

Global Disinformation and Hybrid Influence Operations

State actors and allied networks have mounted persistent propaganda campaigns using troll farms, fake news outlets and botnets. For example, **Russian** disinformation efforts include the Internet Research Agency (IRA) and affiliated media (“Sputnik”, “RT”) pushing pro-Kremlin narratives and election lies. Graphika found that Russian-linked accounts posing as U.S. activists (the “IRA CopyPasta” campaign) spread polarized content on Facebook/Instagram ahead of U.S. elections ¹. **Chinese** influence operations also span platforms: units like the United Front Work Department and state media employ coopted diaspora networks and social platforms (WeChat, TikTok) to censor critics and amplify CCP talking points. Graphika’s *Spamouflage* reports describe Chinese-linked accounts on X and TikTok posing as U.S. citizens to push divisive social-issue posts (“#Americans”) ². Likewise, Chinese state media (CGTN, Xinhua) and bots amplify pro-Beijing narratives globally. **Iranian** campaigns are led by the IRGC and Basij “cyber volunteer” units, which run fake social accounts and pages to support the regime. Graphika documented a 2021 network (mostly on Instagram) of ~300 Iranian inauthentic accounts targeting domestic and overseas audiences, often praising the regime and attacking dissidents ³ ⁴. Other state-aligned disinfo comes from countries like Turkey, Venezuela, or non-state proxies (e.g. extremist media).

Coordinated Inauthentic Behavior & Botnets

Platforms regularly remove *coordinated inauthentic behavior* (CIB) networks. Meta transparency reports and research show dozens of takedowns. For instance, Meta disrupted a Russia-linked network targeting Moldova (Transnistria) with dozens of fake **pages/groups** posing as local news brands (even using AI-generated profile photos) to push pro-Russian, anti-EU narratives ⁵ ⁶. These campaigns typically employ *botnets* and automated scripts. DFRLab found a “Dracula’s Botnet” of Twitter accounts posting only Bram Stoker quotes – in reality a Chinese-linked bot cluster amplifying spam—illustrated by one such account screenshot ⁷. *Example: A Twitter profile from Graphika’s “Dracula’s Botnet”, one of many fake accounts posting generic quotes to camouflage coordinated activity* ⁷.

Across **Facebook/Instagram, Twitter/X, Telegram, TikTok** and **YouTube**, inauthentic armies repost and meme-mash narratives. DFRLab showed how thousands of Telegram accounts posted identical anti-Ukrainian comments to demoralize Ukraine ⁸. Another DFRLab analysis uncovered 39 coordinated **Telegram channels** (named for Moldovan regions) run by bots, using synchronized greetings and repeated messages (with identical translation errors) to feign local discourse – a pro-Russian operation tied to exiled politician Ilan Shor ⁹ ¹⁰. On X, Chinese-operated crypto-bot networks have reposted deepfake videos of “election fraud” (with fake FBI logos) in the 2024 U.S. vote, mimicking Russia’s “Operation Overload” style ¹¹ ¹². In each case, tiny bursts of repeated content (e.g. memes or slogans) are amplified by networks of bots or compromised accounts to push false narratives.

- **Mapping Ecosystems:** Disinformation researchers often visualize these operations as network graphs. For example, Graphika’s investigations reveal clusters of hundreds of accounts connected by shared URLs and posts; DFRLab and others use tools (like *Osavul*) to cluster similar comments or

forwarders. Although private networks cannot be directly shown here, examples include the *Dracula's Botnet* clusters and Telegram channel hierarchies noted above. These maps highlight how fringe forums and social media feeds feed into each other. Narrative laundering often occurs as a false story travels from a fringe website, through coordinated booster accounts, into broader social media, then into mainstream news headlines ¹³.

Disinformation-for-Hire

A lucrative black market of “influence-as-a-service” has emerged. Private **PR firms and mercenary groups** sell covert influence: they create fake news sites, stage viral ads, or hack opponents for clients. Graphika's *Lights, Camera, Coordinated Action!* report exposed Pakistan's AlphaPro, a marketing agency behind 40 Facebook profiles and 25 Pages masquerading as independent media. Those pages produced video “news” segments (with paid actors) pushing praise of Pakistan's military and attacks on India ¹⁴ ¹⁵. *Graphika's cover image for the AlphaPro/“Lights, Camera” takedown: an example of paid media used to covertly advance political agendas* ¹⁴ ¹⁵. OCCRP undercover journalism similarly uncovered a secretive Israeli group (“Team Jorge”) that pitched “disinformation campaigns, false intelligence, hacks and blackmail” to clients worldwide ¹⁶. This group claimed success in dozens of elections and offered services from network hacking to AI-generated smear videos ¹⁷. Other players include reputation-management firms (e.g. Spain's Eliminalia) and freelance “trolls for hire” who create sockpuppet armies on demand. In essence, many marketing or cyber-security companies now serve as covert influence vendors, blurring lines between state and private operations.

Thematic Disinformation Domains

Disinformation networks often coalesce around specific themes. **Anti-vaccine** narratives have been a focus since COVID-19. Graphika tracked a pan-European anti-vax movement (“V_V” in Italy/France) whose activists and fake accounts harassed doctors and downvoted pro-vaccine content ¹⁸ ¹⁹. This loose movement combined old conspiracies with new “health freedom” tropes, even defacing hospitals and disrupting vaccination clinics ¹⁹. **Climate denial** is similarly amplified online: Graphika found a sprawling Spanish-language network (Latin America & Spain) that echoes English-language hoax narratives. The dominant accounts were broad right-wing influencers who translated anti-climate content and wove it into other conspiracies (e.g. globalist elites) ²⁰ ²¹. In the U.S. and Europe, disinfo gangs also exploit **immigration** and **nationalism**: digital campaigns use racist or anti-immigrant memes and false “immigrant crime” stories to stoke fear. For instance, policy experts note many operations deploy **racist, xenophobic or anti-Muslim** themes to mobilize supporters ²². (Disinformation targeting LGBTQ+ communities follows a similar pattern, casting equality movements as “extremist” to troll audiences.)

Around elections, **vote-fraud** and **foreign interference** narratives proliferate. In the 2024 U.S. election, both Russian and Chinese campaigns were spotted: Graphika observed Chinese-controlled “Spamouflage” accounts pushing voter-disenfranchisement stories ², and DFRLab documented Chinese-run bots amplifying Russian-style “Operation Overload” deepfakes about rigged ballots ¹¹. Elsewhere, Ukraine's invasion has produced a torrent of **war propaganda**: Russian-backed media and trolls frequently push anti-Western narratives, nuclear scare memes, and “biolab” conspiracies, while Ukraine-supported online communities counter with their own memes. (DFRLab's recent reports show malicious actors in comments sections spreading anti-Zelensky slurs and false claims to erode morale ⁸.)

Hybrid Warfare Techniques

Modern influence ops are multi-modal. They marry cyberattacks, engineered leaks, AI-forged media and troll networks. For example, disinfo groups may conduct **hacks and doxings** to create newsworthy “leaks” (e.g. stolen documents), then spread those via botnets and friendly accounts. The Israeli “Team Jorge” explicitly offered forged intelligence and blackmail to manipulate elections ¹⁷. At the same time, **deepfakes and synthetic media** are rising. A Bellingcat investigation showed a high-quality AI-manipulated video (inserting false speech into a press conference) that fooled major media outlets in India ²³. *Example: A deepfake of a Pakistani general at a podium (created by swapping the audio of an old speech) was shared hundreds of thousands of times before being debunked* ²³. Intelligence reports now warn of AI-driven impersonation (e.g. voice-cloned calls to officials) as state-level cyber weapons ²⁴. These synthetic assaults are often **laundered** through social media “amplifiers”: a fringe post or bot-generated video gains initial traction, then gets picked up by influencers or news sites, giving fringe lies an aura of legitimacy ¹³.

Actor Profiles

- **Russia (State):** GRU military intelligence, IRA (troll farm), FSB cyber teams, state media (RT, Sputnik), and political foundations (e.g. Rossotrudnichestvo). They push pro-Kremlin and anti-Western narratives in Slavic, Middle Eastern and Western audiences.
- **China (State):** CCP organs (United Front Work Dept, Cyberspace Administration, People's Liberation Army units) coordinate online influence, often via Uyghur/overseas Chinese networks. State media (Xinhua, CCTV) produce propaganda in multiple languages. Chinese firms (e.g. ByteDance) also come under scrutiny for foreign propaganda.
- **Iran (State):** IRGC/“Basij Cyber Army” and Islamic Republic of Iran Broadcasting orchestrate a network of social media pages, Telegram channels and fake news sites. They target domestic opposition (anti-regime activists) and regional audiences with pro-Iranian, anti-Israel/US rhetoric.
- **Others (State/Proxy):** Examples include Turkish Presidency with troll armies supporting Erdoğan, Venezuelan troll networks, or proxy militias like Hezbollah's media arm. Even non-state organized groups (e.g. QAnon) can act as hybrid actors when aligned with a cause.
- **Commercial/Hybrid:** PR and marketing firms (like Pakistan's AlphaPro) that covertly conduct influence ops for clients, *cyber mercenary* groups (e.g. Team Jorge), and underground networks of freelance hackers/trolls. These operate in the gray zone: for-hire but often in sync with state agendas.

Network Maps and Data

Research groups like Graphika, DFRLab and the Stanford Internet Observatory produce detailed network maps of influence operations. These maps typically show clusters of accounts (nodes) linked by shared behavior (e.g. liking the same posts, using identical hashtags or reposting each other). For instance, Graphika visualized the cluster of Facebook Pages managed by the Pakistani AlphaPro campaign ¹⁴, and DFRLab has charted Telegram channel forwarding trees in Moldova ¹⁰. (See, for example, the graph below of accounts and channels involved in a Moldovan influence operation.) These maps reveal the **ecosystem** of disinfo: how botnets, troll pages, legitimate accounts and external sites interconnect across platforms to push a narrative.

Campaign / Network	Key Narrative	Platforms	Tactics / Amplification
Russia: “IRA CopyPasta” (2019)	Polarized U.S. political issues	Facebook, Instagram	Fake U.S. activist personas reposting IRA memes ¹
China: <i>Spamouflage/ #Americans</i>	U.S. social/racial issues, election	X (Twitter), TikTok	Fake U.S. voter profiles cross-posting divisive content ²
Pakistan/AlphaPro (2021)	Pro-Pakistan, pro-military	Facebook, Instagram	Fake media pages with paid actors; covert PR firm links ¹⁴ ¹⁵
Iran/IRGC Network (2021)	Pro-regime, anti-opposition	Facebook, Instagram, Telegram	Coordinated fake outlets; IRGC “cyberspace volunteers” ³ ⁴
Moldova CIB (2024)	Anti-EU, pro-Russia in Moldova	Facebook, Instagram, Telegram, OK.ru	Dozens of fake “news” pages, GAN avatars, cross-posted cartoons ²⁵ ⁶
U.S. Election (2024)	Alleged vote fraud, Biden corruption	X (Twitter)	Botnet amplification of deepfake videos (FBI/CBS-branded) ¹¹ ¹²
COVID Anti-Vax (2021)	COVID conspiracy, “medical Nazism”	Facebook	Coordinated harassment of journalists, down-voting health posts ¹⁸ ¹⁹
Climate Disinfo (2022)	Climate-change denial/hoax	Twitter, YouTube (Spanish)	Translated memes, coordinated sharing by right-wing influencers ²⁰ ²¹

Case Study: Ukraine War Propaganda

Since 2022, the Russia-Ukraine war has spurred intense hybrid campaigns. Russian-affiliated actors spread narratives of Ukrainian aggression or “genocide” while downplaying Russian offenses. DFRLab documented inauthentic networks posting identical anti-Ukrainian comments on Telegram and Facebook to demoralize Ukrainians ⁸. Meanwhile, disinfo about “nuclear threats” or secret biolabs circulated via milbloggers and fringe channels. On the Ukrainian side, allied actors counter with narratives of democratic resistance. The war’s information front illustrates how states integrate media control, cyber tools and troll armies into a full-spectrum strategy.

Case Study: COVID-19 Disinformation

The pandemic saw overlapping conspiracies and cross-border networks. Graphika’s *Viral Vendetta* report (Dec 2021) detailed how Europe’s V_V anti-vax movement coalesced into a guerrilla campaign: activists harassed health workers, coordinated viral hashtags, and even attempted offline disruptions of vaccines ¹⁸ ¹⁹. In the U.S., Russian and Chinese accounts spread false cures and cast doubt on vaccines. Social media CIB takedowns frequently targeted such networks; e.g., Meta removed international accounts linked to anti-

vax propaganda. The COVID case shows how health disinfo can be rapidly amplified by global networks exploiting social fear.

Case Study: 2024 U.S. Election Influence

In the 2024 U.S. elections, foreign influence attempts resurfaced. DFRLab and Graphika observed Chinese-run accounts pushing U.S. election conspiracy claims (via *Spamouflage/#Americans*) ², and a Chinese-linked botnet on X amplifying Russia's "Operation Overload" election fraud deepfakes on Nov 4–5, 2024 ¹¹. Meta also reported removing operations tied to Russia and China targeting U.S. politics. These campaigns reused familiar narratives (voter fraud, rigged voting machines) and show cross-border coordination: Chinese bots even promoted unrelated pro-CCP content, indicating shared infrastructure ¹². This interference illustrates how adversaries prepare malicious memes and bots well ahead of critical elections, ready to flood the network in the final hours.

Recommendations (Counter-Disinfo)

Effective countermeasures require **policy action, tech tools, and public resilience**. Key recommendations from experts include:

- **Platform Accountability & Transparency:** Enforce rigorous takedowns of CIB campaigns and disclose removal data. Platforms should share (privacy-protected) data on algorithms and ads with researchers, as part of codes of conduct ²⁶. *Regulation* like the EU's Digital Services Act (DSA) can mandate such transparency. Independent oversight (audits, a "Digital Democracy Board") can ensure compliance.
- **Content Detection & Tech Defenses:** Invest in AI and network-science tools for real-time detection of fake accounts, bots and deepfakes. As one analysis warns, disinfo producers now wield generative AI at scale, so automated detection must keep pace ²⁷. For example, specialized deepfake-detection systems (like those described by Reality Defender) are needed to flag AI-impersonation of officials ²⁴. Social platforms should integrate these defenses and rapidly label or remove manipulated media.
- **Support for Independent Media & Fact-Checking:** Build the "signal" by funding non-partisan journalism and civil-society watchdogs. Experts suggest using platform ad tax to subsidize public-interest news, fact-checkers and media literacy programs ²⁸. Media organizations and influencers must be trained to verify stories before syndication, closing the fringe-to-mainstream loophole.
- **Public Education & Resilience:** Governments and NGOs should run public awareness campaigns on disinfo tactics. Teaching citizens to critically evaluate sources (e.g. through digital literacy curricula) makes society less susceptible. Civil-society organizations can also promote positive narratives and community dialogue to counter divisive memes.
- **Global Collaboration:** Share threat intelligence internationally. Democracies should cooperate on identifying cross-border networks (via INTERPOL-like cooperation on cyber/influence threats) and harmonize legal frameworks. Aligning sanctions or penalties for state-sponsored disinformation can raise the cost for aggressors.

Each of these steps — from tougher platform rules to better detection tech and a strong civil society — helps shore up the information ecosystem. As analysts note, disinformation campaigns exploit the gap between sophisticated adversary tools and outdated defenses ²⁴. Only a concerted, multi-disciplinary response can maintain trust in elections, public health, and democratic discourse.

Sources: Research and takedown reports from Graphika ¹ ² ³ ⁵ ⁸ ¹⁴ ¹⁸ ²⁰ ¹¹; Meta transparency blogs ⁶; DFRLab analyses ⁸ ⁹ ¹²; OCCRP/Guardian investigation ¹⁶ ¹⁷; Stanford Internet Observatory, EU DisinfoLab, and policy reports ²⁷ ¹³ ²⁴, among others. (All cited claims above are drawn from these open-source investigations.)

¹ graphika.com

<https://graphika.com/reports/copypasta/>

² graphika.com

<https://graphika.com/reports/the-americans>

³ ⁴ graphika.com

<https://graphika.com/reports/likes-for-lorestan>

⁵ ⁶ ²⁵ Taking Action Against Coordinated Inauthentic Behavior in Moldova

<https://about.fb.com/news/2024/10/taking-action-against-coordinated-inauthentic-behavior-in-moldova/>

⁷ graphika.com

<https://graphika.com/posts/draculas-botnet>

⁸ How inauthentic accounts exploit Telegram comments to spread anti-Ukrainian narratives - DFRLab

<https://dfrlab.org/2024/12/18/inauthentic-telegram-accounts-ukraine/>

⁹ ¹⁰ Telegram network seeks to manipulate Moldova's local political discourse - DFRLab

<https://dfrlab.org/2025/03/06/telegram-network-moldova/>

¹¹ ¹² Investigation: Chinese bot network is amplifying Russian disinformation about the US election - DFRLab

<https://dfrlab.org/2024/11/05/russia-china-us-election-operation-overload/>

¹³ ²² ²⁶ ²⁸ Safeguarding Democracy Against Disinformation | German Marshall Fund of the United States

<https://www.gmfus.org/news/safeguarding-democracy-against-disinformation>

¹⁴ ¹⁵ graphika.com

<https://graphika.com/reports/lights-camera-coordinated-action>

¹⁶ ¹⁷ Hacks, Bots and Blackmail: How Secret Cyber Mercenaries Disrupt Elections | OCCRP

<https://www.occrp.org/en/project/story-killers/hacks-bots-and-blackmail-how-secret-cyber-mercenaries-disrupt-elections>

¹⁸ ¹⁹ graphika.com

<https://graphika.com/reports/viral-vendetta>

²⁰ ²¹ graphika.com

<https://graphika.com/reports/los-eco-ilógicos>

²³ India-Pakistan Conflict: How a Deepfake Video Made it Mainstream - bellingscat

<https://www.bellingcat.com/news/rest-of-world/2025/05/09/india-pakistan-conflict-how-a-deepfake-video-made-it-mainstream/>

²⁴ **AI Deepfake Attack Targets Secretary of State Marco Rubio**

<https://www.realitydefender.com/insights/marco-rubio-ai-voice-clone-deepfake-incident>

²⁷ **Internet Observatory Publications | FSI**

<https://cyber.fsi.stanford.edu/io/publications>