrime is increasingly visible. The Russian-linked 'Doppelganger' campaign shows how ideology and criminal capability intersect (VIGINUM, 2023; EU DisinfoLab, 2025). Recent unrest illustrates the societal harm being inflicted. During the Dublin riots in November 2023 and the Southport riots in August 2024, influence networks exploited crime events and spread unverified claims about perpetrators' immigrant status, which fuelled anti-immigrant sentiment and violence. Telegram, X (formerly Twitter) and Gab were key dissemination platforms. In Dublin, anonymous Telegram channels coordinated rioting that escalated into looting, assaults on Gardaí and attacks on migrant camps. In Southport, narratives about a 'two-tier justice system' catalysed protests across the United Kingdom and Northern Ireland, with far-right groups coordinating real-time attacks on mosques and asylum centres (Gouliev et al., 2024; Dunne, 2024; Institute of Strategic Dialogue, 2024). Research indicates that many of the relevant channels were run by foreign actors and amplified awareness of the riots (Morley-Davies, 2024; O'Keeffe, 2024; McDermott, 2024). The pattern is platform agnostic across mainstream and alt-tech services, and actors rebuild quickly even after arrests and takedowns, aided by decentralised platforms and weak moderation.

Operationally, campaigns blend ideological aims with profit and draw on a commoditised market. We analysed over 25 Surface Web forums and about 15 Dark Web forums. For operational reasons we do not name venues, and we include only redacted snippets. Listings show marketplaces selling influence capability using illegal bots and tooling that seed, amplify and target content. Dedicated sections advertise hacking tools, and we observe clear expansion into social media manipulation services. Behavioural analysis of traders shows the same actors offering

crimeware and influence tooling in parallel, including bundles that pair stealer logs, remote-access tools, ransomware, rootkits and bulletproof hosting with social media marketing (SMM) panels, account farms, bulk SMS and engagement boosts.

We also examined bot artefacts linked to the 'Doppelganger' campaign, which indicate that cybercrime infrastructure is being reused in inside information operations. This article combines that supply-side evidence with a 'Doppelganger' case study and a quantitative analysis of foreign information manipulation and interference (FIMI) incidents from the Institute of Global Politics. We describe the tactics, techniques and procedures (TTPs), the actors and the infrastructure, and we set out implications for law enforcement ahead of CEPOL 2025.

The 'Doppelganger' campaign

The Doppelganger campaign operationalises the DaaS supply chain described above. EU and US reporting link the activity to Russian entities, and describe an architecture built from disposable front-end domains, a traffic-direction layer and high-fidelity clones of legitimate outlets. First reported in mid 2022, the operators copied recognised media brands and placed pro-Kremlin material into European information spaces; this was then widely copied. Lookalike sites of outlets such as *Bild*, *20 Minutes*, *ANSA*, *The Guardian* and *RBC* appeared. The network registered typosquatted domains, replicated design and typography and published locally targeted headlines. Distribution relied on seeded social accounts and cross-posting across channels. A commercial tracker sat at the centre. Keitaro, an advertising platform, was repurposed to enforce geofencing, ASN (autonomous system number) / IP (Internet Protocol) checks, referrer and user-agent rules and time-of-day scheduling so that users in different locations received different content. Posts were timed to match EU time zones and were automated to maximise the volume of posts. The infrastructure prioritised resilience, and bulletproof hosting shielded key nodes. Domains and nameservers rotated, while multistage redirection concealed origins and only served payload pages to in-scope visitors. The same link could return a clone in one country and benign content elsewhere. Known crawler ranges and common research VPN (virtual private network) end points were filtered or shown decoys. Cloned pages doubled as phishing lures for credential capture. Some delivery chains carried malware. Procurement and payments used cryptocurrency for domains, hosting, traffic purchases and cash-out. The workflow matches call-centre-style fraud operations that use the same proxy infrastructure and labour markets, placing these providers inside the broader cybercrime economy rather than outside it.

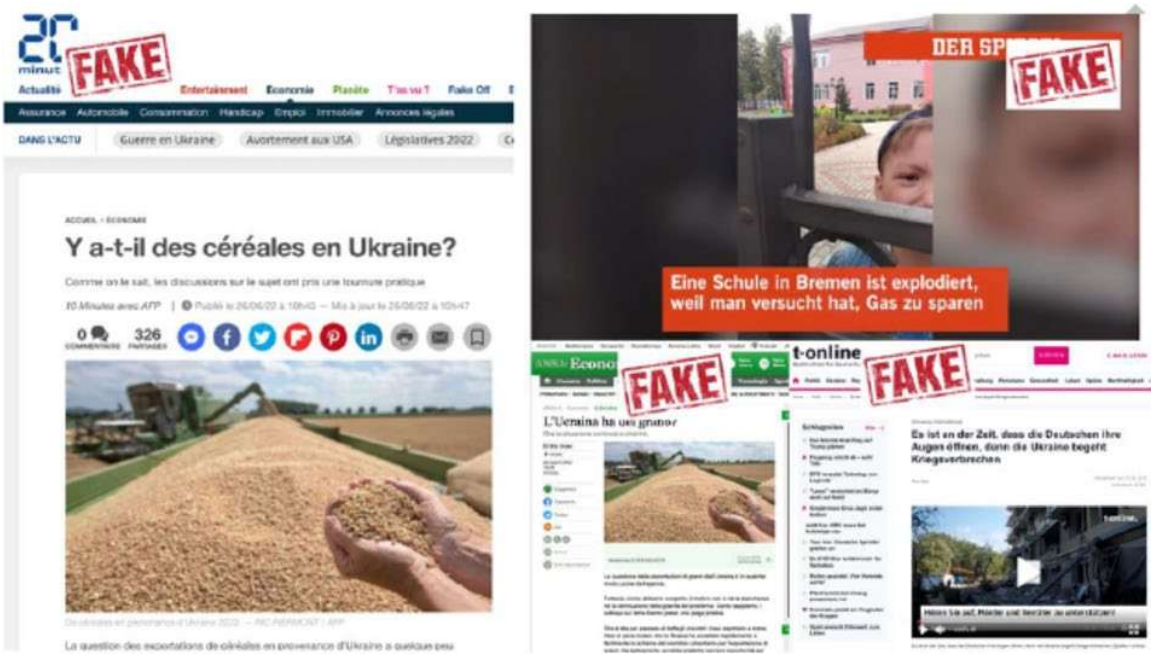

Figure 8.1. Cross-platform delivery in the 'Doppelganger' campaign

Source: EU DisinfoLab.

The core payload sits on cloned news web pages, and traffic is driven by seeded social accounts on mainstream platforms (e.g. Facebook, X (formerly Twitter)). The campaign mixes formats, articles, image overlays, subtitled video and sponsored ads to funnel users back to the clones for narrative uptake and further propagation ([18]). Operators registered many small permutations of media URLs, for example 'washingtonpost.pm'. Content moved between nodes, which reduced the value of simple hash matching and complicated historical crawling. Redirection logic changed frequently, sometimes within a day, which weakened static indicators. Figure 8.2 shows enforcement scaling month-on-month while operator output also grows, signalling takedown resilience and quick rebuild cycles. Open reporting associates' parts of the infrastructure with Russian advanced persist threat (APT) capabilities, notably APT28, indicated support from state units to contractor-style teams operating the influence stack.

([18]) EU DisinfoLab, 'Doppelganger – Media clones serving Russian propaganda', EU DisinfoLab website, https://www.disinfo.eu/doppelganger.

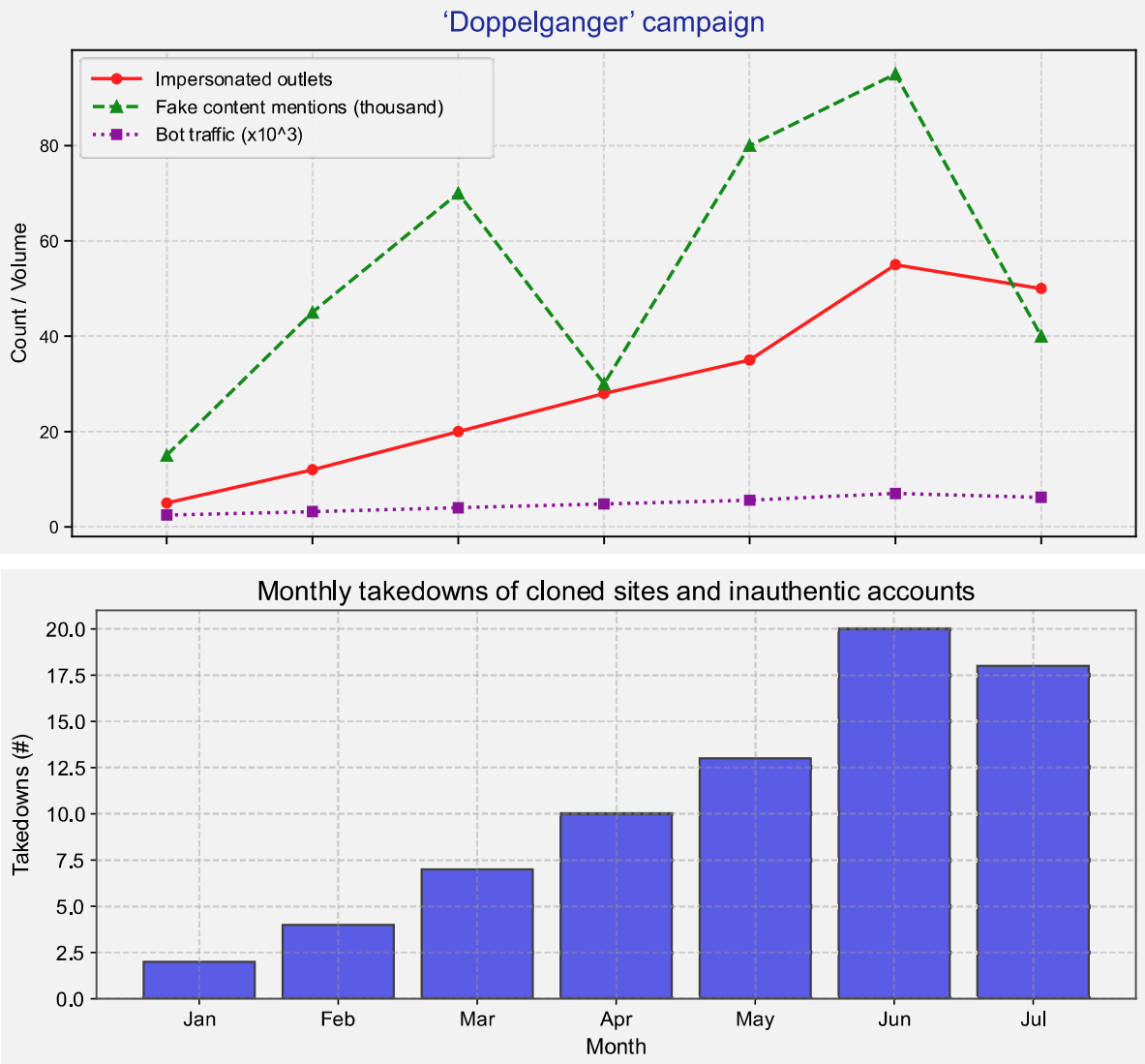

Figure 8.2. Campaign activity versus enforcement, January to July

Source: The author.

The top panel shows growth in impersonated outlets, fake-content mentions (thousands) and bot traffic. The bottom panel shows the monthly takedowns of cloned sites and inauthentic accounts. Outputs rose despite increasing takedowns, with only a modest dip after June, indicating rapid reconstitution and infrastructure churn.

- **Impersonation.** Typosquatted domains mimicking news outlets (e.g. bild.de versus bi1d.de), with cloned design and locally tailored headlines.
- **Distribution.** Seeded social media accounts and cross-posting on multiple platforms to drive traffic to the fake sites.

- **Traffic direction.** Commercial ad-tracking software such as Keitaro was used for geofencing and rule-based delivery that steered users by IP location and matched narratives to local contexts.
- **Automation and timing.** Posting activity aligned with target time zones (e.g. EU daytime) and largely automated to sustain volume.

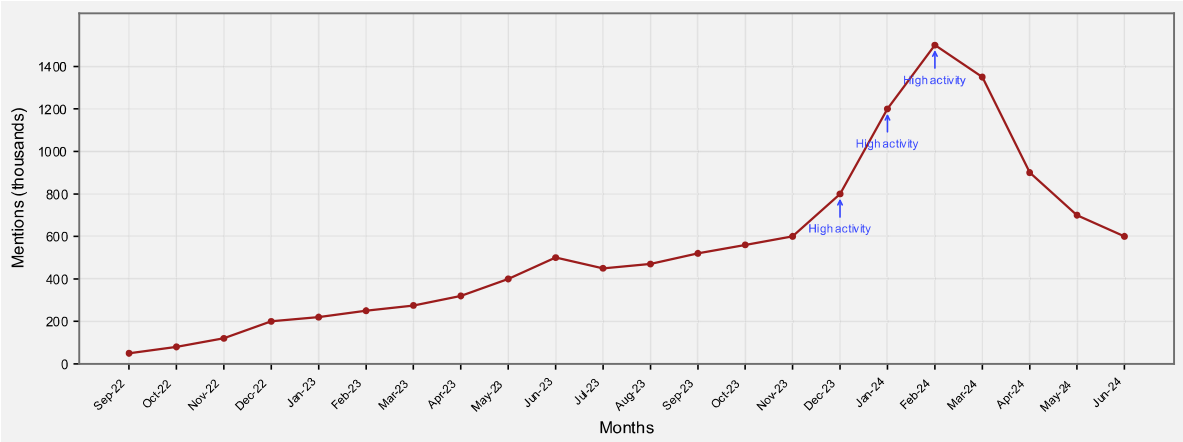

Figure 8.3. Timeline of 'Doppelganger' campaign mentions, September 2022 to June 2024

Mentions climb steadily from late 2022, then spike between December 2023 and March 2024, peaking in February. Activity remained elevated after exposure, suggesting that platform actions did not durably suppress reach and that operators bypassed or rebuilt around removals.

The content strategy tracked Russian geopolitical objectives. During energy price spikes and key political dates, localised stories framed support for Ukraine as costly or unfair and pushed themes aligned with Russian interests. Narrative laundering increased perceived legitimacy: items circulated across multiple clones and then moved through fabricated profiles and community groups, making distribution look organic rather than coordinated. Figure 8.3 highlights post-exposure spikes and sustained volume, consistent with the evasion of platform takedowns.

State reporting attributes the operation to organisations under the Russian presidential administration, including Structura and the Social Design Agency, with direction linked to Sergei Kiriyenko. Evidence cited included domain-registration patterns, technical overlaps across nodes, and internal materials indicating tasking and resourcing. The campaign used AI-assisted content, large-scale cloning and coordinated amplification with automated accounts and fabricated personas. Platform responses were inconsistent. Gaps in domain and hosting policy enabled rapid reconstitution after sanctions and seizures.

Forum-based supply analysis

As part of this research, we analysed over 25 Surface Web forums and 15 Dark Web marketplaces that trade in both cybercrime tools and influence-for-hire services. For operational reasons, we are not naming these platforms, forums and marketplaces. These platforms act as commercial hubs for cybercriminals where influence services have become a routine product category alongside malware, access brokers and credential-stealer logs. Forum sections such as Blackhat and Grayhat include established vendors offering SMMs that provide bulk engagement, content placement

or account management on major social media platforms. Figure 8.4 shows a typical forum hierarchy where influence services appear alongside listings for botnets, keyloggers and operational security support, confirming how manipulation and cybercrime intersect within shared infrastructure.

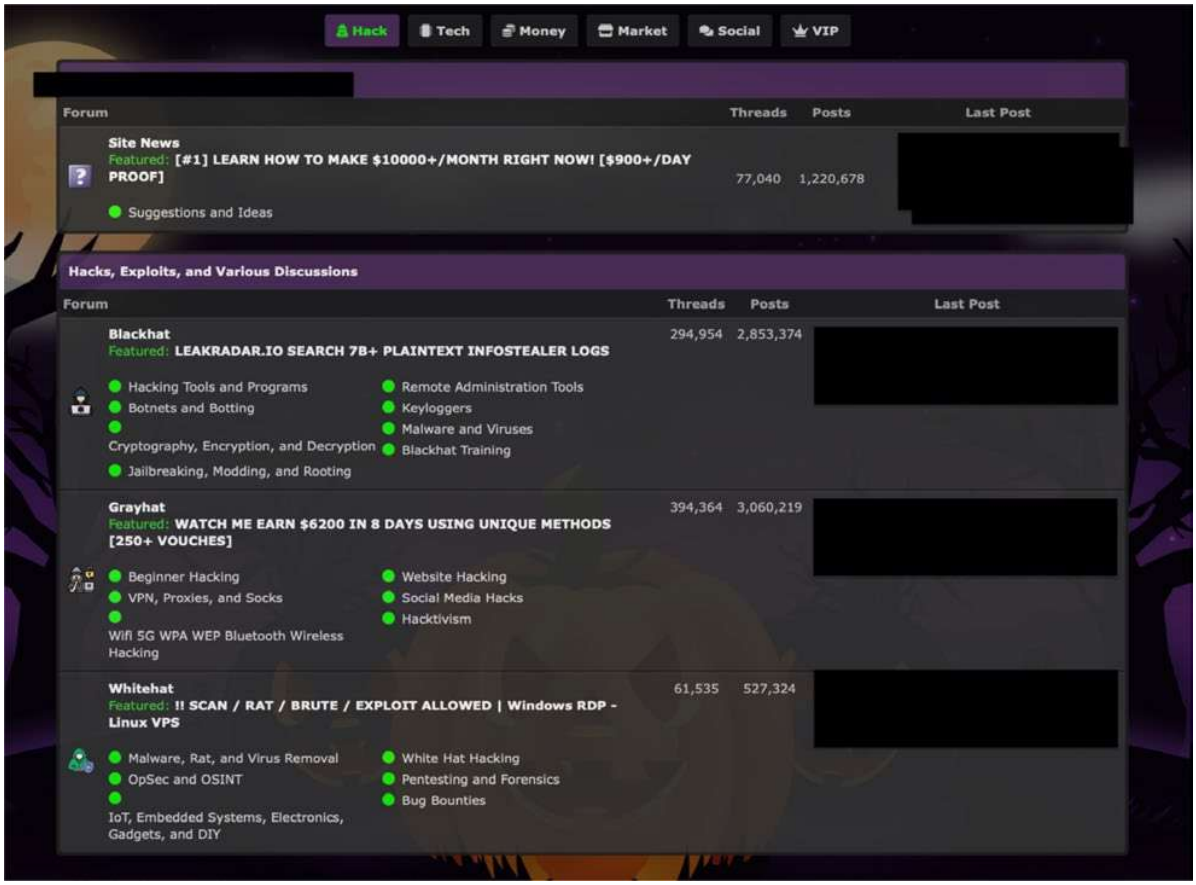

Figure 8.4. Forum index and category structure
Source: The author.

Figure 8.4 presents an index view of a Surface Web forum examined in the investigation. It illustrates how influence-related services are embedded within established cybercrime ecosystems. Sections such as Blackhat, Grayhat and Whitehat host overlapping discussions and vendor threads advertising tools, infrastructure and training. These categories mix traditional cybercrime activities (botnets, keyloggers and remote-access tools) with social media manipulation and 'hacktivism' subforums, showing the convergence of technical exploitation and influence operations under the same market architecture.

Listings across these markets demonstrate a standardised, menu-driven model. Vendors advertise 'verified' or 'aged' accounts, engagement packages and promotion bundles that cover every major platform: Facebook, Instagram, TikTok, Telegram and X (formerly Twitter) (Figures 8.5–8.7). These services include the sale of fake articles, comments, reactions, event promotion, group-member inflation and targeted astroturfing, with optional geographical or demographic filters. Buyers can choose the content type, country, delivery volume and referrer source from drop-down catalogues resembling conventional marketing dashboards. We also obtained access to one of these SMM

tools, confirming the scale of its inventory and its integration with APIs (application programming interfaces) that automate purchases across multiple platforms.

Figure 8.5. Vendor listings offering influence and engagement services
Source: The author.

Active vendor threads advertised SMM panels that automate inauthentic activity across multiple platforms. Each thread represents a commercial offer for engagement metrics such as likes, followers, comments, views or reposts on Facebook, Instagram, YouTube, TikTok, and X (formerly Twitter). Services are presented in a retail format with pricing, bulk discounts, customer reviews and free-trial options. The listings illustrate how this influence manipulation has become a commoditised service, accessible through the same mechanisms as other cybercrime tools.

Figure 8.6. Extended marketplace offers supporting influence operations
Source: The author.

Figure 8.6 shows a continuation of the same forum environment where disinformation-related capabilities coexist with wider cybercrime tools. Alongside SMM and engagement services, vendors advertise bulk SMS gateways with API access, sender-ID spoofing and automated delivery systems. Other listings promote account-banning services, verified profile generation and traffic manipulation through API spoofing or 'no-filter' URL methods. Together, these offers illustrate the breadth of the disinformation ecosystem, where influence amplification, infrastructure abuse and account manipulation are available from the same supply base used for conventional cybercrime.

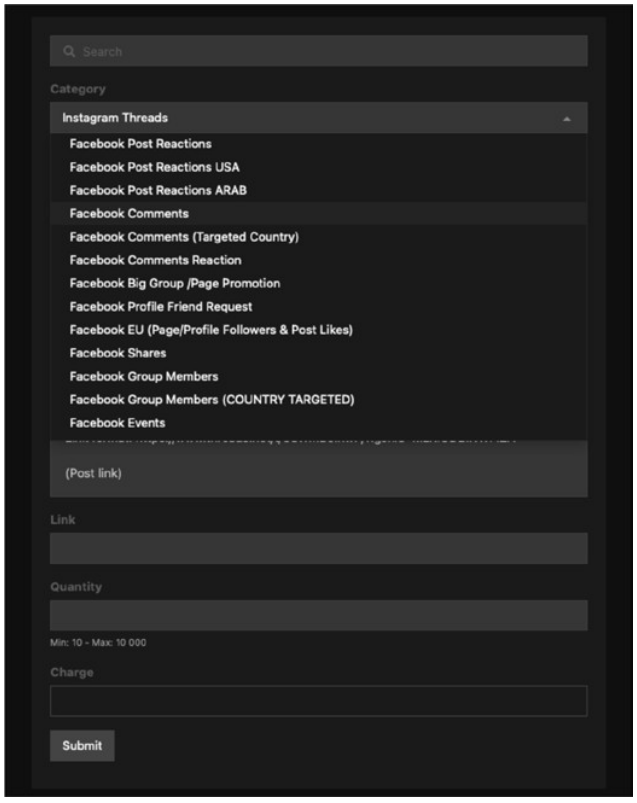

Figure 8.7. Interface of an influence-for-hire automation tool
Source: The author.

Figure 8.7 shows the interface of one of the tools analysed in this study. The platform is purpose-built for automating paid engagement, allowing users to select services, input links and order inauthentic activity at scale. Options include quantity controls, pricing and submission fields, confirming that manipulation services operate through standardised marketing-style dashboards.

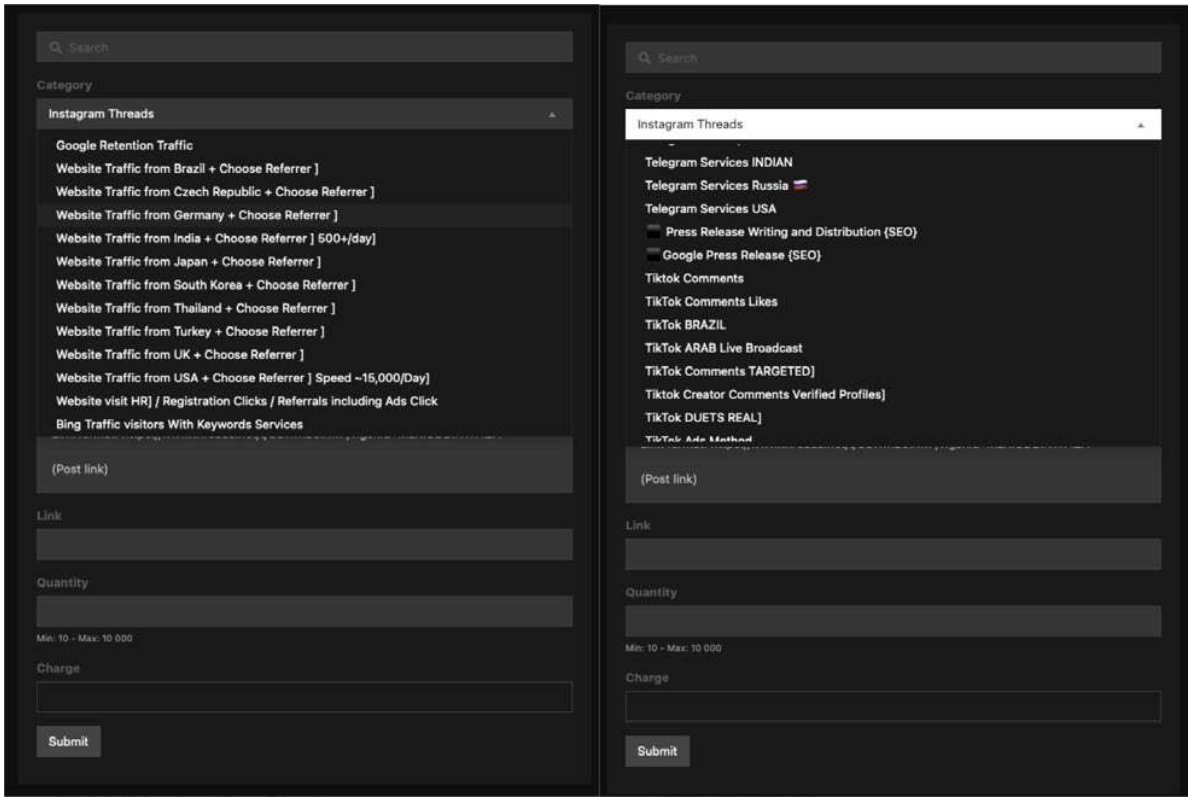

Figure 8.8. Cross-platform service catalogue – Facebook and Meta ecosystem
Source: The author.

NB: Left snippet: this view from the same tool displays Facebook-related categories, offering engagement actions such as post reactions, comments, shares, group-member additions and event promotion. Buyers can specify target countries, languages or audience types, showing how DaaS markets enable precise targeting within mainstream social platforms. Right snippet: this interface section lists traffic and promotion services across Telegram, TikTok, YouTube and regional web domains. It includes press-release distribution, website visits, SEO-based placements and regional targeting options.

The visibility of these services across both Surface Web and Dark Web spaces demonstrates the breadth and normalisation of DaaS. Influence, amplification and visibility can now be purchased through the same retail logic as spam campaigns or credential sales. This commoditised ecosystem forms the operational backbone supporting larger information operations such as the 'Doppelganger' campaign. Having established the micro-level market architecture, the next section moves to a macro-level examination of FIMI incidents.

State-crime convergence in foreign information manipulation and interference

'Doppelganger' showed how a campaign is assembled; the forum review showed where the parts come from. We will now look at the macro level and examine how those market components scale into election-focused FIMI using the Institute of Global Politics election-incident dataset (Fulde-Hardy et al., 2024). Interference concentrates where the payoff is highest, and the calendar is predictable. Presidential contests dominate, followed by general or federal elections; legislative, referendum and municipal contests remain in scope when margins are tight or policy

stakes are visible. This distribution matches a market logic in which clients buy reach and clarity of narrative, and vendors pre-package services for known electoral windows.

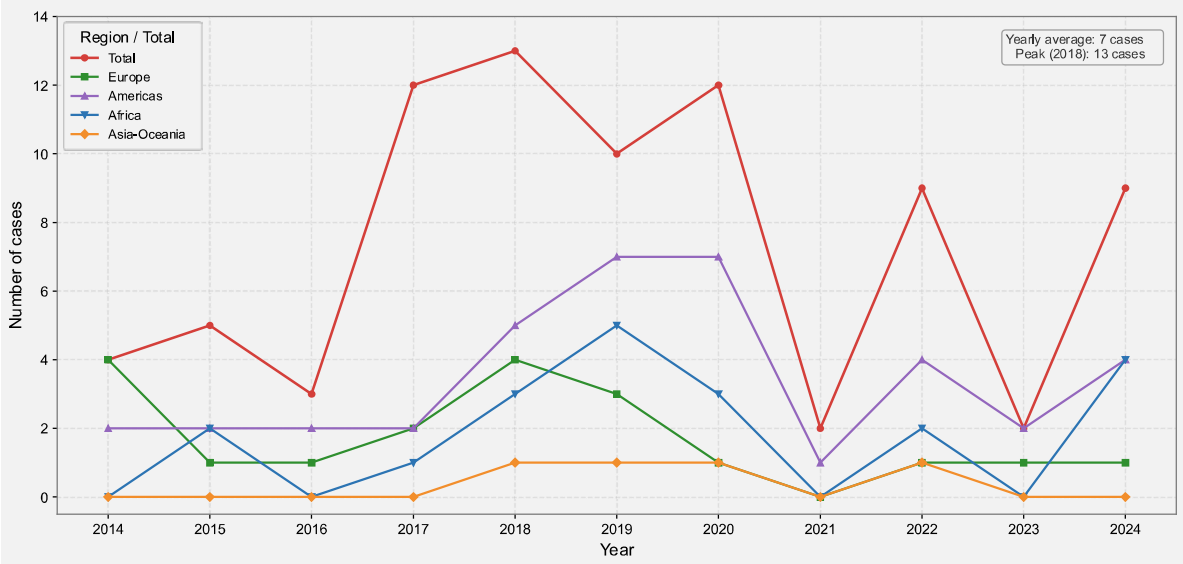

Figure 8.9. Confirmed FIMI election cases, 2014–2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.9 presents the number of confirmed election interference incidents over a 10-year period. The dataset records an average of eight cases per year, with a peak of 13 in 2018. Activity intensifies around major global election cycles, notably in 2018–2020, followed by a brief decline and a renewed rise in 2024. Regional variation shows Europe and the Americas as the most frequent targets, with emerging incidents in Africa and Asia/Oceania. The pattern indicates a cyclical mobilisation of foreign information manipulation around key electoral events rather than a continuous upward trend, suggesting adaptation by both threat actors and platform defenders.

Interference concentrates where the payoff is highest and the calendar is predictable. Presidential contests dominate, followed by general or federal elections; legislative, referendum, and municipal contests remain in scope when margins are tight or policy stakes are visible. This distribution matches a market logic in which clients can buy reach and clarity of narrative, and vendors pre-package services for known electoral windows. Activity comes in waves, and peaks cluster around electoral super-cycles and high-salience crises, followed by adaptation on both attacker and platform sides. The post-2020 dip is better read as a change in tradecraft and reporting than a decline in risk.

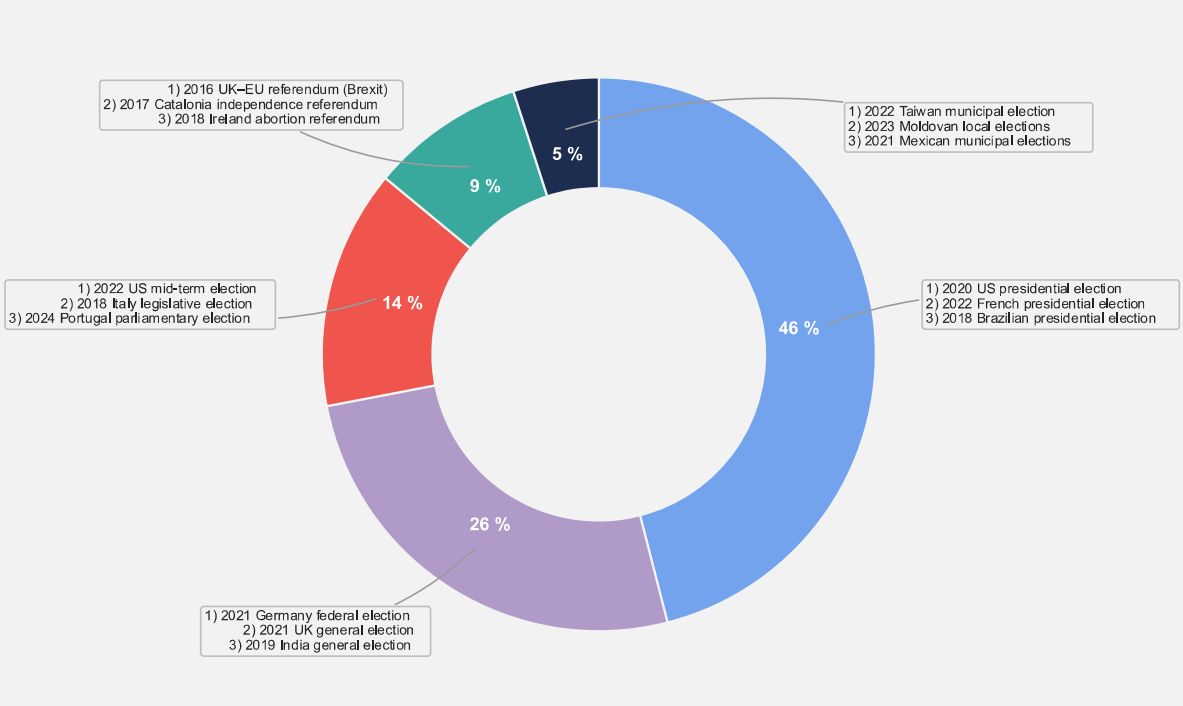

Figure 8.10. Foreign election interference by election type, 2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.10 illustrates the distribution of election types most frequently targeted by foreign interference. Presidential elections represent nearly half of all recorded cases (46 %), reflecting their visibility and strategic importance. General and federal elections account for 26 %, while mid-term and legislative elections make up 14 %. Referendums (9 %) and local or municipal elections (5 %) are also targeted, showing that interference extends beyond national contests to influence political outcomes at multiple levels of governance.

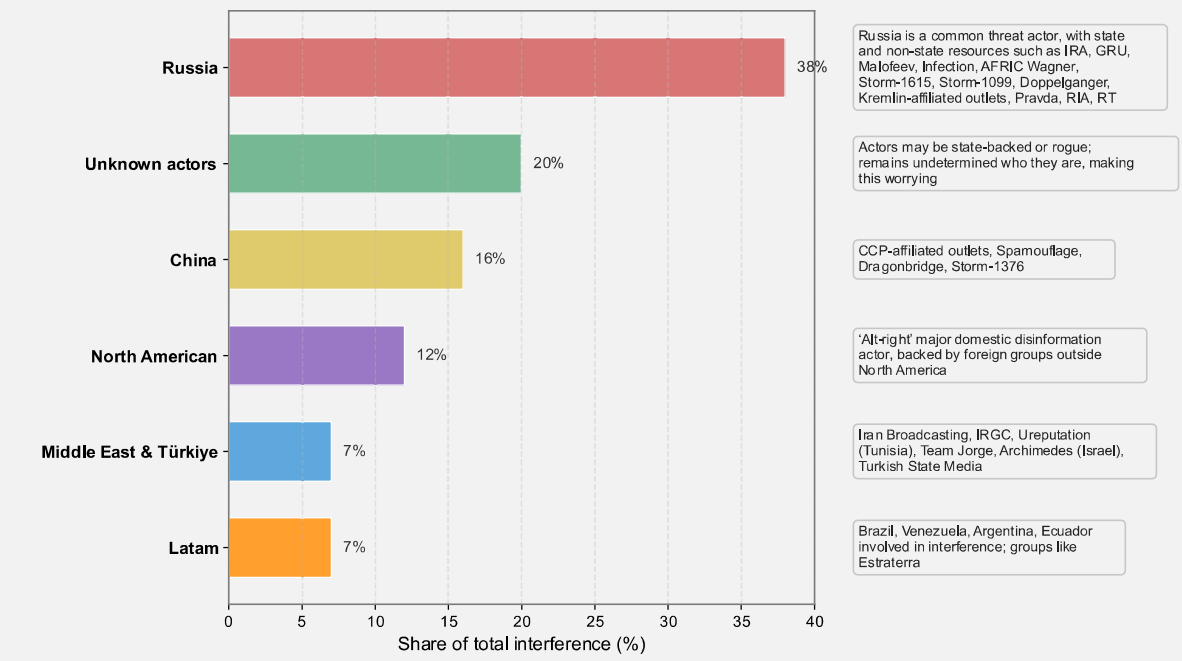

Figure 8.11. Threat actors in foreign election interference, 2024

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.11 presents the principal actor groups identified in documented cases of foreign election interference. Russia accounts for 38 % of attributed incidents, reflecting its established ecosystem of state and proxy entities such as the Internet Research Agency, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation and campaigns like 'Doppelganger'. China follows with 16 %, primarily linked to coordinated networks such as Spamouflage and Dragonbridge. North American and Middle Eastern actors each contribute smaller shares (12 % and 7 %), while Latin American entities account for another 7 %. Notably, 20 % of the cases remain unattributed, indicating a substantial number of operations that likely involve contractors or hybrid actors, further complicating attribution and enforcement. Attribution reflects the same contractor ecosystem seen on forums. Russia accounts for the largest attributed share, followed by China, and there remains a large unknown segment. That unattributed tranche is consistent with cut-outs, intermediaries and blended state–criminal tasking that frustrate clean linkage.

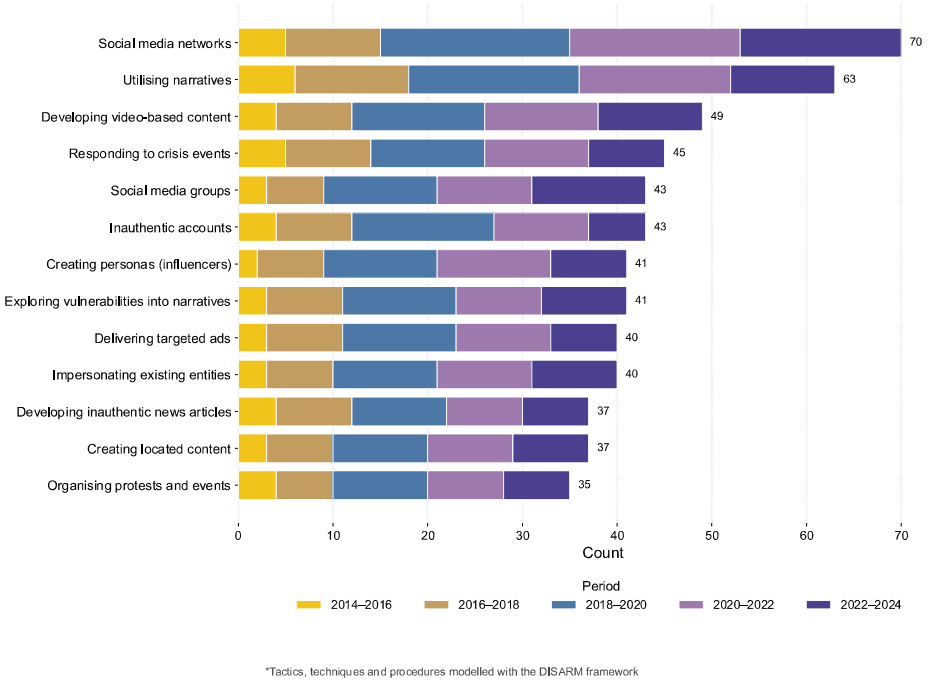

Figure 8.12. Common tactics, techniques and procedures used in foreign information manipulation and interference

Source: The author, using the Institute of Global Politics FIMI dataset from Fulde-Hardy et al., 2024.

Figure 8.12 shows the most frequently observed TTPs across documented FIMI incidents between 2014 and 2024, modelled using the DISARM (disinformation analysis and risk management) framework. The data highlights social media networks and the use of existing narratives as dominant techniques, followed by video-based content, crisis exploitation and the creation of inauthentic accounts. Growth across all categories in recent years (2020–2024) reflects the industrialisation of disinformation tradecraft and its increasing overlap with cybercrime tooling. These methods mirror the DaaS supply market, where services such as persona creation, targeted advertising and social media manipulation are available as packaged capabilities.

The methods line up with what the supply side sells. Social network operations, narrative exploitation, video-led content, inauthentic accounts and personas, targeted advertising and impersonation dominate, with steady growth over time. These behaviours are modular, purchasable and easily reassembled across platforms, which explains their persistence through takedowns and rapid rebuild cycles.

This macro view connects the mechanics of disinformation campaigns to election outcomes: marketised distribution and protection make interference scalable, resilient and timely in relation to democratic events. We next translate these findings into law enforcement tasking and disruption points.

Challenges and countermeasures for law enforcement

The decentralised and borderless nature of these operations present challenges to law enforcement, particularly in attribution and enforcement. Criminal actors exploit jurisdictional complexities, using servers and infrastructure spread across multiple countries, as exemplified by 'Doppelganger' operations. These activities thrive in legal grey zones, complicating prosecution efforts. Moreover, the rapid evolution of adversarial technologies, such as geofencing tools and adversary-in-the-middle (AiTM) kits (Microsoft Threat Intelligence, 2022), often outpaces the development and deployment of countermeasures, leaving law enforcement agencies perpetually on the back foot. International collaboration is critical in addressing these transnational threats, but differing legal frameworks and enforcement priorities among nations impede unified responses. The necessity for cross-border cooperation and knowledge sharing is increasingly recognised, with initiatives such as the VIGILANT (vital intelligence to investigate illegal disinformation) and ATHENA (an exposition on the foreign information manipulation and interference) projects emerging to bolster law enforcement capabilities.

VIGILANT is an EU-funded research project that equips European police authorities with cutting-edge tools to detect and analyse disinformation campaigns. It integrates over 30 forensic and analytical tools into a modular platform and enables law enforcement to identify coordinated networks, fabricated content and tampered multimedia (VIGILANT, 2024). In addition to providing advanced detection capabilities, VIGILANT offers extensive training to police authorities to help enhance their understanding of disinformation's social drivers and psychological impacts. A peer-to-peer network further facilitates the sharing of insights and strategies across jurisdictions, fostering a unified EU response to disinformation campaigns. This is complemented by the ATHENA project, which addresses the broader challenge of protecting democratic processes from FIMI. It combines technical innovation with behavioural and societal analysis to develop novel countermeasures against FIMI (ATHENA, 2024). There are tools such as a disinformation analysis dashboard and a dynamic knowledge graph, which provide actionable insights for governments and law enforcement. Similarly, it offers training and resources in recognising and countering FIMI threats.

Both these projects are promising and well timed by the European Union, as it recognises the need for multidisciplinary strategies, blending technological innovation with social and behavioural insights to address the growing nexus of disinformation and cybercrime.

References

Arceneaux, P. and Harman, M. (2021), 'Social cybersecurity: A policy framework for addressing computational propaganda', *Journal of Information Warfare*, Vol. 20, No 3, pp. 24–43, https://www.jstor.org/stable/27124997.

Brangetto, P. and Veenendaal, M. A. (2016), 'Influence cyber operations: The use of cyberattacks in support of influence operations', in: Pissanidis, N., Rõigas, H. and Veenendaal, M. (eds), *2016 8th International Conference on Cyber Conflict – Cyber power*, NATO CCD COE Publications, Tallinn, https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

Braun, J. A. and Eklund, J. L. (2019), 'Fake news, real money: Ad tech platforms, profit-driven hoaxes, and the business of journalism', *Digital Journalism*, Vol. 7, Issue 1, pp. 1–21, https://doi.org/10.1080/21670811.2018.1556314.

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014), 'Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime', *International Journal of Cyber Criminology*, Vol. 8, Issue 1, pp. 1–20, https://research-management.mq.edu.au/ws/portalfiles/portal/62156293/Publisher%20version%20(open%20access).pdf.

Chavane, C., Amaury-Jacques, G. and Seznec, K. (2024), 'Master of puppets: Uncovering the DoppelGänger pro-Russian influence campaign', Sekoia, 21 May, https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/#h-observables.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A. and Chua, Y. T. (2021), 'Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services', *Policing and Society*, Vol. 32, Issue 1, pp. 103–124, https://doi.org/10.1080/10439463.2021.1883608.

Colomina, C., Sánchez Margalef, H. and Youngs, R. (2021), 'The impact of disinformation on democratic processes and human rights in the world', PE 653.635, European Parliament: Directorate-General for External Policies of the Union: Policy Department for External Relations, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

Cybersecurity and Infrastructure Security Agency (2022), *Russian state-sponsored and criminal cyber threats to critical infrastructure*, https://www.cisa.gov/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf.

Dunne, S. A. (2024), 'Too far right? The role of alt-tech and mainstream social media platforms in far-right political violence', UCD Centre for Digital Policy, https://digitalpolicy.ie/too-far-right-the-role-of-alt-tech-and-mainstream-social-media-platforms-in-far-right-political-violence-dr-sarah-anne-dunne/.

European Network Against Crime and Terrorism (2024), 'State of play policy report 01 – Public version – September 2024', https://enact-eu.net/enact-state-of-play-policy-report-2024/.

Fulde-Hardy, M. and François, C. (2024), 'IGP releases new dataset of online foreign information operations targeting elections', Institute of Global Politics, 26 June, https://igp.sipa.columbia.edu/news/igp-releases-new-dataset-online-foreign-information-operations-targeting-elections.

Ganguli, P. (2024), 'The rise of cybercrime-as-a-service: Implications and countermeasures', *International Journal for Multidisciplinary Research*, Vol. 6, Issue 5, https://doi.org/10.36948/ijfmr.2024.v06i05.27724.

Gouliev, Z. and Dunne, S. A. (2024), 'Policing alt-tech for disinformation? VIGILANTly moving in the right direction', UCD Centre for Digital Policy, https://digitalpolicy.ie/policing-alt-tech-for-disinformation-vigilantly-moving-in-the-right-direction-zaur-gouliev-and-dr-sarah-anne-dunne/.

Insikt Group® (2019), 'The price of influence: Disinformation in the private sector', *Recorded Future*, 30 September, https://www.recordedfuture.com/research/disinformation-service-campaigns.

Institute of Strategic Dialogue (2024), 'ISD submission on the Irish state's response to disinformation and digital/media literacy', https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_tourism_culture_arts_sport_and_media/submissions/2024/2024-11-06_submission-institute-for-strategic-dialogue_en.pdf.

Laruelle, M. and Limonier, K. (2021), 'Beyond "hybrid warfare": A digital exploration of Russia's entrepreneurs of influence, *Post-Soviet Affairs*, Vol. 37, Issue 4, pp. 318–335, https://doi.org/10.1080/1060586X.2021.1936409.

Loukas, G., Patrikakis, C. Z. and Wilbanks, L. R. (2020), 'Digital deception: Cyber fraud and online misinformation', *IT Professional*, Vol. 22, Issue 2, pp. 19–20, https://doi.org/10.1109/MITP.2020.2980090.

Marvi, A., Chew, S. and Boonyakarn, P. (2024), 'Chinese espionage group UNC3886 found exploiting CVE-2023-34048 since late 2021', Mandiant, https://cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/.

McDermott, S. (2024), 'The disinfluencers: How over 150 anonymous "Irish" accounts are swamping X with extreme views', *The Journal*, https://www.factchecking.ie/articles/the-disinfluencers-how-over-150-anonymous-irish-accounts-are-swamping-x-with-extreme-views.

McGuire, M. and Dowling, S. (2013), 'Chapter 2: Cyber-enabled crimes – fraud and theft', *Cyber Crime: A review of the evidence – Research report 75*, Home Office, https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf.

Menlo Security (2024), 'Highly evasive and adaptive threats (HEAT)', Menlo Security website, https://www.menlosecurity.com/what-is/highly-evasive-adaptive-threats-heat.

Microsoft Threat Intelligence (2022), 'From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud', 12 July, https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/.

Microsoft Threat Intelligence (2023), 'Analysis of Storm-0558 techniques for unauthorized email access', 14 July, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/.

Milanovic, M. and Schmitt, M. N. (2020), 'Cyber attacks and cyber (mis)information operations during a pandemic', *Journal of National Security Law and Policy*, Vol. 11, No 1, pp. 247–284, https://centaur.reading.ac.uk/93850/.

Müller, M. (2024), *Looking Doppelganger: An analysis of evolving state-sponsored disinformation tactics*, University of Twente, https://purl.utwente.nl/essays/102708.

Morley-Davies, J. (2024), 'How did foreign actors exploit the recent riots in the UK?', Royal United Services Institute, 28 August 2024, https://www.rusi.org/explore-our-research/publications/commentary/how-did-foreign-actors-exploit-recent-riots-uk.

National Crime Agency (2024), *National Strategic Assessment 2024: Cross-cutting threat enablers*.

National Cyber Security Centre (2023), 'Experts reveal latest insights into world of cyber criminals', 11 September, https://www.ncsc.gov.uk/news/experts-reveal-insights-cyber-crime-ecosystem.

Newman, H. (2022), *Foreign Information Manipulation and Interference Defence Standards: Test for rapid adoption of the common language and framework 'Disarm'*, European Centre of Excellence for Countering Hybrid Threats and NATO Strategic Communications Centre of Excellence, https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf.

O'Keeffe, C. (2024), 'Foreign actors are influencing more extreme protests on the domestic scene', *Irish Examiner*, 6 May, https://www.irishexaminer.com/news/spotlight/arid-41387437.html.

Oxford Internet Institute (2020), 'Computational propaganda: Investigating the impact of algorithms and bots on political discourse in Europe', European Commission website, https://doi.org/10.3030/648311.

Oxford Internet Institute (2021), 'Social media manipulation by political actors an industrial scale problem', University of Oxford website, 13 January, https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report.

Pijpers, P. B. M. J. and Ducheine, P. A. L. (2020), 'Influence operations in cyberspace: How they really work', University of Amsterdam: Amsterdam Center for International Law, https://doi.org/10.2139/ssrn.3698642.

Athena (2024), 'An exposition on the foreign information manipulation and interference', European Commission website, https://doi.org/10.3030/101132686.

Reddick, J. (2024), 'Change Healthcare confirms BlackCat/ALPHV behind ransomware attack', *The Record from Recorded Future News*, 29 February, https://therecord.media/change-healthcare-ransomware-attack-blackcat-alphv.

Shahbaz, A. (2018), Freedom on the Net 2018 – The rise of digital authoritarianism, Freedom House Washington, DC, https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf.

Thomas, E. and Reyes, K. D. (2023), 'Commercial disinformation', Institute of Strategic Dialogue, https://www.isdglobal.org/isd-explainer/commercial-disinformation/.

United Nations Office on Drugs and Crime (2025), 'Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia', Cybercrime Technical Brief Series, Regional Office for Southeast Asia and the Pacific, Bangkok https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf.

United States Department of Justice (2024), 'Justice department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere', Office of Public Affairs, 4 September, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

Vigilant (2024), 'Vital intelligence to investigate illegal disinformation', Vigilant project website, https://www.vigilantproject.eu/.

Viginum (2023), 'RRN: A complex and persistent information manipulation campaign – Technical report', 19 July, https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf.

Wahlstrom, A., Mainor, D. and Kapellmann Zafra, D. (2024), 'Life after death? IO campaigns linked to notorious Russian businessman Prigozhin persist after his political downfall and death', Mandiant, 28 March, https://cloud.google.com/blog/topics/threat-intelligence/io-campaigns-russian-prigozhin-persist.