Annual Report 2022

G7

RAPID RESPONSE MECHANISM

PROTECTING DEMOCRACY

Global Affairs Canada's Rapid Response Mechanism Canada (RRM Canada) team serves as a permanent secretariat for the G7 Rapid Response Mechanism (G7 RRM). RRM Canada prepared this report in close collaboration with Germany, as the 2022 G7 Presidency, and in partnership with G7 RRM members and observers, including Australia, New Zealand, NATO, the Netherlands and Sweden.

TABLE OF CONTENTS

G7

RAPID RESPONSE MECHANISM

PROTECTING DEMOCRACY

INTRODUCTION

The G7 Rapid Response Mechanism (G7 RRM) was established by leaders at the 2018 G7 Summit in Charlevoix to strengthen coordination between G7 countries to identify and respond to diverse and evolving foreign threats to democracy. These threats include hostile state activity targeting our democratic institutions and processes, our media and information environment, and the exercise of human rights and fundamental freedoms.

The G7 RRM comprises Focal Points from the G7 community, including the EU. It counts Australia, New Zealand, NATO, the Netherlands and Sweden as observers. Focal Points leverage their respective institutional structures and processes to support whole-of-government engagement. Canada leads the G7 RRM on an ongoing basis.

During the G7 Foreign and Development Ministers meeting in London in 2021, foreign ministers committed to producing G7 RRM annual reports. The reports address different aspects of the evolving threat landscape and outline possible responses by members and observers aimed at enhancing public awareness and building resilience, including proactive responses. While the 2021 report focused on disinformation as a specific vector of foreign information manipulation and interference (FIMI) activities, this 2022 report focuses on the broader phenomena of *hybrid threats*, including specific examples encountered by the G7 RRM community in 2022.[1]

The report is structured as follows:

1. Overview of hybrid threats faced by the G7 RRM in 2022
2. Updates on FIMI threats and government efforts to safeguard national elections against these threats
3. Outline of G7 RRM activities over the past year
4. Examples of initiatives undertaken by G7 RRM members in response to foreign threats

1 According to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the term "hybrid threat" refers to an action conducted by state or non-state actors whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities across the political, economic, military, civil or information domains. For more background information, visit the Hybrid CoE.

FOCUS ON HYBRID THREATS IN 2022

The international threat landscape in 2022 was dominated by Russia's war against Ukraine. As the world began to recover from the COVID-19 pandemic, Russia's ongoing war of aggression against Ukraine commanded the attention of democratic governments and challenged the rules-based international order. In June 2022, the G7 Leaders' Communiqué defined the situation as a "critical juncture for the global community."[2] Meanwhile, German Chancellor Olaf Scholz called it *Zeitenwende*—a turning point in history.[3]

Against the backdrop of the full-scale invasion, hybrid threats have emerged as a key concern for democracies worldwide. These threats can be understood as a mix of coercive and subversive activities conducted with conventional and unconventional methods across various domains, including the diplomatic, military, economic and technological domains. Hybrid activities can be used in a coordinated manner by state actors and their proxies in pursuit of specific objectives while remaining below the threshold of formal war.[4]

Due to their nebulous and wide-ranging nature, hybrid activities may be difficult to recognize and counter. This report highlights several hybrid threats that came into focus for the G7 RRM in 2022, including:

1. Efforts to manipulate the information environment that undermine democratic processes and institutions, including at the subnational level
2. Information and cyber attacks during the full-scale invasion of Ukraine
3. Economic coercion and scientific espionage to pursue strategic objectives

EFFORTS TO UNDERMINE DEMOCRATIC PROCESSES AND INSTITUTIONS

Foreign state actors and their proxies leverage vulnerabilities in open societies in pursuit of their objectives. They do so at both national and subnational (below federal jurisdiction) levels, affecting public institutions, private enterprises, communities and individuals. They try to influence public opinion and behaviours, change policy and disrupt democratic processes, including attempts by the Russian and Chinese governments to interfere in elections.[5] These actors deploy a wide range of hybrid activities, including information manipulation, in order to suppress independent or critical voices, foment division or advance narratives favourable to their national interests while eroding the integrity of our information environments and rules-based international order.[6]

INFORMATION AND CYBER ATTACKS

Russia's military aggression against Ukraine has been accompanied by a broad range of hybrid activities, including information-based attacks. During the reporting period, Russian state-aligned actors and their proxies engaged in interference and information manipulation globally in order to legitimize Russia's illegal war, to undermine public support for Ukraine and to deflect blame for food insecurity and economic and energy disruptions.

In all likelihood, these false narratives aimed to undermine cohesion between like-minded partners and within the international community. They sought to foster resentment between industrialized and emerging and developing countries. These activities have had a negative effect on political and economic

2 G7 Leaders Communiqué (Elmau, June 28, 2022).
3 See Scholz, Olaf, "Die globale Zeitenwende", originally published in German, December 5, 2022.
4 See Joint Communication to the European Parliament and Council, "Joint framework on countering hybrid threat: a European Union response" (European Commission, June 2016).
5 "China's Growing Attempts to Influence U.S. Politics" (Council on Foreign Relations, October 31, 2022), "Chinese interference: What government documents tell us about election meddling" (Global News, December 16, 2022), "Report on foreign interference in all democratic processes in the European Union, including disinformation", A9-0022/2022 (European Parliament, February 9, 2022).
6 Among others, see European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), "The Landscape of Hybrid Threats: A Conceptual Model" (Hybrid CoE) and "Hybrid Threats: A Comprehensive Resilience Ecosystem" (Hybrid CoE, GRC 130097).

conditions in Africa, Asia and Latin America, where Russia and China both sought to foster dependencies.[7] In addition, Russia's widespread and continuous cyberattacks against Ukrainian civilian critical infrastructure and government agencies, which provide essential services, were contrary to the expectations set by all UN Member States of responsible state behaviour in cyberspace.[8]

ECONOMIC COERCION, SCIENTIFIC ESPIONAGE AND SABOTAGE

These global challenges emphasized the need to protect private enterprises, especially their value and supply chains, and research institutions against illegitimate influence, espionage, illicit knowledge leakage and sabotage, both online and offline.[9] Furthermore, economic and diplomatic coercion, such as implicit or explicit threats to restrict trade or discussion of human rights, are increasingly used as hybrid tactics in pursuit of strategic objectives.

In this context, hostile foreign states and affiliated actors are pursuing the acquisition of information related to issues of economic and political importance.[10] Using human and financial resources deployed through overt and covert means, these activities aim to attain a knowledge advantage and close gaps in skills or expertise. At the same time, they may also be carried out to identify vulnerabilities for future exploitation through hybrid attacks.

For instance, state-controlled investments or sending state-sponsored scientists to work in sectors of interest within the target country can be used to obtain technologies, expertise or intellectual property. While purportedly legal, such activities can translate into risks for our economies and require carefully calibrated responses that combine prevention, detection and raising costs for perpetrators of hostile activities, while still maintaining and promoting opportunities for collaboration and innovation.

7 For an example of long-term influence on local structures and the creation of long-term dependencies, see the expert report by Gelpern, Horn, Morris et al., How China lends (Kiel Institute for the World Economy, March 2021).

8 "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless" (Wired, November 18, 2022), Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union (EU Council, May 10, 2022).

9 For reference purposes only, see the G7 Hiroshima Leaders' Communiqué at the G7 Hiroshima Summit (May 2023).

10 See Hunter, Impiombato et al., Countering China's coercive diplomacy (Australian Strategic Policy Institute (ASPI), February 2023), Adachi, Brown, Zenglein, Fasten your seatbelts: How to manage China's economic coercion (MERICS China Monitor, August 2022), Hackenbroich, Jonathan, Tough Trade: The hidden costs of economic coercion (European Council on Foreign Relations, February 2022).

IMPLICATIONS AND RESPONSE

Russia is using information manipulation as a crucial instrument of its war of aggression against Ukraine with an unprecedented intensity. More broadly, authoritarian governments employ information manipulation and interference as key vectors for exerting illegitimate political influence. Other forms of hybrid threats also loom large across the G7 RRM community, including economic coercion, scientific espionage and sabotage. These threats manifest themselves at the subnational, community or individual levels.

Countering these threats requires coordination across governments, sectors, levels of government and policy files. While structures to counter hybrid threats on the national level have been established within some G7 and observer states,[11] foreign interference at the subnational level remains a daunting challenge. It is incumbent upon us to continue to work across domestic and foreign policy silos and to strengthen collaboration with industry, academic and civil society partners.

In recognition of this reality, G7 RRM countries began to share information and best practices under the German Presidency in 2022 to better understand how subnational threats manifest themselves.

For example, towards the end of 2022, the issue of transnational repression was thrust into the public spotlight following a series of civil society reports about transnational policing across the globe by the People's Republic of China (PRC).[12] Transnational repression—including but not limited to these "overseas stations"—has become a significant concern for democratic governments, including G7 RRM members, due to increasing cases of foreign state actors intimidating diaspora communities, human rights defenders and other critical voices who have fled repressive regimes, and due to other potential risks they may pose to democratic societies.

Identifying effective approaches to countering transnational repression and other subnational threats will be an area of focus and strengthened collaboration for G7 RRM members in 2023.

11 See the U.S. National Security Strategy (October 2022), France's National Strategic Review (November 2022), Japan's National Security Strategy (December 2022), Netherland's Security Strategy (April 2023), Germany's National Security Strategy (June 2023). Also, see EU Report A9-0022/2022 "REPORT on foreign interference in all democratic processes in the European Union, including disinformation" (February 2022) that calls for an EU strategy on foreign interference, including disinformation.

12 Safeguard Defenders, 110 Overseas: Chinese Transnational Policing Gone Wild (Safeguard Defenders: September 2022) and Patrol and Persuade: A follow-up investigation to 110 Overseas (Safeguard Defenders: December 2022).

GOVERNMENT EFFORTS TO SAFEGUARD NATIONAL ELECTIONS IN 2022

In 2022, concerns about foreign information manipulation and interference (FIMI) by foreign states featured as a prominent threat vector in national and subnational elections globally, including in G7 RRM member and observer countries. While FIMI is not unique to elections, election campaigns are often flashpoints around which some hostile state activities intensify in what are likely attempts to influence electoral outcomes, to undermine trust in democratic processes and institutions, or to drive polarization.

In fall 2021, **France's** agency for vigilance and protection against foreign digital interference (VIGINUM) launched operations to secure the 2022 French presidential and legislative elections from FIMI. The agency worked closely with key domestic stakeholders responsible for safeguarding the integrity of elections, such as the Ministry of the Interior, the National Commission for the Control of the Election Campaign for the Presidential Election, and the Constitutional Council, among others. It also established working relations with digital platforms and provided awareness sessions to political parties. Throughout these elections, VIGINUM worked in close coordination with partners to ensure timely and agile responses to possible incidents. Particular attention was paid to narratives which risked undermining the credibility of the electoral process, both before and after the elections. Overall, while no major malign campaigns were identified, VIGINUM detected sixty cases of inauthentic activity on digital platforms, five of which were categorized as foreign digital interference.

In 2022, the **Swedish** Psychological Defence Agency (PDA) collaborated with domestic partners, including election administration, police, cyber and intelligence services, to protect Sweden from foreign interference in the September general election. The Agency prepared for a worst-case scenario based on an assessment of foreign threat actors' capabilities and intentions to interfere with the elections or critical infrastructure at local, regional and national levels. The PDA presented a report on threats and vulnerabilities to the government and relevant stakeholders in order to increase awareness and resilience. The Agency also launched an information campaign,

"Don't be fooled," in the summer of 2022 to raise public awareness. The campaign described adversaries' methods and tools to help citizens stay vigilant against malign interference. The Agency conducted training with key personnel in election administration and, on request, with journalists and representatives of political parties. Ultimately, while attempts by foreign actors to influence political opinion were identified, the PDA assessed that foreign interference did not affect the Swedish elections or the electoral process.

In **Italy**, national authorities closely monitored both social and traditional media during the electoral campaign for the parliamentary elections in September. A Russian disinformation campaign that targeted political leaders and candidates with narratives favouring Russia's illegal invasion of Ukraine was identified, but assessed as having no significant impact.

Ahead of **Australia's** federal election in May 2022, the Electoral Integrity Assurance Taskforce (EIAT) was set up to provide advice to the Electoral Commissioner on matters that risked compromising the integrity of the election. The EIAT is an inter-agency mechanism responsible for assessing, understanding and mitigating threats to electoral integrity and, if required, for providing advice to the Electoral Commissioner on how to manage these threats. Following the election, Australian Electoral Commissioner Tom Rogers stated that the EIAT did not identify any interference, whether foreign or otherwise, that compromised the delivery of the 2022 federal election or would undermine the confidence of the Australian people in the results of the election.

Ahead of the 2022 midterm elections in the **United States**, the Cybersecurity and Infrastructure Security Agency (CISA) conducted security assessments of election infrastructure and cybersecurity vulnerability scanning in hundreds of U.S. election jurisdictions. CISA facilitated information sharing via the 3,400-member Election Infrastructure Information Sharing and Analysis Center, a source of real-time, actionable threat and mitigation information to help state and local election officials understand the election security risk environment. CISA also conducted training, exercises, panel presentations and keynote speeches across the U.S., reaching more than 5,000 local, state, federal, international and private sector entities with a role in election security and resilience. Additionally, the U.S. federal law enforcement and intelligence agencies monitored foreign threat activity, shared information and provided election security assistance to state and local election authorities and the private sector. Following the elections, CISA Director Jen Easterly issued a statement indicating that there was no evidence that would indicate that any voting system "deleted or lost votes, changed votes, or was in any way compromised in any race in the country."

TRENDS IN FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

The 2021 G7 RRM Annual Report focused on disinformation as a vector of FIMI. This has continued to be the case throughout 2022[13] and was a primary focus for the 2022 G7 RRM conference in Berlin.[14]

Throughout the reporting period, the information manipulation tactics and methods employed by foreign state actors expanded in terms of both the breadth of targets and sophistication. For example, Russia increasingly targeted women or LGBTQI+ persons in Italy, Tunisia, Brazil and Hungary, whereas Iran engaged in cyber-enabled influence operations and online harassment.[15] Russia increasingly sought to manipulate the global information environment by using "cloned" websites of internationally known media (for example, *Der Spiegel* or CNN)[16] and by supporting the growth of a commercial "disinformation industry,"[17] among other efforts. We anticipate that these phenomena will likely increase in the years to come, affecting susceptible institutions and societies, especially those where resilience to foreign information manipulation and interference remains low, like Germany.[18]

13 See first EEAS Report on Foreign Information Manipulation and Interference Threats (February 2023).

14 See G7 Leaders' Communiqué (June 2022), G7 Interior and Security Ministers' Statement (November 2022), G7 Foreign Ministers' Communiqué (May 2022), G7 Media Ministers' Communiqué (June 2022).

15 See Di Meco, Monetizing Misogyny – Gendered Disinformation and the Undermining of Women's Rights and Democracy Globally (ShePersisted, February 2023) and Jankowicz, Hunchak et al., Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online (Wilson Center, January 2021). On Iran, see Watts, "Rinse and repeat: Iran accelerates its cyber influence operations worldwide" (Microsoft, May 2, 2023).

16 See Alaphilippe, A. et al., Doppelgänger – Media clones serving Russian propaganda (EU Disinfo Lab, September 2022) and the VIGINUM report RRN: une campagne numérique de manipulation de l'information complexe et persistante (June 13, 2023).

17 See Europol Innovation Lab's Facing reality? Law enforcement and the challenge of deepfakes (April 2022), Kwon H., The Disinformation Business is Booming (Defence One, November 15, 2021), Christoph, Diehl, Hopoenstedt et al. (in German), So funktioniert das System der Lügenindustrie (Der Spiegel, February 14, 2023). See also Forbidden Stories, a collection of investigative reports on the disinformation industry.

18 See Lamberty and Frühwirth (in German), Ein Jahr russischer Angriffskrieg: Die Rolle von Desinformation in Deutschland, CEMAS Research Paper (February 2023), Brandt, Ichihara, Jalli et al., Impact of Disinformation democracy in Asia (Brookings Institution, December 2022).

In this context, new challenges are being raised by the continued evolution of generative AI technologies and synthetic media, such as large language models, powerful chat bots, image and video generation, and voice simulation software. These technological advancements are capable of creating complex, high-quality and concerning content in a matter of seconds. For example, image generation tools can create authentic-looking pictures and videos of events that never happened, while voice generation software can persuasively imitate the voice of a person based on a sample of a few seconds.[19] Especially when automated, these synthetic media capabilities could dramatically increase the generation and propagation of disinformation campaigns or present manipulated "realities" at scale and across the globe.[20]

The G7 RRM identified the following eight noteworthy trends through primary and secondary research across the G7 RRM community.

RUSSIAN FIMI AND DISINFORMATION

1. Ongoing information manipulation targeting Ukraine

Russia continued to undertake information manipulation activities to legitimize its territorial conquest of Ukraine. The themes of the Russian disinformation narrative have changed from pre-war propaganda (for example, "the West" as aggressor, the "Nazification" of Ukraine) to wartime propaganda (for example, surrender of Ukrainian troops in crucial theatres of war, military failures or Ukrainian "war crimes," "ethnic cleansing" operations in Donbas). As the conflict continued, the main narratives also included false allegations regarding the impact of Western sanctions on food security and the energy crisis. Some narratives fuelled by Russian disinformation—for example, on alleged biological weapons laboratories in Ukraine, on the depressive effects of sanctions and on rampant "Russophobia"—were amplified by conspiracy, anti-vax and anti-EU groups in the West.

2. Impersonation of EU/Western media

In the context of Russia's war of aggression against Ukraine, there was a surge in incidents involving the impersonation of mainstream media imagery and brands on social media platforms and the production of falsified news content and mimicked websites promoting pro-Russian messages. This trend began in summer 2022 and included impersonations of Germany's *Der Spiegel* and *Deutsche Welle*, the UK's BBC and CNN in the U.S.[21] Malign actors also bought Internet domain names almost identical to established and authentic media websites, creating "clones" of at least 17 media providers and targeting users with fake articles.[22] Additionally, pro-Kremlin actors created fake covers of satirical magazines in Spain, Germany and France, which were then promoted by the Russian FIMI ecosystem.[23] This confusion between authentic and inauthentic traditional media poses challenges to the domain name industry and further muddied public confidence in credible and recognizable media sources.

3. Gender- and identity-based disinformation on the rise

Throughout the reporting period, Russia spread sexualized falsehoods about Ukrainian women and the LGBTQI+ community to stoke sexism and homophobia,[24] while Chinese state-linked actors targeted female journalists with harassment.[25] The effect of identity-based disinformation is the silencing of the targets. In addition, this form of disinformation reinforces hierarchies of institutional power that place

19 See Helmus, Todd C., "Artificial Intelligence, Deepfakes, and Disinformation" (RAND Corporation, July 2022), Sadeghi M. and Arvanitis L., "Rise of the Newsbots: AI-Generated News Websites Proliferating Online" (Newsguard, May 1, 2023).

20 See Buchanan, Lohn et al., "Truth, Lies, and Automation: How Language Models Could Change Disinformation" (Georgetown Center for Security and Emerging Technology, 2021).

21 Weber J. and Baig R., "Fake content targets international media" (DW, August 2022).

22 See Alaphilippe A. et al., "Doppelganger – Media clones serving Russian propaganda" (EUDisinfoLab, September 2022) and the VIGINUM report, RRN: une campagne numérique de manipulation de l'information complexe et persistante (June 13, 2023).

23 "'Fake news inception': Debunking fake Charlie Hebdo covers" (France 24 English, December 12, 2022).

24 Jankowicz, Hunchak, Pavliuc et al., Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online (Wilson Center, January 2021), Bilousenko, Pivtorak, Iliuk, Slyvenko, "Prostitution will save Ukraine from the default": Investigating Russian gender disinformation in social networks" (Detector Media, September 2022).

25 See Zhang, A. and Cave, D., "Smart Asian women are the new targets of CCP global online repression" (ASPI, June 2022), Allen-Ebrahimian, B., "China-linked Twitter harassment targets female Asian journalists outside China" (Axios, June 2022).

women, the LGBTQI+ community, people of colour and other vulnerable communities at the bottom, further polarizing Western societies.[26]

4. Use of professional video-based content mocking EU citizens

The Russian FIMI ecosystem produced and distributed satirical videos attacking Western values and exposing the purported reasons why Russia is superior to Western democracies. The European External Action Service (EEAS) Data team detected this new trend, including a video highlighting the Western "Russophrenia" and supposed attempts to cancel Russian culture, an advertisement inviting EU citizens to move to Russia, and commercial videos mocking EU citizens on the energy crisis.[27] The videos featured professional actors that previously played roles in Russian TV shows, series and movies, which points to the increasing "professionalization" of this propaganda industry.

5. Kremlin-backed outlets rebrand to circumvent EU sanctions

After the EU announced sanctions on state-owned media outlets RT (Russia Today) and Sputnik, and with Telegram subsequently banning them from their platform, Kremlin-aligned Telegram channels responded by rebranding and making changes that put them "multiple steps ahead" of regulators.[28] Propagandists used tactics such as copycat and mirror accounts and changing channel names, colours and logos. They also relied on loyal listeners to share content in livestreams and instructions on how to access banned channels with a VPN.[29] Channels also began posting articles to anonymous publishing platforms to maintain their news-like appearance without Kremlin-backed outlet names in their URLs and turned to official diplomatic channels to continue to spread disinformation, as the social media accounts of many leaders in state media and the network of MFA and Russian embassy accounts were unaffected by the bans.

GLOBAL DEVELOPMENTS

6. Security guarantees and the use of history to gain credibility and influence

In 2022, Russian state-affiliated actors like Wagner Group, the private military company, continued attempts to gain influence globally, including in Africa, the Middle East and Latin America. Seemingly unconstrained by human rights considerations and responsible business practices, the tactics employed by these actors involve the promise of security guarantees in exchange for extracting natural resources or access to strategic locations like ports.[30] Their presence in several African countries also involved interference in the information environment, as was demonstrated recently in Mali, Burkina Faso, Madagascar and Sudan.[31] Another Wagner tactic involved exploiting the history of African colonialism of certain European countries, like France, or negative perceptions of the United States' historical role in Latin America to gain more credibility for Russia's actions in these countries, as well as in Ukraine.

7. PRC amplifier networks and anti-Western narratives

Chinese authorities leveraged amplifier networks, normally involved in the promotion of regional or city-based government programs, to inorganically overwhelm ("swarm") the information space in defence of

26 See the proceedings of the 46th NATO Committee on Gender Perspectives focuses on hybrid threats, disinformation and human security (NATO, October 2022), Strand and Svensson, "Disinformation campaigns about LGBTI+ people in the EU and foreign influence" (EU Parliament, July 2021), Bradshaw, S., "Identity-based Propaganda: Discrimination, Division and Democracy" (Stanford University, on-line lecture, January 2022).

27 The following links are provided for research references only: Russian culture (link), moving to Russia (link), and energy crisis (link, link, link).

28 See Killeen, M., "Kremlin-backed media evading EU sanctions, report finds" (Euractiv, May 2022).

29 See Gerster L. and Arcostanzo F., "How Russian State-Controlled Media and its Supporters are Circumventing Social Media Restrictions" (ISD, March 2022).

30 Fasanotti, F. S., "Russia's Wagner Group in Africa: Influence, commercial concessions, rights violations, and counterinsurgency failure" (Brookings Institution, February 2022).

31 Ehl, D., "More than mercenaries: Russia's Wagner Group in Africa" (DW, April 2023). Also, Fasanotti in Fn. 30.

policies the CCP government deems sensitive (for example, Xinjiang, Taiwan). While these networks of inauthentic accounts appear to be operating independently in different regions, they in fact exhibit many indicators of coordination.[32] In addition, we have observed significant alignment between the Russian Federation and the PRC, with Chinese profiles and troll networks significantly focused on disseminating pro-Russian propaganda and disinformation in Southeast Asia. Following the Samarkand Summit between Putin and Xi, disinformation circulated by these networks aligned more closely with Russian narratives. Accounts purporting to cover events in Ukraine include erroneous reports of developments on the ground, including annexation "referendums."

8. Attempts by Iran to discredit the West

Iran consistently circulated disinformation and propaganda narratives likely intended to discredit the West, particularly the United States, and Iran's adversaries in the Middle East, particularly Israel. It amplified narratives of Western duplicity, hegemony and interventionism in a likely effort to undermine Western policies and actions. It similarly sought to discredit or counter revelations about the Iranian authorities by Western and diaspora news outlets.[33] Iran faced broader international censure following its violent suppression of anti-government protests, which it claimed were orchestrated by the U.S. and Israel. The Iranian authorities also sought to deny they had delivered military equipment, including drones, to Russia for use in Ukraine.[34]

32 For reference, see Linvill D., and Warren, P., "Understanding the Pro-China Propaganda and Disinformation Tool Set in Xinjiang" (Lawfare, December 1, 2021).
33 Al-Faour N., "How Iran is manipulating the online narrative to cover up its violent crackdown on protests" (Arab News, October 2022).
34 Martinez A., "Iran denies that it is supplying weaponry to Russia for use in Ukraine" (NPR, October 20, 2022)

G7 RRM ACTIVITIES IN 2022

Throughout 2022, the Mechanism stepped up its information sharing activities in partnership with like-minded democracies in order to strengthen collective response to the Russian war of aggression against Ukraine. The G7 RRM also continued providing a platform to discuss evolving national and international approaches.

INFORMATION SHARING

G7 RRM Focal Points met monthly to share updates, analyses, best practices and lessons learned. Thematic priorities included the emergency situation in Ukraine, lessons learned from securing elections in 2021, foreign threats to the rights and freedoms of our citizens, including subnational interference, and more. Focal Points engaged expert stakeholders from academia and civil society to inform our assessments regarding evolving threats (including during elections), the Ukrainian information environment and COVID 19-related disinformation. In addition, working level meetings took place on a monthly basis to foster coordination between support teams on evolving policy issues, including FIMI and hybrid threats.

BUILDING ANALYTICAL CAPACITY

G7 RRM analysts met regularly to share real-time insights and analyses on a range of topics, including FIMI, disinformation regarding the war against Ukraine and Russian information manipulation pertaining to food and energy supplies. Analysts also systematically engaged in joint analysis of the online environment and information sharing facilitated by a U.S.-led Analytics Working Group, established in 2021. The Working Group continued to develop a typology to assess the level of affiliation between state actors and media outlets. In addition, a number of exchanges between G7 RRM analytical teams, including capacity-building activities, took place throughout 2022 to facilitate knowledge and skills transfer, fostering the development of a shared framework for threats analysis to support collective responses.

KNOWLEDGE DEVELOPMENT

The G7 RRM enabled and supported a US-led working group to create the "International Counter-Disinformation Research Agenda" for universities and think-tanks. The Working Group comprised representatives from ten partner nations and governmental organizations, as well as nine U.S. government agencies. The agenda was developed based on surveys and consultations, and the final report has been shared broadly with university and think-tank researchers to enable research on key knowledge gaps and priority topics in support of evidence-informed policy development.

STRENGTHENING COLLECTIVE RESPONSE CAPABILITY

With the start of the Russian war of aggression against Ukraine in February 2022, G7 RRM work shifted into high gear. In addition to supporting analysis of the Ukrainian information environment, monitoring online spaces for Russian disinformation, sharing information and developing strategic communications responses, the G7 RRM partnered with the Carnegie Endowment for International Peace to launch a pilot project aimed at coordinating a multi-stakeholder response in and around Ukraine. Sponsored by Canada, a partnership of representatives from G7 RRM governments, industry and civil society organizations was formed in July to facilitate coordination with Ukrainian authorities with the objective of preserving the integrity of the Ukrainian information environment. The lessons learned from this pilot can be used to inform the manner in which countries and organizations respond to future crises in the information environment. During their meeting in Berlin in October 2022, G7 RRM Focal Points confirmed the need to strengthen collective response capabilities by developing a clear response framework and operational principles. This work will begin in 2023.

IN-FOCUS FEATURES

Canada

Countering Russian disinformation about Ukraine and supporting Canadian research

Countering Russian disinformation about Ukraine was a significant concern for the Government of Canada in 2022. To help counter Russian false narratives and conspiracy theories regarding the illegal invasion, the Government of Canada adopted an assertive public position, issuing dozens of refutations of Russia's falsehoods from the departments of Global Affairs Canada, National Defence, and the Communications Security Establishment.[35] These refutations were published on popular social media platforms in multiple languages and directly debunked false claims. Canada also sanctioned more than 100 Russian entities and individuals complicit in peddling Russian disinformation and propaganda[36] and disseminated advice on how to identify disinformation, misinformation and malinformation online.[37] In August 2022, the Prime Minister also announced the establishment of a dedicated unit within the RRM Canada at Global Affairs to monitor, detect, and counter Russian and other state-sponsored disinformation.[38]

Domestically, the Government of Canada committed more than $5,500,000 to partner with civil society and academia on strengthening non-governmental partners' capacity to counter disinformation. Chief among these efforts is the Canadian Digital Media Research Network, coordinated by the Media Ecosystem Observatory at McGill University and the University of Toronto. This network will produce and support the production of research into the dynamics of Canada's information ecosystem and how this information affects Canadians' attitudes and behaviours. It will also inform Canadians about the quality of information in the information ecosystem, including disinformation narratives, and develop and support the implementation of broader strategies to build Canadians' information resilience and digital literacy.

European Union

Developing dedicated toolboxes for countering hybrid threats, FIMI and protection of academic and research integrity

In December 2022, the EU adopted a framework for coordinated responses to hybrid campaigns (*the EU Hybrid Toolbox*), enabling more informed and targeted action against hybrid influencing based on comprehensive situational awareness and drawing from a wide range of internal and external measures. As a response to foreign interference threats that target higher education institutions and research-performing organizations, the European Commission published a toolkit in January 2022 on how to mitigate foreign interference in research and innovation while safeguarding fundamental values, including academic freedom, integrity and institutional autonomy.

The EEAS continued to advance work on FIMI by strengthening the EU's framework for responding to FIMI through a common definition, analytical methodology and toolbox. There is significant interest from European citizens in learning about FIMI, as evidenced by the more than 2.5 million people who visited the EUvsDisinfo website and the approximately 20 million people who were reached through the EUvsDisinfo social media channels. In the context of Russia's continued use of FIMI in its war against Ukraine and in multilateral forums, including at the United Nations and the UN Security Council, EEAS laid the basis in 2022 for increased cooperation with and within the United Nations. The European Commission works in tandem with the EEAS on strategic communications, monitoring and media literacy to address the nexus of domestic and foreign challenges.

35 Global Affairs Canada, Countering disinformation with facts - Russian invasion of Ukraine.
36 Global Affairs Canada, Sanctions – Russian invasion of Ukraine.
37 Canadian Centre for Cybersecurity, How to identify misinformation, disinformation, and malinformation - Canadian Centre for Cyber Security.
38 Prime Minister of Canada, Prime Minister announces additional support for Ukraine | Prime Minister of Canada.

France

Bolstering government capabilities to detect FIMI and coordinate countermeasures

In 2021, France set up VIGINUM in an effort to strengthen its domestic system to combat information manipulation. The agency monitors and detects foreign digital interference and aims to protect against foreign information manipulation campaigns that seek to harm France and its fundamental interests. The agency operates within a rigorous legal and ethical framework and its activity is reviewed by an ethical and scientific committee composed of legal, diplomatic, scientific and media experts. In 2022, during its first full year of operations, most of the agency's activity focused on protecting the presidential elections (April) and legislative elections (June). VIGINUM also conducted operations to protect the digital public debate around various national or international events that could be exploited by malicious foreign actors.

Building on these efforts, a new Analysis and Strategy (*Veille et Stratégie*) department was created in the Ministry of Foreign Affairs in July 2022 to coordinate the countering of FIMI campaigns, including strategic communications, monitoring of international media spaces (newspaper, radio, TV, social media) and international engagements with like-minded partners. In order to help foster information integrity globally, this department works in close coordination with its diplomatic missions and other units within the Ministry to support press freedom, the protection of journalism abroad and platform regulation (for example, content moderation and algorithmic transparency).

Germany

Improving intergovernmental coordination and public communications to counter hybrid threats

The ongoing pandemic and the Russian war of aggression against Ukraine have underlined that hybrid threats, including disinformation, are one of the central security and sociopolitical challenges facing Germany. Following Russia's invasion of Ukraine, Germany established an inter-ministerial taskforce led by the Federal Ministry of the Interior and Community to foster close cooperation on responses to hybrid threats, especially disinformation. This taskforce coordinates all activities against the deliberate spread of false and misleading information in the context of the war against Ukraine, including strengthening proactive and transparent communication and enhancing societal resilience against threats in the information space.

A federal-state open working group on hybrid threats was also set up under the Federal Ministry of the Interior and Community with the aim of strengthening cooperation between all levels of government. In a cross-level format with representatives of national ministries, federal states, security authorities, municipal umbrella organizations and the intelligence services, this working group focuses on specific aspects of hybrid threats at the subnational levels.

Furthermore, the Federal Foreign Office (FFO) has strengthened Germany's proactive communications globally through its network of more than 220 missions and regional content hubs abroad. By sharing its social media analysis, the FFO ensures a close exchange on disinformation with international partners and in multilateral forums. In addition, the FFO continues to promote societal resilience to disinformation in partner countries, with a special focus on the Baltics and the Western Balkans.

Italy

Strengthening domestic resilience and countering Russian disinformation

Since Russia's invasion of Ukraine, Italy has seen an increase in Russian disinformation narratives spread mostly through official state-affiliated profiles, pro-Kremlin affiliates and influencers in the Italian information ecosystem. Following the imposition of sanctions, Italy shut down two Russian state-sponsored media outlets (*Sputnik* and *RT*) that amplified the Kremlin's narratives and disinformation. Italy also witnessed significant alignment between Russia and the PRC in the information environment, with Chinese profiles and trolls spreading pro-Russian propaganda and disinformation narratives in Southeast Asia.

To counter disinformation, Italy has adopted a series of measures, including raising public awareness and resilience through media campaigns (RAI news), implementing the national Cybersecurity Strategy 2022-2024, contributing

to the development and implementation of the EU *Digital Services Act*, undertaking a risk assessment analysis to protect electoral campaigns, creating a monitoring unit within the Ministry of Foreign Affairs to counter the spread of disinformation, creating an interdepartmental working group on countering hybrid threats, and employing strategic communications to push back against Russian false narratives on specific issues.

Japan

Introducing a new National Security Strategy to address foreign threats, including disinformation

In December 2022, Japan released a new *National Security Strategy*, which outlined approaches aimed at bolstering Japan's responses to information warfare. The Strategy includes the establishment of a new government structure to aggregate and analyze information regarding threats that originate abroad, including disinformation. The new structure aims to strengthen external communications, enhance cooperation with non-governmental agencies and actively employ strategic communications in a coordinated manner across the government to counter these threats.

United Kingdom

Defending Democracy Taskforce

In November 2022, the UK announced the establishment of a new whole-of-government Defending Democracy Taskforce. The Taskforce's mission is to reduce risks with respect to the UK's democratic processes, institutions and society and ensure that they are secure and resilient to threats of foreign interference. The Taskforce brings together relevant government departments, law enforcement and the intelligence agencies and works in close partnership with Parliament. It will also engage with partners outside the central government and Parliament, including international partners, the UK devolved administrations, local government and private and non-governmental organizations.

United States

Countering foreign propaganda and disinformation

The Global Engagement Center (GEC) works with diverse partners to holistically build global resilience to foreign propaganda and disinformation. Using a whole-of-society approach, the GEC builds partner capacity to recognize and counter malign influence, supports research on and exposure of foreign actors' propaganda and disinformation activities and methods, and ensures that high-quality, independent and factual information is available to vulnerable audiences. Since 2019, the GEC has strengthened the capacity of individuals, civil society, academia, media and partner organizations in more than 70 countries to build global resilience to propaganda and disinformation. The GEC leverages its unit grant-making authorities and various funding mechanisms to facilitate localized programming to support these efforts. Its public facing reports may be found on state.gov/disarming-disinformation.

OBSERVERS

Australia

New taskforces established to strengthen national resilience and democracy

On December 8, 2022, the Australian government announced the establishment of two taskforces within the Department of Home Affairs to bolster Australia's resilience to both enduring and emerging challenges to national security: the National Resilience Taskforce (NRT) and the Strengthening Democracy Taskforce (SDT). The NRT is working to enhance Australia's national resilience by examining Australia's increasing exposure and vulnerability to nationally significant crises and ensuring the Australian government has the necessary policy, legislation and capability to manage increasingly complex and concurrent national crises, including those exacerbated by climate change.

The SDT is working to identify practical initiatives for safeguarding and sustaining Australia's democratic resilience, both in the near and long term. The Taskforce draws on extensive data, evidence, research and emerging practice to identify the most significant strengthening (democratizing) and weakening (anti-democratizing) forces that can be bolstered and disrupted respectively in order to have the greatest potential for impact. The taskforce will leverage the extensive range of measures already in place or in development that support a strong and resilient democracy.

These taskforces form complementary lines of effort positively reinforcing Australia's prosperity, security and sovereignty.

New Zealand

Supporting higher education: "Trusted Research – Protective Security Requirements"

In September 2022, the national body representing Aotearoa New Zealand's university sector published a guide for how senior leaders should consider their university's ongoing response to the ever-changing and increasingly complex geopolitical environment. For universities, this means considering how they manage risks related to research activities (especially those that involve international partnerships) in the areas of applied research, emerging dual-use or culturally sensitive technologies research, or their applications that could result in harm or reputational damage. The recommended approach to policy, planning and risk assessment focuses on managing potential risks and protecting people, assets and reputation while maintaining a strong commitment to upholding academic freedom and promoting the broad benefits of international collaboration.

North Atlantic Treaty Organization (NATO)

Countering hostile information activities, including disinformation

NATO made an unprecedented effort at pre-bunking Russia's narratives on the invasion of Ukraine in order to help make audiences more resilient to disinformation, bolster alliance unity and maintain support for Ukraine.

Starting in the autumn of 2021, NATO deliberately declassified significant amounts of intelligence on Russia's military build-up and its plans for the full-fledged invasion of Ukraine, including potential false flag operations. This was done in coordination with Allies in order to call out and deter Russia's actions and increase understanding, resilience and support in our public audiences. This was done systematically through the public communications of the NATO Secretary General and senior officials, as well as through a range of background briefings. In 2022, NATO maintained this approach, fostering unity among Allied publics about Russian activities, facilitating continued support for Ukraine and pre-bunking Russian disinformation instead of debunking once it gained traction. Furthermore, NATO consistently tracked hostile narratives, de-bunking and pre-bunking the main Russian lies about NATO through proactive communications and its *Setting the Record Straight* platform, which was set up in 2014 after Russia's illegal annexation of Crimea.

Sweden

The Psychological Defence Agency: first year of operations

Established in January 2022, the Swedish Psychological Defence Agency is tasked with identifying, analyzing, preventing and responding to foreign malign information influence and interference directed at Sweden or Swedish interests. The Agency has both an operational role

and a mandate to strengthen societal resilience against foreign interference.

As a result of the increase in Russian disinformation campaigns following the invasion of Ukraine and Sweden's decision to apply for NATO membership, the Agency initiated a nationwide information campaign ahead of Sweden's general elections to raise awareness of disinformation and advise citizens to remain vigilant. Throughout 2022, Sweden was subjected to a large-scale, coordinated information influence campaign claiming that Muslim children and families were being systematically subjected to abuse by Swedish authorities. The campaign is still ongoing and spreading globally, although now on a smaller scale. Several countermeasures were initiated by the government, including multi-stakeholder strategic communication activities.

The Netherlands

Advancing a "whole-of-government" approach to countering hybrid threats

The Netherlands has continued working on an inter-agency structure to facilitate a whole-of-government approach to countering hybrid threats, including developing a training module for civil servants to increase their knowledge and understanding of this kind of threat. In addition, the Netherlands Intelligence Services and National Coordinator for Counterterrorism and Security published the second comprehensive National State Threat Assessment in November 2022. The assessment paid special attention to the way in which the social and political stability of the Netherlands was being impacted by state-sponsored interference in addition to the increased threats to economic security. Parliament was informed about both processes in a letter on state threats signed by nine ministers, which highlighted main principles, approaches and focus areas to counter hybrid threats, including cooperation with international partners. In a separate letter to Parliament on countering disinformation, specific attention was paid to countering foreign information manipulation and interference FIMI.