Policy Brief
June 23, 2025

G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region: A Framework for Enhanced Multilateral Coordination and Response

Niklas Swanström and Toby J. Logan

Photo credit: Jixiang Liu / Shutterstock

Russian Foreign Information Manipulation and Interference (FIMI) operations across the Indo-Pacific have evolved into sophisticated, multi-domain campaigns that systematically exploit political tensions and technological innovations. These operations demonstrate added complexity through strategic partnerships with China and North Korea, coordination with regional proxy networks, and alignment with right-wing nationalist movements spanning from Belgium to Japan. This expanded operational architecture enables Moscow to project influence across diverse political and cultural contexts, posing significant challenges to democratic institutions and the rules-based international order that the Group of Seven (G7) seek to preserve. This strategic framework provides G7 leaders with actionable recommendations to enhance collective capabilities for identifying, countering, and bolstering resilience against Russian FIMI operations in the Indo-Pacific. Moreover, it emphasizes the need for coordinated multilateral action and deeper regional partnerships, using approaches that balance security imperatives with democratic values. Key findings include:

- Russian information operations have become more coordinated and intensified significantly, with activities in Europe nearly tripling between 2023 and 2024.[1] There has also been increased activity in the Indo-Pacific region as a result of this operational shift.
- Russian FIMI operations are not typically stand-alone attacks, rather, they are part of a global network of interconnected operations that complement one another. They comprise of numerous techniques that often work in tandem with one another and involve real-world actors.
- Current G7 mechanisms, while foundational, require substantial enhancement to address the scale and sophistication of modern threats, including deeper collaboration with G7 partners.
- Willing partners must firstly recognize a unified typology of harmful content and the main perpetrators of such content. Mapping and defining Russia's various FIMI manifestations will contribute to preventing them in the future.
- Regional partnerships, beyond traditional allies, are essential for effective counter-disinformation efforts. This is especially relevant to the smaller community of Pacific nations who may be less equipped to deter Russia's extensive influence enterprise.
- Technology platforms and private sector engagement remain inconsistent and require structured coordination.

Primary Recommendations

1. The establishment of an Indo-Pacific Information Security Coordination Center to complement the existing G7 RRM; add regional focus rather than duplicating existing security architectures (Quad, AUKUS) to provide real-time FIMI threat assessments and coordinate response protocols.
2. Create a unified typology / taxonomy of harmful content, including standardized classifications to isolate the main perpetrators of disingenuous content; design G7 engagement practices around this to create synchronized enforcement mechanisms that enable a more unified response to threats before they escalate.
3. Develop comprehensive intelligence-sharing frameworks with regional partners and more transparency on FIMI operations developing in real-time.
4. Implement coordinated regulatory approaches while preserving democratic values, such as coordinated national legislation and sanction packages on those conducting FIMI operations. These common legal frameworks must maintain robust protections for free speech and freedom of press.
5. Build long-term societal resilience through education and capacity building. This can involve digital literacy efforts and improved collaboration with social networking sites.

Introduction

Russian Foreign Information Manipulation and Interference (FIMI) operations in the Indo-Pacific have evolved beyond Cold War-era propaganda into multi-domain influence campaigns that exploit technological vulnerabilities and societal fissures. These operations deploy what analysts characterize as a "firehose of falsehood" approach, involving a high velocity of channels, messages, and narratives engineered to fracture epistemic consensus and delegitimize authority.[2] Having demonstrated tactical value in key democratic events, including the 2016 U.S. Presidential Election and the UK Brexit referendum, Moscow's influence apparatus has undergone strategic modernization, incorporating a myriad of expanding FIMI methodologies. The latest trend seems to indicate a deliberate targeting of nations who support Ukraine, in an effort to destabilize their relations and slow the delivery of military aid.[3] For the Indo-Pacific region, their aim is to fragment multilateral frameworks, diminish the value of western partnerships, and widen domestic political cleavages.

Ultimately, targeted influence operations destabilize democratic pillars, resulting in autocratic states that are more likely to collaborate with Russia and consolidate their own power. To reiterate a report from CSIS, disinformation has become a vital component of authoritarian regimes seeking to coerce and influence their opponents in what is often described as the "gray zone", thereby below the threshold of all-out armed conflict.[4]

These objectives represent an evolution from broad-spectrum Soviet-era destabilization toward more precision-targeted strategic influence. This analysis provides G7 policymakers and relevant security professionals with actionable information on Russian FIMI operational patterns, emerging innovations, and the broader vulnerabilities facing the Indo-Pacific region. As G7 nations confront an increasingly assertive China-Russia autocratic partnership, understanding Russia's contribution of influence operations becomes

critical for maintaining democratic unity and preserving the rules-based international order in the world's most economically vital region. More succinctly, this represents an opportunity for China to influence the Indo-Pacific region and for Russia to divert resources away from Ukraine.

Key Operational Characteristics

Russian FIMI operations draw from a sophisticated and varied toolkit; this multi-vector approach integrates both established and emerging influence methodologies. Documented techniques, such as Russia's infamous industrial-scale bot networks designed to flood social media platforms and suppress authentic discourse still remain central to their modus operandi. However, less visible tactics including influencer handling, real-world vandalism, and gig-economy sabotage. Democratic nations must not underestimate both the breadth and sophistication of Russian capabilities, which function as integrated systems rather than isolated instances. This methodology enables Moscow to simultaneously target democratic institutions and social cohesion across G7 nations and the Indo-Pacific, creating cascading vulnerabilities that amplify each attack method.

Moreover, Russia has weaponized information to amplify discord across politically sensitive issues, from internet memes and street art to AI-generated content and fictitious media outlets. The following examples represent a preliminary assessment of Russian operational methodologies rather than a comprehensive inventory. These operational characteristics demonstrate the nuanced nature of modern FIMI campaigns—which frequently operate below the threshold of public awareness. As intelligence collection and analytical capabilities improve, a clearer picture emerges. The methodologies outlined in the boxes are categorized thematically to illustrate both the diversity of Russian influence and their synergistic implementation for improved strategic effect.

Covert Influence Operations

False Flag Mobilization

- Creation of fictional or controlled political groups spanning ideological extremes, designed to stoke conflict, polarize, and undermine democratic participation. Often used in tandem with bots to amplify contentious topics and promote conspiracy theories.[5]

Financial Incentivization of Online "Influencers"

- Direct or indirect payment—often through cryptocurrencies—to online influencers, politicians, and activists to push Kremlin-aligned narratives or sow domestic division.[6]

Proxy Sabotage via the Gig Economy

- Employment of local actors to conduct vandalism, disinformation, or infrastructure disruption. Actors are typically paid via anonymous digital currencies.[7]

Academic and Think Tank Infiltration

- Covert funding of academic positions, policy papers, or conferences to subtly steer elite discourse in favor of Russian geopolitical interests.[8]

Cultural and Religious Exploitation

- Manipulation of ethnic, religious, or linguistic tensions to inflame divisions: particularly potent in multi-ethnic states vulnerable to identity-based unrest.[9]

Cyber Information Operations and Criminal-State Integration

Hack-and-Leak Operations

- Cyber-attacks aimed at extracting and strategically releasing sensitive communications (e.g., political emails) to shape public discourse and ultimately election outcomes.[10]

Web Spoofing and Defacement

- Hijacking or mimicking legitimate sites to distribute false information while leveraging the target's brand authority and user trust.[11]

Data Pollution and LLM Corruption

- Introduction of false or manipulated data into trusted systems, databases, or information repositories to erode decision-making reliability and institutional credibility.[12]

Integration of Organized Crime

- Collaboration with transnational criminal entities for a range of malign activities including cyber-attacks, human trafficking, money laundering, and political violence. These actors provide plausible deniability and extend operational reach.[13]

Illicit Financing Channels

- Use of criminal networks and 'dark money' to anonymously finance information operations globally, particularly where transparency regulations are weak or absent.[14]

Digital Manipulation and Content Operations

Disinformation: Information Flooding and Manipulation

- The saturation of information environments and platforms with contradictory, false, or misleading content to overwhelm users and diminish trust in authoritative sources. Often targets democratic engagement via disillusionment and fatigue.[15]

Amplified Traffic on Social Media Networks

- Large-scale use of bots and online trolls to artificially inflate online engagement, shape trending topics, and simulate grassroots movements (also termed "astroturfing"). These networks frequently adapt messaging in real-time using ML algorithms.[16]

Artificial Media (Deepfakes)

- AI-generated audio-visual mimicries of political actors are deployed to distort authentic discourse, distract from real-world events, and erode truth standards, ultimately creating plausible deniability for genuine scandals.[17]

State-Aligned Media Outlets

- Utilization of pseudo-independent outlets (e.g., 'Pravda', 'RT', and 'Sputnik') to frame Kremlin narratives as legitimate journalism, maintaining editorial deniability while reaching global audiences and exploiting freedom of press rights.[18]

Doppelgänger Campaigns

- Creation of cloned websites mimicking reputable media outlets (e.g., *Le Monde*, *The Guardian*) and law enforcement to distribute falsified reports and discredit genuine journalism.[19]

Search Engine Optimization (SEO) Manipulation

- Engineered content saturation designed to push misinformation into top search results for trending or divisive topics, exploiting search algorithms.[20]

Information Laundering

- Repackaging disingenuous content through a series of proxy outlets and re-publication cycles to obscure its origin and increase perceived legitimacy.[21]

Psychological Operations and Intimidation

Fear Conditioning via Graphic Content

- The use of extreme violence in digital form (e.g., filmed executions, torture) to foster psychological submission and project deterrence in unstable regions, as seen in CAR, Ukraine, and Syria.[22]

Dual-Track Messaging

- Contrast overtly benevolent media campaigns (e.g., security / development / humanitarian support) with threats and terroristic messaging to confuse and control populations. Notably deployed in CAR as a means of intimidation in fear of collective retaliation against civilians.[23]

Kompromat Operations

- Harvesting and leaking compromising materials on foreign political or civil actors to ensure compliance or eliminate resistance through reputational damage.[24]

Recent Russian FIMI Operations: Scale and Sophistication

Russian information operations have demonstrated unprecedented growth and intricacy, with the number of attacks in Europe nearly tripling between 2023 and 2024, likely as a result of Russia's full-scale invasion of Ukraine in February 2022.[25] Similar patterns are emerging in the Indo-Pacific, where operations target multiple audiences simultaneously across diverse linguistic, cultural, and political contexts. The Russian state conduct FIMI in coordination with Kremlin-affiliated actors. These operations are typically carried out through Russia's security services, their diplomatic networks, and private corporations; they are the product of a carefully engineered system.

Since 2020, Russian-attributed cyber influence has been discovered in 85 countries spanning a total of six continents and 16 regions.[26] The following examples are merely four of over seventy-seven recent international information operations identified by the French General Secretariat for Defense and National Security (VIGINUM).[27]

The "Doppelgänger" Campaign

The "Doppelgänger" Campaign is a series of Russian information operations, presumed to have originated in 2022, utilizing a mixed-method approach involving a selection of the operational characteristics mentioned earlier. Each operation under this campaign is an attempt to destabilize G7 members and their partners, including those in the Indo-Pacific region. Orchestrated by Russian companies Struktura and Social Design Agency (SDA), the campaign has primarily involved the creation of convincing replica websites of legitimate news sources and social media accounts across multiple languages, including Thai, Vietnamese, Indonesian, Tagalog, and Te Reo Māori versions of respected regional publications.[28] These fake sites publish articles that appear authentic while embedding disinformation designed to undermine confidence in democratic institutions and Western partnerships, especially those in support of Ukraine.

Operation "Matriochka"

Operation "Matriochka" (Russian Doll), was coined by Russian activists on 'X' (Twitter) and the broader open-source intelligence (OSINT) community. These activists discovered a series of interlinked content focusing on undermining the nations providing support to Ukraine, to destabilize its sovereignty and to sow divisions

among its allies. Since at least September 2023, a multi-faceted online information operation originating from Russia has targeted over 60 countries worldwide, including Japan, Australia, and the Philippines, which the report suggests utilized a pre-determined list.[29] The operation was reportedly conducted in two stages: A first group of accounts, referred to as "seeders", posted fake content on the platform, while a second group of accounts, known as "quoters", then shared a seeder's post in response to posts by authentic media outlets, public figures, and fact-checkers. Much of this content sought to deepen societal divides within democratic countries, exploiting sensitive topics like aid to Ukraine and Gaza.

Operation Overload (Storm-1099)

Operation Overload is a continuation of the "Matriochka" Operation. Specifically, it targeted journalists and media organizations. Their primary objective was to target fact-checkers, newsrooms, and researchers across the globe with the aim of depleting their resources and exploiting credible information environments to disseminate the Kremlin's political agenda. In Australia, the operation has thus far targeted fifteen local organizations, including 'AAP', 'the ABC', 'The Conversation', and 'The Daily Aus'.[30] Globally, Operation Overload targeted some 800 fact checking organizations and newsrooms in 60 countries, sending fake content through tweets and over 71,000 emails, with the intent to overburden their capacity and inundate their ability to discern accurate sources.[31]

Operation Storm-1099 and Storm-1679

Operation Storm-1099 and Storm-1679 were both discovered by Microsoft's Threat Analysis Center (MTAC). This operation used a combination of established techniques and AI, though previous operations are also thought to have employed AI to fabricate and distribute content on a larger scale. Beginning in the summer of 2023, various Telegram feeds began circulating pro-Kremlin content (beginning with AI-engineered videos) which sought to disrupt the 2024 Paris Olympic Games.[32] MTAC reports that the actors involved have a history of heavily targeting the Ukrainian refugee community living in the U.S. and Europe. These specific actors wished to instill a sense of fear and instability around the event. Understanding the considerable soft power behind the Olympic Games, Russia sought to disrupt and defame the democratic participants. A plethora of diverse narratives and media were used, such as manipulating fake terror threat warnings via fraudulent CIA press release videos. While these hybrid tactics are novel, their objective is not a new phenomenon. For the 1984 Olympics in Los Angeles, the Soviet Union sent leaflets to countries, including South Korea, claiming all non-white competitors would be targeted by U.S. extremists. Then, 34 years later during the Winter Olympics, Russia targeted South Korea yet again with a series of cyber-attacks coined "Olympic Destroyer" which disconnected internal servers and generally disrupted services during the event.[33]

The Global "Pravda Network" (Portal Kombat)

The "Pravda Network" is a highly sophisticated and rapidly expanding disinformation system designed to promote pro-Kremlin narratives on an international level. Still ongoing, the infrastructure thus far comprises of more than 87 subdomains, each tailored to specific countries, languages, or public figures.[34] The "Pravda" (or "Truth") network comprises of approximately 200 fabricated news outlets designed to amplify and legitimize content originating from pro-Kremlin social media channels, Russian state agencies, and official governmental sources. This infrastructure serves as a mechanism to evade sanctions, enabling Russian state media to continue operations via distributed networks. The network employs local branding strategies to target specific language groups, focusing predominantly on narratives surrounding the Russian invasion of Ukraine

while exploiting community-specific information environments to enhance its credibility. The Pravda Network has distributed more than 4.3 million articles. Telegram acts as the main platform for circulation, comprising of 75 percent of the network's production. Telegram's third most popular country is Indonesia with roughly 27 million users. Vietnam has circa 12 million users, and Malaysia around 5 million, indicating the number of users potentially exposed to this content.

Stand-Alone FIMI Operations within the Indo-Pacific Region

Examples of Russian FIMI operations across the Indo-Pacific reveals campaigns that extend beyond identifiable operations like Doppelgänger and Pravda. They illustrate how interconnected activities are tailored to exploit nation-specific political and cultural vulnerabilities. These country-specific operations demonstrate Moscow's strategic adaptation to local contexts while maintaining coherence within a broader global enterprise. Rather than operating as isolated incidents, these campaigns represent components of Russia's systematic approach to regional destabilization, where methods are likely tested and calibrated to leverage unique historical grievances, specific linguistic communities, and political fault lines within each nation to erode institutional trust and fragment cooperation.

Japan

Japan's geographic proximity to Russia, combined with unresolved territorial disputes over the Kuril Islands and Tokyo's central role in democratic alliances positions it as a primary target for Russian FIMI operations. Moscow's approach demonstrates sophisticated understanding of Japanese political sensitivities, employing state media outlets (Sputnik, RT) to disseminate historically manipulated narratives that falsely characterize Japan's defense modernization as products of U.S. aggression toward China, North Korea, and Russia. Additionally, high-ranking Russian officials have directly amplified these false narratives through diplomatic channels. In July 2022, Russian Security Council head Nikolai Patrushev fabricated claims regarding Japanese military action in the Kuril Islands, subsequently escalating rhetoric by falsely positioning Japan as a leader in global "Russophobic" movements.[35] Research by Professor Maiko Ichihara supports this trend: the Russian embassy in Japan has been consistently ranked the fourth or fifth most influential 'X' (Twitter) account among Russian government accounts around the world since the invasion of Ukraine began.[36] Russian propaganda regarding Ukraine penetrates Japanese information spaces through networks involving Russian diplomatic channels, domestic conspiracy theorists, and social media accounts with established patterns of promoting Chinese and Russian state content.

South Korea

In addition to targeting South Korea during the Olympics, Russia has responded to actions by Seoul that it deems pro-Western. As a result of South Korea's support of Ukraine, Russia launched a series of cyber-attacks linked to pro-Kremlin hacker groups. Moreover, in November 2023, South Korea's National Intelligence Service identified two PRC public relations firms creating websites that impersonated authentic Korean news outlets to spread propaganda criticizing South Korea's participation in the U.S.-led Summit for Democracy.[37] Additional cyber-attacks have occurred after DPRK's decision to deploy troops to attack Ukraine.

Philippines

In 2018, the journalists behind the Filipino news website Rappler—heavily targeted by Rodrigo Duterte's government administration—connected information operations in the Philippines with Russian disinformation networks operating through "news and current affairs" websites with Russian IP addresses. They were able to

find sources and links between the disinformation network in the Philippines and Russia's infamous Internet Research Agency (IRA) which was responsible for various FIMI attacks, including interference in the 2016 U.S. Presidential Election. In the Philippines, these accounts dispersed pro-Russian content and attempted to influence public opinion. More recently, a 2025 investigation by Cyabra revealed that approximately 33 percent of profiles discussing former President Duterte's arrest were inauthentic. These fake accounts generated over 1,300 posts with 7,000 engagements and a potential reach of 11.8 million views, promoting pro-Duterte narratives and attacking the legitimacy of the International Criminal Court.[38] The campaign extended to the upcoming mid-term elections, with up to 45 percent of election-related discourse driven by fake accounts.[39]

Malaysia

In Malaysia, Russia has sought to expand its influence through more traditional means, predominantly via media partnerships. In 2017, Russia's state-run news agency Sputnik signed a memorandum of understanding (MoU) with Malaysia's official news agency, Bernama, to exchange news content and media/communications training in Russia. This partnership was widely seen by experts as a means to disseminate Russian narratives in Southeast Asia, and to make the broader influence network more resilient and durable.[40] Similar media partnerships exist in several nations within the Indo-Pacific.

Indonesia

Russia has utilized social media and historical narratives to sway public opinion in Indonesia. Similar to the "Doppelgänger" campaign, pro-Russian content on platforms like TikTok and Telegram have been used to blame Ukraine for the continuation of the war, citing its rejection of a peace plan proposed by Defense Minister Prabowo Subianto under former Indonesian President Joko Widodo. President Widodo was the first leader from Asia to visit Ukraine and Russia following the invasion. This narrative capitalizes on anti-Western sentiment and historical grievances spreading among South-East Asia.

Solomon Islands

During the 2024 Solomon Islands elections, Russian outlet Sputnik and Chinese state media Global Times coordinated to spread fabricated claims of a U.S.-sponsored coup against Prime Minister Manasseh Sogavare.[41] Sputnik published an initial false narrative citing an anonymous source (allegedly from the International Foundation for Electoral Systems), which Chinese media then amplified across several news networks. The campaign included unsubstantiated allegations that U.S.-funded supporters of former Malaita premier Daniel Suidani planned to attack government infrastructure with explosives—claims that lack any evidentiary basis. This timing coincided with broader attempts to delegitimize Western engagement in the Pacific, including China-Russia saber rattling from Russia's OKEAN 2024 joint military exercise. Thus, the operation demonstrates significant coordination, combining Russian narrative creation with Chinese amplification methods to target democratic processes among the diverse constellation of Pacific nations.

Augmenting Russian FIMI Operations: A Strategic Partnership with China

Russia's information warfare capabilities are significantly enhanced through deepening cooperation with China, creating what intelligence analysts describe as an "axis of disinformation" that combines Russian operational expertise with Chinese technological capabilities and regional influence.[42] This partnership operates across multiple dimensions, from military coordination that provides cover for information operations to direct media collaboration on

narrative development and dissemination. Joint military exercises, such as the November 2024 joint bomber patrol involving Russian Tu-95 and Chinese H-6 nuclear-capable aircrafts or Russia's OKEAN 2024 exercise, provide cover for power projection and coordinated information operations. The latter collaboration allegedly involved 90,000 troops, 120 aircrafts, and 400 naval assets, although these figures are heavily disputed by British Defense Intelligence (DI).[43] These exercises are typically accompanied by false narratives portraying the exercises as peaceful cooperation while simultaneously distributing false information about Western military "provocations" and exaggerated claims about the defensive nature of Sino-Russian military coordination.

Sino-Russian Security & Intelligence Cooperation

There is a continually expanding mutual trust and security cooperation between Russia and China, propped up by their shared interest in undermining Western influence. This security partnership is especially evident through their clandestine cooperation in drone and satellite technologies.[44] Within the context of Russian FIMI in the Indo-Pacific, the boundary between state espionage and information operations has become increasingly opaque, especially with the added complexity of real-world actors. Experts argue that China and Russia's increasing isolation (such as the removal of diplomats) will lead to less human-orientated intelligence sources (HUMINT) and instead rely on more innovative and aggressive measures to revive lost espionage abilities.[45]

Thus, China is almost certainly borrowing from Russia's expansive FIMI toolkit, using the methods and techniques in the key operational characteristics mentioned above. China has demonstrably adopted and adapted Russia's disinformation playbook, embedding sophisticated influence techniques into its foreign policy apparatus.[46] In May 2024, China and Russia declared their intent to cooperate in several areas to weaken U.S. power.[47]

This collaboration is even apparent within more covert examples, such as the case wherein a Chinese Ministry of State Security officer allegedly recruited a far-right Belgian parliamentarian, for influence and intelligence activities.[48] The recruited official supposedly engaged in election observation missions in Russian-occupied Ukrainian territories, demonstrating potential coordination between Chinese and Russian intelligence. Moreover, recent incidents involving undersea cable damage demonstrate potential Russian Chinese operational coordination. Chinese-flagged vessels departing from Russian ports and ships with assorted Sino-Russo crews have been implicated in activities directly targeting critical power cables and gas infrastructure.[49] This pattern indicates either direct collaboration or complacency in enabling coordinated sabotage operations across Europe and Asia.

Russian and Chinese Media Cooperation

Russia and China share a comprehensive media relationship that typically echo one another. This mutual arrangement is used to disseminate fake narratives that benefit their national interests. Russia has a history of sharing Chinese propaganda, especially with regard to Hong Kong and Taiwan, meanwhile Chinese media sources typically cite or parrot the Kremlin's stance on the war in Ukraine. There are also areas of convergence, where both parties share or recycle the same content, such as the tensions around the U.S. presence in Okinawa, or broader military cooperation between Japan, the U.S., and Australia.[50] The increasing sophistication of China's information operations clearly reflects a pattern of studying Russian strategies and techniques. Meanwhile, their strategic media cooperation is illustrated by a series of cooperation agreements, including MoUs with Voice of Russia and People's

Daily Online in 2013, Russia Today (RT) and People's Daily in 2014, and China's official Xinhua News Agency and RT in 2015.[51] This allows the two nations to circulate mutually beneficial pro-government narratives that increase their perceived legitimacy. While Sino-Russia collaboration in this realm is present within mainstream partnerships, it is equally present among fringe alternative news sources. For instance, content originating from the Russian-registered website SouthFront, which pushed "deep-state" conspiracy theories on the COVID-19 pandemic and the U.S. border-wall, was particularly popular among Japanese media users.[52] Therefore, both mainstream media and their more extreme alternatives have created a fruitful alliance for spreading both pro-China and pro-Russian propaganda.

Technological Integration

Russian operations increasingly leverage artificial intelligence and machine learning to enhance effectiveness and evade detection. Advanced deepfake technology has been deployed to create fabricated video content featuring regional political leaders making inflammatory statements about neighboring countries. In one documented case, an advanced AI voice-cloning operation targeted Thailand's Prime Minister Paetongtarn Shinawatra through fraudulent phone calls impersonating a fellow ASEAN leader, highlighting the emerging threat posed from AI, allowing deception campaigns against high-level government officials.[53] Moreover, this technology allows Russian operators to test multiple versions of disinformation simultaneously and scale successful approaches across different platforms and linguistic communities. Sophisticated bot networks utilizing natural language processing create increasingly human-like social media personas that engage in extended conversations with real users. These "sleeper" accounts build credibility over months through seemingly ordinary interactions before deploying targeted disinformation during critical moments, such as elections or regional crises. During the 2018 elections in Malaysia, over 44,000 pro-government and anti-opposition tweets were posted by 17,000 bots in a week, disrupting a campaign which sought to increase voter turnout.[54] On a broader level, a study by researchers at Carnegie Mellon University found that, during contentious news periods across the Asia-Pacific, between 10 percent and 30 percent of all captured 'X' (Twitter) users were identified as bots, rapidly outnumbering news agencies and government accounts to obscure authentic sources.[55]

Current G7 Counter-Disinformation Architecture

G7 Rapid Response Mechanism (RRM)

Established at the 2018 Charlevoix Summit, the G7 RRM represents the primary multilateral coordination mechanism for addressing foreign threats to democracy. Led by Global Affairs Canada, the RRM has developed significant capabilities for threat identification, analysis, and coordination among G7 partners through dedicated working groups, annual threat assessments, and crisis response protocols.

The RRM has successfully coordinated responses during major electoral cycles, including the 2020 U.S. presidential election and multiple European parliamentary elections. The mechanism has produced comprehensive annual threat assessment reports that have informed national security strategies across G7 nations. According to observers, Sweden and Finland's accession into NATO has enhanced intelligence sharing and operational coordination. Thus, specialized working groups have contributed expertise in various threat vectors, including cyber operations, economic manipulation, and electoral interference.

Despite these achievements, the RRM still faces significant constraints that limit its effectiveness

in addressing the unchecked threats arising in the Indo-Pacific. This may be a result of insufficient funding and staffing which restrict the mechanism's ability to expand operations beyond its current European and North American focus. Limited engagement with Indo-Pacific regional partners creates intelligence gaps and reduces operational effectiveness in the region. The RRM's reactive rather than proactive operational posture means that responses often lag behind rapidly evolving threat environments. Moreover, inadequate technological capabilities for AI-era threats leave the mechanism vulnerable to sophisticated synthetic media and automated influence operations.

The RRM's Budget 2022 provides CAD $13.4 million over five years, with $2.8 million ongoing to Global Affairs Canada to renew and expand the G7 Rapid Response Mechanism.[56] While sizable, it is insufficient for the scale of operations required to address Indo-Pacific threats effectively. Staffing limitations mean that only 30 full-time analysts cover global threats, creating inevitable gaps in regional expertise and language capabilities essential for Indo-Pacific operations.

Bilateral and Trilateral Partnerships

The G7 nations maintain various bilateral arrangements for counter-disinformation cooperation, including the U.S.-Japan Strategic Dialogue on cyber and emerging technologies, the Australia-U.K. cyber cooperation framework, and multiple intelligence sharing agreements between European partners. However, these arrangements often lack coordination and may create redundancies or gaps in coverage. The Five Eyes intelligence alliance provides a foundation for information sharing among English-speaking partners, but its limited membership excludes key regional actors and creates potential coordination challenges with broader G7 initiatives. Bilateral partnerships between individual G7 nations and Indo-Pacific countries, while valuable, lack the comprehensive approach necessary to address sophisticated, multi-national threat operations.

Platform and Private Sector Engagement

Current G7 engagement with technology platforms remains ad hoc and inconsistent, with individual nations pursuing separate relationships with major social media companies and technology firms. While some companies have demonstrated willingness to cooperate during crisis situations, the absence of standardized protocols creates inefficiencies and limits effectiveness. Meta, Google, and Twitter have established individual relationships with various G7 governments, but these arrangements often result in contradictory requests and inconsistent enforcement of content policies.

The lack of unified G7 standards for identifying and responding to information threats means that platforms receive different guidance from different governments, creating confusion and reducing the overall effectiveness of important initiatives. Given the volume of content on social media, it remains a daunting challenge to quantify. According to one study, almost 20 percent of all search results on TikTok lead to some form of disinformation.[57] On Telegram, a major contributor to this landscape, the situation may be even worse. According to a separate study, 33 percent of all views on the platform go to junk news sources within the 12 most popular news sources.[58] This is particularly alarming given that Telegram has over 400 million users worldwide.

Strategic Framework for Enhanced G7 Coordination: Steps to Countering Russian FIMI in the Indo-Pacific

Institutional Strengthening and Coordination

Russian FIMI campaigns in the Indo-Pacific have evolved in sophistication, scale, and strategic intent, exploiting linguistic diversity, regional

political fault lines, and gaps in multilateral coordination. In response, the G7 must adopt a more centralized and forward-leaning posture. This begins with the establishment of an Indo-Pacific Information Security Coordination Center—a dedicated facility designed to augment, not replicate, existing mechanisms such as the Rapid Response Mechanism (RRM). The center would serve as a real-time hub for multilingual threat monitoring, predictive analysis, and early-warning operations. Leveraging artificial intelligence, machine learning tools, and digital forensics, the center would identify FIMI activity before it gains traction and operational success.

However, success will require a significant uplift in resources. A sustained annual investment of $250 million across G7 partners is essential to ensure capacity for 24/7 monitoring, interagency co-location, and secure information-sharing protocols. For reference, the U.S. Department of State Global Engagement Center (GEC) operated with an annual budget of circa USD $60 million, prior to it being shut down in 2024, making it no longer operational and thus exposing the U.S. and its partners to disinformation.[59] The GEC comprised of 120 staffers, which was reported to have been insufficient for the threats encountered.[60] Moreover, legal harmonization among G7 members must be prioritized to eliminate jurisdictional inconsistencies currently exploited by foreign actors. A robust framework for sharing classified information—including source protection measures—will be critical for integrating regional allies without compromising operational integrity. To meet the pace of adversarial operations, the RRM must also be upgraded with 24-hour operations center and integrated crisis response protocols, to reduce the time lag between detection and action. Current efforts are too often fragmented and reactive; speed and cohesion must become foundational principles.

Regional Partnership Development

Strategic partnerships in the Indo-Pacific are indispensable. The Quadrilateral Security Dialogue (Quad) offers an existing foundation for coordination. Formalized links between the G7's enhanced information mechanisms and the Quad's Countering Disinformation Working Group would enable synchronized analysis, training, and regional threat assessments. AUKUS (while primarily defense-oriented) contains underutilized potential for intelligence-sharing on information threats. Its inclusion in broader information warfare coordination would accelerate technology integration and cyber defense cooperation.

Nonetheless, ASEAN and Pacific Island states remain disproportionately vulnerable. Russian influence operations systematically exploit underdeveloped media ecosystems and limited resources. While ASEAN has initiated frameworks aimed at combating online disinformation, these measures remain inadequate for the scale to which Russia can operate. Current policies lack clear content classifications, enforcement standards, and interoperability with broader regional or international regimes. Without more nuanced and enforceable governance, ASEAN's information space will remain exposed. This should begin with recognizing a unified typology/taxonomy of harmful content and FIMI operations.[61]

To build on this regional resilience, G7 efforts should assist capacity-building programs in digital literacy, independent journalism, and institutional analysis. Establishing regional training centers, providing sustained technical assistance, and supporting civil society actors will strengthen local defenses. Fellowship and analyst exchange programs should embed regional talent into G7 institutions, cultivating long-term intelligence and policy ties. Efforts must also address the economic dimension of information warfare. Russia and China deploy narratives positioning Western engagement as unreliable or exploitative. To counter this, the G7 must promote a compelling alternative. Strategic communication should be backed by tangible infrastructure investments and

public diplomacy initiatives that emphasize transparency, sovereignty, and shared growth. Credibility will come not from rhetoric, but from visible, sustained commitment to democratic partnerships.

Platform Engagement and Technology Coordination

Private sector platforms remain the primary terrain on which information conflicts unfold. Current G7 engagement with such platforms is fragmented and duplicative, undermining both credibility and efficacy. A unified G7 communication channel should be established to streamline interaction with major digital platforms. Coordinated threat reporting, joint crisis protocols, and routine consultation with platform leadership are necessary to ensure fast, consistent action during emerging information campaigns.

Technological innovation must be treated as a strategic priority. Joint G7 investments in emerging AI-driven threat detection tools to identify deepfakes, automated bot networks, and cross-platform narrative coordination are essential. These capabilities should include predictive modeling informed by past Russian operational behavior, allowing for preemptive rather than reactive action.

Public-private partnerships should be formalized through structured programs that allow for secure technology testing, shared intelligence products, and mutual protection of sensitive data. Sandboxed environments can enable platforms to trial new detection tools alongside government analysts. Incentivized data-sharing arrangements must be developed to ensure the private sector remains an active participant without risking intellectual property or user privacy. The recent dismantling of the Russian-linked "Doppelgänger" network by OpenAI and partners in May 2024 illustrates both the importance and difficulty of timely private-sector intervention. The campaign reached operational impact before removal, highlighting the urgent need for earlier detection methods and integrated response mechanisms with partners.

Societal Resilience and Long-term Capacity

Ultimately, counter-disinformation efforts must extend beyond government and technology. Societal resilience is the long-term antidote to sustained FIMI operations. G7 nations should develop standardized digital and media literacy curricula tailored to different educational contexts and exportable to regional partners. Programs must be linguistically and culturally adapted to meet specific Indo-Pacific requirements. Partnership with local institutions is essential to ensure both relevance and legitimacy. Civil society actors—particularly independent media organizations—play a critical role but face chronic underfunding and, in some cases, state intimidation. G7 support should include targeted financial aid, digital security assistance, and emergency funds for organizations under threat. Legal protection mechanisms must be strengthened for journalists and researchers operating in hostile or semi-authoritarian environments.

In sum, the Russian disinformation threat in the Indo-Pacific is a strategic challenge requiring coordinated, sustained, and multidimensional countermeasures. The G7 must evolve from fragmented defense to proactive resilience—leveraging technology, partnerships, and credibility to contest the information battlespace with speed and unity.

Conclusion

Russian information operations in the Indo-Pacific represent a targeted, sophisticated, and evolving threat that requires a coordinated and comprehensive response from the G7 community and their regional partners. These trends, if left unchecked, will compound the operational challenge FIMI poses to democratic

nations in the Indo-Pacific region. The strategic framework outlined in this document provides a roadmap for enhancing collective capabilities while preserving democratic values and building sustainable partnerships. Success will require unprecedented levels of coordination among G7 nations, innovative approaches to technology and private sector engagement, and sustained commitment to capacity building and partnership development in the Indo-Pacific region. The investments required are substantial, but the costs of inaction—measured in terms of democratic erosion, regional instability, and strategic advantage ceded to authoritarian competitors—are far greater.

The framework emphasizes the need for immediate action while building sustainable, long-term capabilities. By combining enhanced institutional coordination, deeper regional partnerships, innovative technology applications, and comprehensive societal resilience building, G7 nations can effectively counter Russian information warfare while strengthening the democratic foundations that underpin the rules-based international order. Implementation of this strategy will require political will, financial commitment, and operational excellence from all G7 partners. However, the alternative—allowing Russian information operations to continue expanding and exploiting regional vulnerabilities to undermine democratic institutions—poses unacceptable risks to shared security and prosperity in the Indo-Pacific and beyond. The time for coordinated and comprehensive action is now. The framework provides the roadmap; success depends on the commitment and execution of G7 leaders and their regional partners in one of the most consequential information warfare challenges of the 21st century.

Authors –

Dr. Niklas Swanström *is the Executive Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) and a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI).*

Toby J. Logan *is an intern at the Stockholm Center for South Asian and Indo-Pacific Affairs. Originally from Scotland, he holds an MA in Digital Humanities and an MSc in International Relations. His research focuses on AI governance, disinformation, and security, with a recent focus on intelligence and diplomacy at the University of Cambridge.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 Seth G. Jones, "Russia's Shadow War Against the West," Centre for Strategic & International Studies (CSIS), March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

2 Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND, July 11, 2016, https://www.rand.org/pubs/perspectives/PE198.html.

3 Daniela Richterova, Elena Grossfeld, Magda Long, and Patrick Bury, "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal* 169, no. 5 (September 2024): 10–21.

4 Christopher B. Johnstone and Leah Klass, "Combatting Disinformation: An Agenda for U.S.-Japan Cooperation," Center for Strategic & International Studies (June 2024): 1–25.

5 Darren Linvill and Patrick Warren, "New Russian Disinformation Campaigns Prove the Past Is Prequel," The Lawfare Institute, January 22, 2024, https://www.lawfaremedia.org/article/new-russian-disinformation-campaigns-prove-the-past-is-prequel; Paul Bleakley, "Panic, pizza and mainstreaming the alt-right: A social media analysis of Pizzagate and the rise of the QAnon conspiracy," *Current Sociology* 71, no. 3 (2023): 509–525.

6 Russell Hanson, Adam R. Grissom, and Christopher A. Mouton, "The Future of Indo-Pacific Information Warfare: Challenges and Prospects from the Rise of AI," RAND, March 14, 2024; Alan Suderman and Ali Swenson, "Right-wing influencers were duped to work for covert Russian operation, US says," *Associated Press*, September 2024, https://apnews.com/article/russian-interference-presidential-election-influencers-trump-999435273dd39edf7468c6aa34fad5dd; Niina Meriläinen, "Influencers as Tools in Hybrid Operations Online," Proceedings of the 19th International Conference on Cyber Warfare and Security (2025): 265–272.

7 Nichita Gurcov, "Testing the waters: Suspected Russian activity challenges Europe's support for Ukraine," ACLED. May 22, 2025, https://acleddata.com/2025/05/22/testing-the-waters-suspected-russian-activity-challenges-europes-support-for-ukraine/; Richterova, n. 3.

8 John Lenczowski, "U.S. Strategy for the Growing China Threat," Institute of World Politics, January 19, 2020, https://www.iwp.edu/speeches-lectures/2020/01/29/u-s-strategy-for-the-growing-china-threat/.

9 Eleanor Knott, "The Securitised 'Others' of Russian Nationalism in Ukraine and Russia," *LSE Public Policy Review* 3, no. 1 (2023), https://ppr.lse.ac.uk/articles/10.31389/lseppr.80.

10 U.S. Department of Justice, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," Special Counsel Robert S. Mueller, March 2019, 1–182.

11 U.S. Cyber Command, "Russian Disinformation Campaign 'DoppelGänger' Unmasked: A Web of Deception," September 3, 2024, https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/.

12 McKenzie Sadeghi and Isis Blachez, "A well-funded Moscow-based global 'news' network has infected Western artificial intelligence tools worldwide with Russian propaganda," Newsguard, March 6, 2025, https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global; Canyu Chen and Kai Shu, "Combating misinformation in the age of LLMs: Opportunities and challenges," *AI Magazine* 45 (2024): 354–368.

13 Mark Galeotti, "Crimintern: How the Kremlin uses Russia's criminal networks in Europe," European Council on Foreign Relations, April 18, 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/.

14 Laura Rosenberger, "Laura Rosenberger's Testimony: 'Undermining Democracy: Kremlin Tools of Malign Political Influence'," German Marshall Fund of the United States, July 2024, https://www.gmfus.org/news/laura-rosenbergers-testimony-undermining-democracy-kremlin-tools-malign-political-influence; Kristine Baghdasaryan, "Unravelling the Web," Transparency International Russia, 2024, 1–25.

15 David Gioe and Alexander Molnar, "It's Time to Stop Debunking AI-Generated Lies and Start Identifying Truth," RUSI, November 2, 2023, https://www.rusi.org/explore-our-research/publications/commentary/its-time-stop-debunking-ai-generated-lies-and-start-identifying-truth.

16 Darren L. Linvill, Brandon C. Boatwright, Will J. Grant, and Patrick L. Warren, "The Russians are hacking my brain!" investigating Russia's internet research agency Twitter tactics during the 2016 United States presidential campaign, *Computers in Human Behavior* 99 (2019): 292–300.

17 Hannah Chemerys, "Deepfakes and Synthetically Reproduced Media Content as a Form of Disinformation in the Context of the Russian Aggression Against Ukraine,"*Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи: тези доп. учасників міжн. наук.-практ. конф. (Анн-Арбор - Харків, 12-13 груд*, (2023): 41–45; Marina Miron, and Rod Thornton, "The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?" *Applied Cybersecurity & Internet Governance 3, no. 1* (2024): 147–169.

18 Ilya Yablokov, "Russian disinformation finds fertile ground in the West," *Nat Hum Behav* 6 (2022): 766–767; Olena Kalashnikova and Fabian Schäfer, "Russian State-controlled Propaganda and its Proxies: Pro-Russian Political Actors in Japan," *Asia-Pacific Journal* 22, *Issue 3, No. 6* (2024).

19 German Federal Foreign Office, "Germany Targeted by the Pro-Russian Disinformation Campaign 'Doppelgänger'," Technical Report, June 5, 2024.

20 Evan M. Williams and Kathleen M. Carley, "Search engine manipulation to spread pro-Kremlin propaganda," *Misinformation Review*, Harvard Kennedy School, February 16, 2023.

21 U.S. Department of State, "Russia's Pillars of Disinformation and Propaganda," GEC Special Report, 2020.

22 United Nations, "Widespread use of torture by Russian military in Ukraine appears deliberate," Press Release, June 15, 2023, https://www.ohchr.org/en/press-releases/2023/06/widespread-use-torture-russian-military-ukraine-appears-deliberate-un-expert.

23 Julia Steers, "'The Terror Was Palpable': Inside Russia's Notorious Mercenary Group," VICE News, May 11, 2022, https://www.vice.com/en/article/inside-russia-wagner-group-mercenaries/.

24 Dmitry Zinoviev, "A Social Network of Russian 'Kompromat'," Cornell University, 2020, 1–12; Allon J. Uhlmann and Stephen McCombie, "The Russian Gambit and the US Intelligence Community: Russia's Use of *Kompromat* and Implausible Deniability to Optimize its 2016 Information Campaign against the US Presidential Election," Library Trends 68, no. 4, (2020): 79–696; Sarah Oates, "Kompromat Goes Global?: Assessing a Russian Media Tool in the United States," *Slavic Review* 76, no. S1 (2017): 57–65.

25 CSIS, "Russia's Shadow War Against the West," 2025.

26 Conor Cunningham, "A Russian Federation Information Warfare Primer," Henry M. Jackson School of International Studies, November 12, 2020, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.

27 VIGINUM, "Analysis of the Russian Information Manipulation Set Storm-1516," Technical report, May 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

28 Disinformation Social Media Alliance (DISA), "Russian Disinformation Campaign Utilizes Te Reo Māori News Platform to Target New Zealand," March 14, 2025, https://disa.org/russian-disinformation-campaign-utilizes-te-reo-maori-news-platform-to-target-new-zealand/.

29 VIGINUM, "Matryoshka: A Pro-Russian Campaign Targeting Media and the Fact-Checking Community," Technical report, June 2024, https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf.

30 "Pro-Russian influence campaign targets Australian media outlets, including ABC, researchers find," *ABC News*, June 4, 2024, https://www.abc.net.au/news/2024-06-04/russia-war-ukraine-propaganda-disinformation-australian-media/103927386.

31 James Pamment and Darejan Tsurtsumia, "Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency," Swedish Agency of Psychological Defense, MFA Report Series No. 8, 2025, https://mpf.se/download/18.7cffbee41969f6d83e115221/1747230166207/Beyond%20Operation%20Doppelganger.pdf.

32 Clint Watts, "How Russia is trying to disrupt the 2024 Paris Olympic Games," Microsoft, June 2, 2024, https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/.

33 MTAC, "Russian influence efforts converge on 2024 Paris Olympic Games," Microsoft Threat Intelligence Report, June 2024.

34 Jakub Kubś, "Global Offensive: Mapping the Sources behind the Pravda Network," GLOBSEC, 2025.

35 Marcus Kolga, "The growing threat of Russian information operations against Japan," Macdonald-Laurier Institute, March 28, 2023, https://macdonaldlaurier.ca/the-growing-threat-of-russian-information-operations-against-japan-marcus-kolga-for-inside-policy/.

36 Maiko Ichihara, "How To Tackle Disinformation In Japan: Lessons From The Russia-Ukraine War," Brookings, December 2022, 36–43.

37 U.S. Department of Defense, "Military And Security Developments Involving The People's Republic Of China 2024," Report to Congress, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

38 Rotem Baruchin, "Fake Profiles Swarmed Philippines Elections," Cyabra, May 13, 2025, https://cyabra.com/blog/fake-profiles-swarmed-philippines-elections/.

39 Poppy Mcpherson, "Exclusive: Fake accounts drove praise of Duterte and now target Philippine election," *Reuters*, April 11, 2025, https://www.reuters.com/world/asia-pacific/fake-accounts-drove-praise-duterte-now-target-philippine-election-2025-04-11/.

40 Nataliya Bugayova and George Barros, "The Kremlin's Expanding Media Conglomerate," Institute for the Study of War, January 15, 2020, https://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-expanding-media-conglomerate.

41 Australian Institute of International Affairs, "Foreign State-Sponsored Disinformation in the Pacific Islands," March 13, 2025, https://www.internationalaffairs.org.au/australianoutlook/foreign-state-sponsored-disinformation-in-the-pacific-islands/.

42 Andrew Whiskeyman and Michael Berger, "Axis of Disinformation: Propaganda from Iran, Russia, and China on COVID-19," Washington Institute Fikra Forum Policy Analysis, February 2021, https://www.washingtoninstitute.org/policy-analysis/axis-disinformation-propaganda-iran-russiaand-china-covid-19.

43 UK Ministry of Defense on "X", October 13, 2024: https://x.com/DefenceHQ/status/1845390134432194852; Chris Bott, "Okean Returns: A Battered Russian Navy Brings Back a Soviet-Era Exercise," October 2024, https://www.usni.org/magazines/proceedings/2024/october/okean-returns-battered-russian-navy-brings-back-soviet-era#:~:text=Okean%202024%20was%20designed%20to,weapon%20systems%2C%20and%2090%2C000%20personnel.

44 "EU has 'conclusive' proof of armed drones for Russia being made in China," Reuters, September 25, 2024, https://www.reuters.com/world/russia-has-secret-war-drones-project-china-intel-sources-say-2024-09-25/.

45 Dries Putter and Sascha-Dominik Bachmann, "Russia and China expected to renew their espionage vigour," *Journal on Baltic Security* 9, no. 1 (2023): 1–31.

46 Jill Goldenziel and Daniel Grant, "Information Resilience: Countering Disinformation and Its Threat to the U.S. Alliance System," War on the Rocks, Commentary, November 15, 2023, https://warontherocks.com/2023/11/information-resilience-countering-disinformation-and-its-threat-to-the-u-s-alliance-system/.

47 M. Taylor Fravel, "China: Balancing the US, increasing global influence," Chatham House, Research Paper (March 27, 2025).

48 Chris Kremidas-Courtney, "Hybrid storm rising: Russia and China's axis against democracy," European Policy Centre (EPC), May 2, 2025, https://www.epc.eu/publication/Hybrid-storm-rising-Russia-and-Chinas-axis-against-democracy-64b158/; Lucas Minisini and Thomas Eydoux, "How Chinese spies used a far-right politician for anti-EU influence operations," *Le Monde*, December 15, 2023, https://www.lemonde.fr/en/international/article/2023/12/15/how-chinese-spies-gave-orders-to-a-far-right-european-politician_6345886_4.html.

49 Seth G. Jones, "Russia's Shadow War Against the West," Center for Strategic & International Studies, CSIS Briefs, March 2025, https://www.jstor.org/stable/pdf/resrep68536.pdf?acceptTC=true&coverpage=false&addFooter=false; Police of Finland, "National Bureau of Investigation has clarified technically the cause of gas pipeline damage," October 24, 2023, https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage.

50 CSIS, Combatting Disinformation, 2024.

51 David Bandurski, "China's official Xinhua News Agency signed a cooperation agreement with RT," Brookings, March 11, 2022, https://www.brookings.edu/articles/china-and-russia-are-joining-forces-to-spread-disinformation/.

52 GEC, "Pillars of Russia's Disinformation and Propaganda Ecosystem", 2020.

53 AIAAIC, "Thailand's prime minister targeted in ASEAN AI voice scam," February 2025, https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/thailands-prime-minister-targeted-in-asean-ai-voice-scam.

54 Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Online Supplement to Working Paper 2018, University of Oxford, 2018, 39–42.

55 Daniel Tkacik, "Social Media Bots Interfere in Asia-Pacific Elections, too," CyLab – Carnegie Mellon University, July 11, 2025, https://www.cylab.cmu.edu/news/2019/07/11-social-bots-interfere-elections.html.

56 Government of Canada, "Chapter 5: Canada's Leadership in the World," Federal Budget: Budget 2022.

57 Fransisco Ruak, "The Impact of TikTok on Combating and Filtering Hoax News: A Mixed-Methods Study," *KAMPRET Journal* 3, no. 1 (September 2023): 22–32.

58 Aleksi Knuutila, Aliaksandr Herasimenka, Jonathan Bright, Rasmus Nielsen, and Philip N. Howard, "Junk News Distribution on Telegram: The Visibility of English-language News Sources on Public Telegram Channels," *COMPROP Data Memo*, University of Oxford, July 2020, 1–5.

59 Josh Meyer, "US nerve center to combat China and Russia global propaganda shut down by GOP opposition," *USA Today*, December 28, 2024.

60 Joshua Brustein, "The Tiny U.S. Agency Fighting Covid Conspiracy Theories Doesn't Stand a Chance," *Bloomberg*, October 29, 2023, https://www.bloomberg.com/news/features/2020-05-14/the-tiny-u-s-agency-fighting-covid-conspiracy-theories-doesn-t-stand-a-chance.

61 Michele Banko, Brendon MacKeen and Laurie Ray, "A Unified Typology of Harmful Content," Proceedings of the Fourth Workshop on Online Abuse and Harms, November 2020, 125–137.