G7 GERMANY
2022

G7
RAPID RESPONSE MECHANISM
PROTECTING DEMOCRACY

Annual Report 2021

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 partnership with G7 RRM members and observers, including Australia, New Zealand, NATO, the Netherlands and Sweden.

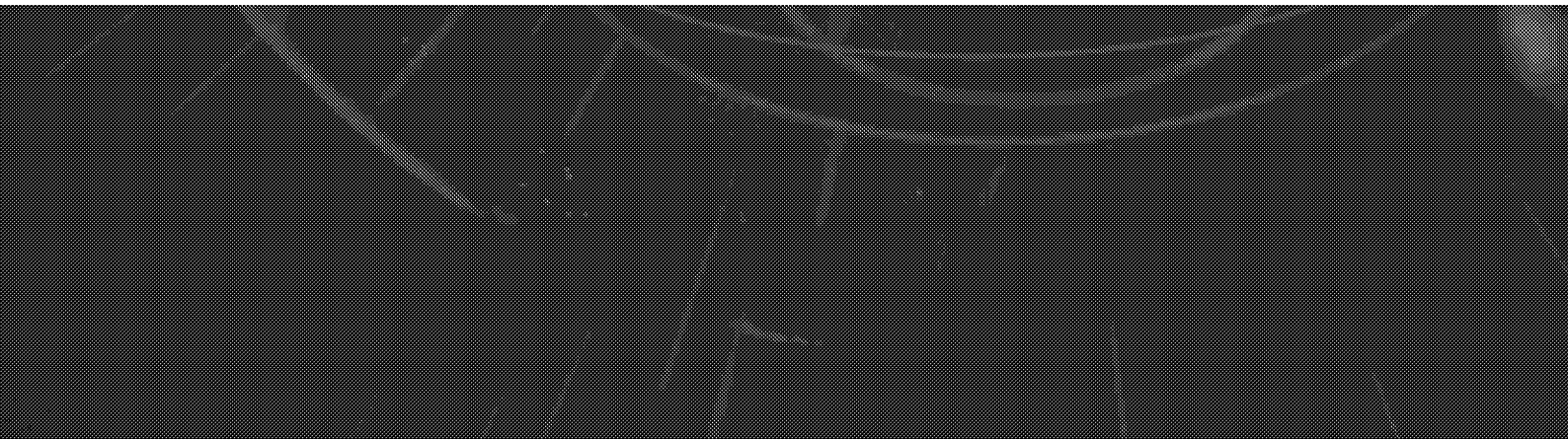
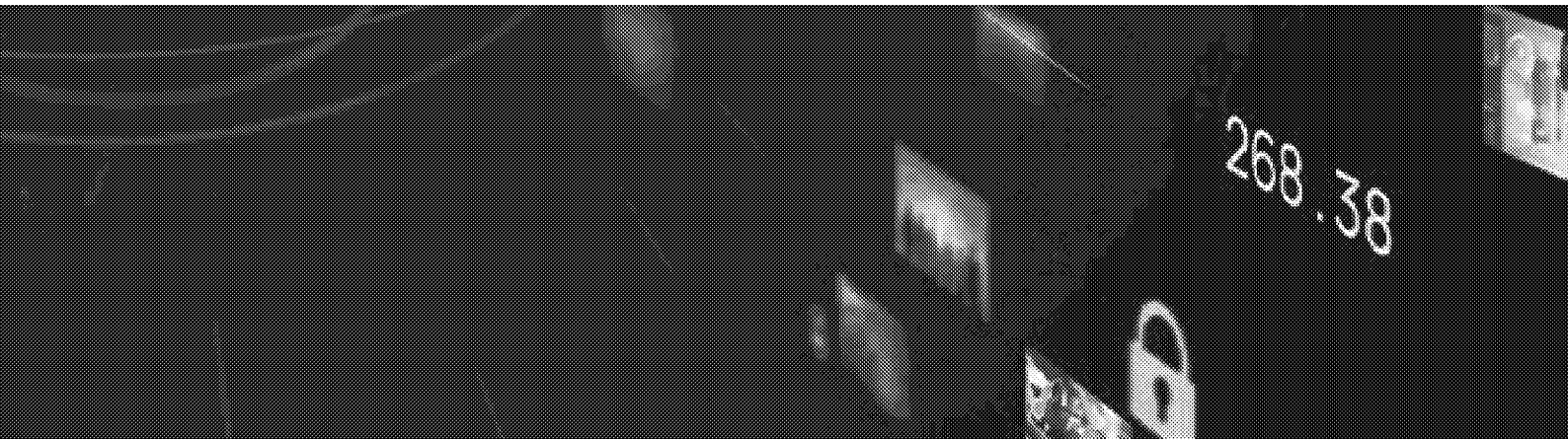


TABLE OF CONTENTS



G7 GERMANY
2022

G7 RAPID RESPONSE MECHANISM

PROTECTING DEMOCRACY

INTRODUCTION

At the 2018 G7 Summit in Charlevoix, leaders established the G7 Rapid Response Mechanism (G7 RRM) to strengthen coordination 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, and 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 Mechanism on an ongoing basis.

During the 2021 G7 Foreign and Development Ministers meeting in London, foreign ministers committed to the G7 RRM producing annual thematic reports on different aspects of the evolving threat landscape and possible responses in order to promote public awareness and resilience.

At the request of G7 foreign ministers, this first annual report focuses on disinformation as an increasingly prominent vector of foreign interference threatening democracies. The report provides an overview of the disinformation threat landscape, including prominent events and developments in 2021, emerging trends and the implications for response options that include safeguards for respecting freedom of opinion and expression. It also outlines broader G7 RRM activities over the past year and provides a look ahead for G7 RRM priorities in 2022. Finally, the report includes various examples of initiatives undertaken by G7 RRM members—often informed by mutual sharing of information and best practices—to counter foreign threats to democracies.

DISINFORMATION THREAT LANDSCAPE 2021

CONTEXT

The threat to democracies from hostile state activity persisted and evolved in 2021, with disinformation constituting a key vector.[1] Acting directly, through state and affiliated media and influencers, or indirectly, through proxies, a number of states continued to create, spread or amplify disinformation to advance their strategic objectives.

While there is no internationally agreed definition of disinformation, it commonly refers to false or misleading information that is spread deliberately, as opposed to misinformation, which refers to false or misleading information that is spread unwittingly. Disinformation can be employed by an actor, foreign or domestic, to achieve political, ideological, economic or military objectives. Disinformation is a term often employed as shorthand for the broader challenge of information manipulation, which, in addition to false information, includes tactics such as partial or full omission of facts, doctored audio/visual content, inauthentic amplification of narratives, trolling, and efforts to censor or coerce self-censorship of information—all aiming to distort the public's perception of reality.[2] For the purposes of this report, we use the term "disinformation" to refer to all efforts to deceive in the information environment, with a focus on disinformation propagated by state actors and their proxies.

Disinformation thrived in the context of COVID-19, as the global pandemic provided fertile ground for hostile state actors, acting directly or through proxies, to manipulate the information environment.[3] Life continued to shift online, with more eyes on screens than ever before accessing an unprecedented volume of information, both accurate and inaccurate, resulting in what has been popularly termed an "infodemic."[4] This rendered it increasingly difficult to distinguish manipulative content and tactics employed by hostile state actors or their proxies from authentic information. Moreover, these actors leveraged the pandemic-related hardships and frustrations experienced by individuals and communities, including uneven social and economic impact, to introduce and amplify narratives aimed at undermining the credibility of democratic governments and further polarizing democratic societies.

KEY EVENTS AND DEVELOPMENTS

Issues related to disinformation continued to dominate headlines and policy agendas in G7 countries and globally throughout 2021, as hostile state activities manifested themselves in relation to the ongoing pandemic, national and sub-national elections, and other events of global importance.

The efforts of governments and public health authorities to confront successive **waves of COVID-19** were frustrated by a steady stream of hostile state-sponsored disinformation campaigns, often inspiring and/or amplifying domestic disinformation. Since the beginning of the pandemic, hostile state actors have been manipulating information to sow doubt about the origins of the virus and the means required to counter it; discredit democratic responses; undermine public health measures; and promote their own responses as superior.[5] We saw hostile state actors—drawing on one another's campaigns—amplify false allegations that COVID-19 originated in a U.S. bioweapons lab or was designed by Washington to weaken other countries.[6] We also saw them spread misleading messages regarding the provision of personal protective equipment (PPE) to third countries to weaken the cohesion and solidarity of democratic donor countries and to downplay the importance of aid provided by democratic countries.

1 See the following Canadian sources: Foreign Interference Threats to Canada's Democratic Process (July 2021) and Cyber Threats to Canada's Democratic Process (July 2021 update)
2 Combating Information Manipulation: A Playbook for Elections and Beyond (International Republican Institute, September 2021)
3 For example, see the EU External Action Service communication on COVID-19 disinformation
4 For more information, tools and guidelines for countering the health-related infodemic, consult the World Health Organisation
5 Superspreaders of Malign and Subversive Information on COVID-19 (Rand Corporation, 2021).
6 Weaponized: How rumors about COVID-19's origins led to a narrative arms race (DFR Lab, February 2021).

Since early 2021, we have seen foreign state-disinformation campaigns aimed at both undermining confidence in vaccines produced in democratic countries and promoting the states' own products.[7] We have also seen hostile state actors actively amplifying anti-vaccine sentiment, including by hosting conspiracy theorists on state-linked media channels.[8] As a result, these disinformation campaigns contributed to the erosion of confidence in measures implemented by democratic governments, and, to the extent they undermined the public's trust in the advice of public health authorities, also put lives at risk.

Foreign state-disinformation campaigns were also a prominent feature of various **national and sub-national elections**, including in G7 countries, with the aim of influencing electoral outcomes, undermining trust in democratic processes and institutions, and driving polarization. While disinformation is not unique to elections, election campaigns are often the flashpoints around which hostile state activities, including disinformation, intensify. See the box below for an overview of the actions G7 RRM governments adopted to help safeguard their elections.

GOVERNMENT EFFORTS TO SAFEGUARD NATIONAL ELECTIONS IN 2021

In March 2021, the **United States** federal government released 2 reports on foreign interference in the 2020 presidential election. The Intelligence Community Assessment on Foreign Threats to 2020 Elections noted that there were no indications that any foreign actor attempted to alter any technical aspect of the voting process but that some foreign actors spread false or inflated claims about alleged compromises of voting systems to undermine public confidence in election processes and results. The joint Department of Justice and Department of Homeland Security report on foreign interference identified no evidence that any foreign government-affiliated actor prevented voting or altered any technical aspect of the voting process, despite broad campaigns by Russia and Iran targeting multiple critical infrastructure sectors that did compromise the security of several networks that managed some election functions. Federal intelligence, law enforcement and national security agencies continued to monitor foreign threat activity, share information, and provide election security assistance to state and local election authorities and the private sector as they prepare for federal mid-term elections in 2022.

Several regional elections and the federal election took place in **Germany** in 2021. With hostile activities in the information and cyber domain on the rise, the German federal government set up a dedicated cooperative platform to enhance existing capabilities and cooperative structures to counter disinformation and other forms of foreign interference. Through this platform, the federal Ministry of the Interior coordinated all measures for prevention, detection and response related to hostile activities. Engagement and information sharing with different national stakeholders and international partners, as well as close cooperation within G7, EU and NATO, further strengthened the government's efforts. Only limited malign influence activities from foreign states ultimately materialized. There were, for instance, a number of cyberattacks against German politicians, which the German federal government attributed to Russia in early September 2021. In particular, extensive awareness-raising measures for the general public and specific target groups as well as coordinated governmental communicative measures contributed to the successful protection of the election from hybrid threats.

The Government of **Canada** updated and activated its Plan to Protect Canada's Democracy for Canada's 2021 general election. This included the Critical Election Incident Public Protocol, a panel of non-partisan senior civil servants mandated to inform the public during the caretaker period, should influence operations and interference threaten Canada's ability to hold a free and fair election. The Plan also included the Canada Declaration on Electoral Integrity Online, a voluntary code between the government and social media companies to support principles of integrity, transparency and authenticity. Throughout the election, the Security and Intelligence Threats to Elections (SITE) Task Force actively monitored for indicators of foreign information manipulation and interference, among other foreign threats. Canada's security and intelligence agencies repeatedly warned in advance of the election of hostile actors' efforts to inject and amplify false and misleading information on online platforms to advance their specific agendas, including attempts to undermine Canada's democratic processes and interfere in elections. Ultimately, the Government of Canada did not detect interference activities that compromised the integrity of the election.

General elections for the House of Representatives were held in **Japan** in October 2021. The Government of Japan remained vigilant against possible malicious cyber activities threatening democracy, including spreading of disinformation about the elections by foreign actors. In parallel, a fact-checking initiative was implemented by a non-governmental organization aiming to protect society from mis/disinformation, which helped to monitor the information environment during elections and raise public awareness through its website. Ultimately, no malign influence activities by foreign states were reported.

7 For example, see EUvsDisinfo communications providing regular updates on the evolving information manipulation narratives in the pro-Kremlin media.

8 Pillars of Russia's Disinformation and Propaganda Ecosystem (Global Engagement Center, August 2020).

Throughout 2021, other noteworthy instances of disinformation included the Belarus-manufactured border crisis; efforts by the People's Republic of China (PRC) to pressure Taiwan; narratives on tightening security restrictions in Hong Kong; and the manipulative portrayal of the human rights situation in Tibet and Xinjiang through various means, including suppression of voices and information.[9]

Since the 2014 Maidan Revolution in Ukraine and Russia's illegal annexation of Crimea, the Kremlin has waged relentless disinformation campaigns against Ukraine. These campaigns have targeted Russian-speaking populations in Ukraine, but have also been wielded to influence neighbouring countries and international audiences more generally.[10] After November 2021, the Kremlin's campaign intensified to support military build-up on the ground and pave the way for an escalation of aggression. This campaign falsely characterized the Ukrainian government as weak, corrupt and a pawn of the West. It claimed that the Ukrainian government was committing atrocities against civilians in Donbas and that Ukraine was a historical part of Russia. It advanced a false narrative casting Western democracies as the aggressors responsible for Russia's unprecedented build-up of troops on Ukraine's borders and Russia as an innocent party acting in self-defence, open to diplomacy. The Kremlin continued to spread a range of false claims to advance its objectives in tandem with its military encroachment, including about the capability and intent of the Ukrainian government to develop and deploy chemical, bacteriological, radiological and nuclear weapons.

In response, the G7 and partner democracies have strived to counter Russia's disinformation[11] by boosting support for the G7 RRM; sharing real-time assessments; coordinating communication approaches; imposing sanctions on individuals and entities linked to Russian violations of international law; and exposing those who spread Russia's disinformation at the behest of its intelligence services.[12] Some countries have also provided capacity-building support to Ukrainian civil society organizations fighting Russian disinformation and protecting the integrity of the Ukrainian information environment.

EVOLVING TRENDS

The G7 RRM identified the following 12 noteworthy trends in foreign state-sponsored information manipulation activities in 2021 where disinformation tactics played a key role. These trends were identified through primary and secondary research across the G7 RRM community and have important implications for our policy and legislative efforts to respond to foreign threats.

1. Foreign state actors, such as Russia and the PRC in particular, and, to some extent, the Islamic Republic of Iran, among others, leveraged **divisive issues and social cleavages** to polarize societies, influence political outcomes, and undermine democratic institutions and processes.[13] These issues and divisions were exacerbated by stresses related to the impact and management of the COVID-19 pandemic.
2. In an attempt to lend legitimacy to their messages in different contexts, foreign state actors often co-opted or leveraged **key influencers**, such as celebrities, traditional media and public figures to validate or amplify their content.[14]

---

9 Xinjiang Nylon: The anatomy of a coordinated inauthentic influence operation (Clemson University Media Forensics Hub, December 2021).

10 Russian Hybrid Threats Report: Kremlin pushes claims about Ukrainian offensive, 'junk' weapons from West (DFR Lab, January 2022).

11 Fact vs. Fiction: Russian Disinformation on Ukraine (U.S. Department of State, January 2022); Disinformation About the Current Russia-Ukraine Conflict – Seven Myths Debunked (East StratCom Task Force, January 2022); NATO-Russia: Setting the Record Straight (NATO Public Diplomacy Division, January 2022)

12 Taking Action to Expose and Disrupt Russia's Destabilization Campaign in Ukraine (U.S. Department of State, January 2022)

13 Threat Report: Combating Influence Operations (Facebook, May 2021). See also, Pinault, Nicolas (March 25, 2021), "Macron Warns Turkey Not to Interfere in French Elections", Voice of America. See Foreign Threats to the 2020 US Federal Elections (U.S. National Intelligence Council, March 2021) for the analysis of Russia's and Iran's covert influence campaigns targeting elections integrity. With regard to PRC activities, see Superspreaders of Malign and Subversive Information on COVID-19 (Rand Corporation, 2021) and China's Influence in Southeastern, Central, and Eastern Europe: Vulnerabilities and Resilience in Four Countries (Carnegie Endowment, October 13, 2021). For additional references on Iran's activities, see Iranian Influence Networks in the United Kingdom: Audit and Analysis (Henry Jackson Society, June 7, 2021) and Designation of Iranian Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election (U.S. State Department, November 18, 2021).

14 Culliford, Elizabeth (August 10, 2021), "Facebook removes Russian network that targeted influencers to peddle anti-vax messages", Reuters. Also, see Meta's report on the network removal: July 2021 Coordinated Inauthentic Behaviour Report.

3. A range of **disruptive non-state actors** played a growing role in spreading foreign state-sponsored disinformation.[15] These disruptive non-state actors include transnational extremist movements, foreign state-affiliated proxies and private profit-driven actors who spread disinformation for hire.[16] These actors often manipulated information and amplified falsehoods in parallel with or at the behest of foreign state actors.

4. Different **diaspora communities** continued to experience direct and indirect pressures through censorship, disinformation campaigns and covert manipulation of information from state actors in their country of origin aimed at curbing dissent or supporting the country of origin's policies.[17]

5. Both state and non-state actors spread **gendered and identity-based disinformation** (race, ethnicity, sexual orientation, etc.) about political leaders, journalists and other public figures. Recent examples of these attacks include disinformation campaigns against German Foreign Minister Annalena Baerbock,[18] U.S. Vice-President Kamala Harris[19] and Belarusian pro-democracy leader Sviatlana Tsikhanouskaya.[20] The deceptive messages in such campaigns often included degrading narratives, coded language to circumvent moderations systems, and inaccurate text or doctored/misattributed images and videos that were meant to discourage targets from participating in public life.

6. Foreign state actors targeted **non-state bodies and forums at sub-national levels**, including corporate entities, civil society, and educational and scientific or research institutions, to gain undue influence, obtain critical information and prime target audiences to on-going disinformation campaigns.[21]

7. Foreign state actors, such as Russia, continued to **use state-controlled or state-affiliated media** and leveraged proxy news sites, also known as "**grey news sites**,"[22] to manipulate public discourse and engage with target audiences. They deployed this tactic in democratic countries, especially during elections. By doing so, they blurred the line between public diplomacy and covert manipulation of information.

8. The PRC's "**wolf warrior diplomacy**" has come to the fore in recent years, with senior officials posting aggressive viewpoints, and sometimes disinformation, on social media. These "wolf warriors" created content or amplified state and affiliated media content in their social media feeds. In turn, these state and affiliated media also used "wolf warrior" posts as fodder in influence campaigns, increasing content sources for both amplification and trolling by coordinated networks of social media accounts.[23]

9. While the disinformation tactics and techniques deployed by foreign state actors differed in their sophistication, a growing imitation of Russia's tactics has been observed, particularly by the PRC. Russia's model is characterized by coordination of disinformation campaigns and other destabilizing actions across a range of hybrid means and capabilities.[24]

10. Foreign state actors conducted influence campaigns across **different social media platforms and channels**, including closed and encrypted channels. This posed numerous challenges for governments, civil society, online platforms and academic researchers in their efforts to detect, coordinate and combat the spread of disinformation and measure its scale and intent.

11. **Alternative social media platforms** continued to provide refuge to non-state, ideologically motivated actors who were removed from mainstream platforms or "de-platformed" for violations of terms of service. Some of these alternative platforms are directly linked to or influenced by hostile state actors.[25] On such platforms, accurate and reliable information is often crowded out by hate speech,

15 While the G7 RRM mandate focuses on monitoring for and countering threats to democracy from foreign state actors, we note the complex web of actors operating across borders and issues.
16 Disinformation-For-Hire: The Pollution of News Ecosystems and Erosion of Public Trust (Center for International Media Assistance, December 2021).
17 Disinformation, stigma and Chinese diaspora: policy guidance for Australia (First Draft News, August 2021).
18 Targeting Baerbock: Gendered Disinformation in Germany's 2021 Federal Election (Alliance for Securing Democracy, August 2021).
19 Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online (Wilson Center, January 2021)
20 See EUvsDisinfo analyses of disinformation attacks against Tsikhanouskaya.
21 Big fish in small ponds: China's subnational diplomacy in Europe (Merics and Heinrich Böll-Stiftung, November 2021).
22 These websites may appear as legitimate alternative news sources in an attempt to blur attribution of the ultimate source or state affiliation. Often, in order to increase the perception of credibility, they would publish accurate information alongside disinformation. See the US Global Engagement Center's report on Pillars of Russia's Disinformation and Propaganda Ecosystem (August 2020; updated in January 2022).
23 Growling Back at the West (China Media Project, University of Hong Kong Journalism and Media Studies Centre, August 2021).
24 Chinese Influence Operations: A Machiavellian Moment (L'Institut de Recherche Stratégique de l'École Militaire, October 2021).
25 Posing as Patriots (Graphika, June 2021).

disinformation and false conspiracy-related narratives that are amplified by hostile states, political fringe groups and profit- or influence-seekers.

12. In 2021, foreign governments continued to research and develop advanced **"deepfake" technology**, which enables the rapid generation of synthetic video, audio and text, and can be used for malign purposes. Deepfakes were employed at a low scale in support of foreign influence campaigns during the 2020 U.S. elections, and research advancements will likely make these technologies more sophisticated in years to come.[26]

IMPLICATIONS

These trends demonstrate that foreign state-sponsored disinformation online and offline—just one tool in the broader arsenal of hostile state activity—is an increasingly transnational, multi-dimensional and cross-platform challenge. In this context, it is difficult to distinguish between foreign and domestic actors; both are growing in number and their tactics in complexity. At the same time, the boundaries between public diplomacy on one hand and malign information manipulation on the other are also blurring.

These challenges are complicating efforts aimed at countering information manipulation by hostile state actors—from identifying and assessing threats to designing effective response options while respecting freedom of expression. For example, attribution is increasingly difficult to achieve with a high degree of certainty. Measuring the real or potential impact of disinformation is also challenging. This, in turn, tests our ability to develop effective and responsible response options. And, since those who engage in disinformation campaigns conduct myriad activities across time and space, responding to disinformation as a single event misses the point. It also underscores the broader societal challenge of fostering resilience and a healthy skepticism of unverified claims, while also ensuring respect for the integrity of facts and science.

Meanwhile, many of the foreign states responsible for disinformation are increasingly investing resources to exercise control over their own domestic information environments; draconian legislation enshrines state controls over the free flow and content of information and limits the exercise of a range of human rights and fundamental freedoms, including freedom of expression. The most recent and egregious example of this trend is the Kremlin's clamp-down on independent media in Russia, accompanied by restrictions and blocking of social media platforms and criminalization of opposition to the war. These states, with Russia at the forefront, are also actively seeking to shape multilateral initiatives, at the United Nations[27] and elsewhere, with a view to ensuring that any normative and legal frameworks developed with respect to the global information environment are fashioned in their own image.

As our combined understanding of the evolving threats stemming from disinformation grows, so, too, does momentum among democracies to coordinate through mechanisms such as the G7 RRM. This momentum is informed by a keen understanding that policy responses must be evidence-based and should be proportional, and that countering information manipulation in all its forms effectively requires a networked approach guided by democratic values and principles.

26 Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations (Federal Bureau of Investigation, March 2021).

27 Countering disinformation and promotion and protection of human rights and fundamental freedoms (UNGA resolution A/RES/76/227, November 2021)

G7 RRM ACTIVITIES IN 2021

The G7 RRM was guided by its 2021 Action Plan (see Annex 1). The Plan aimed to strengthen G7 RRM members' and observers' shared understanding of and response to foreign threats to democracy. Throughout 2021, the Mechanism continued to enable real-time information sharing on disinformation and other foreign malign influence tactics and threats, and served as a platform to discuss national approaches and coordinated responses.

INFORMATION SHARING

G7 RRM Focal Points met monthly to share information, best practices and lessons learned. Thematic priorities included foreign agent registries, foreign threats to the rights and freedoms of our citizens, engagement with social media platforms, and elections security. Several meetings engaged academia and civil society to speak to evolving threats, including COVID 19-related disinformation; convergence of practices and messaging among hostile state actors; and, in preparation for the G7 RRM 2022 Action Plan, key trends and priorities in countering foreign threats to democracy. These discussions contributed to a shared understanding of evolving foreign threats, present and future, and informed national approaches to countering them. Canada continued to produce a monthly digital newsletter, the Wire, that aims to share insights and information about new developments and projects and identify potential partners working in countering foreign malign influence and interference operations.

BUILDING ANALYTICAL CAPACITY

G7 RRM analysts met regularly to share real-time insights and analysis, including on disinformation associated with unfolding developments such as the Belarus migration crisis. They also systematically engaged in online analytics and information sharing facilitated by the U.S. Department of State Global Engagement Center. To strengthen G7 RRM analytical capacity for assessing and countering disinformation, a U.S.-led Analytics Working Group was established. It began developing a typology to assess the level of affiliation between state actors and media outlets. This shared framework will ultimately enable G7 members and observers to employ common terminology in analytical reporting and help guide counter-messaging approaches. This work will continue in 2022.

STRENGTHENING RESPONSE POSTURE

The European External Action Service (EEAS) led a Terminology Working Group with a view to fostering a common conceptual understanding of threats to the information environment and to establish a basis for enabling coordinated responses. The working group identified the core characteristics of foreign information manipulation and interference (FIMI), with a focus on the coordinated, intentional and harmful manipulative behaviour of foreign actors and their proxies. This work will continue in 2022, in collaboration with the Analytics Working Group, with the aim of socializing a shared vocabulary and corresponding analytical methodology across the G7 RRM. In addition, Canada launched a research project aimed at mapping existing national and international frameworks to countering disinformation to assess possible foundations for subsequent work on norms development with respect to foreign information manipulation and interference.

FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

In 2021, the G7 RRM established a Working Group on Terminology with a view to distinguishing between legitimate and illegitimate state and state-sponsored behaviour in the information environment. Led by the EEAS, members discussed the concept of foreign information manipulation and interference (FIMI) to capture the constantly evolving tactics, techniques and procedures (TTPs) deployed by state actors and their proxies to exercise malign influence in the information environment.

The FIMI concept describes patterns of behaviour that negatively impact or have the potential to negatively impact values, procedures and political processes. Such activities are manipulative in character and are conducted in an intentional and coordinated manner by a range of actors, from state to non-state, including their proxies inside and outside of their own territory. It includes all tactics used to manipulate information. The adoption of the FIMI concept as a working definition allows G7 RRM members to develop a common operational vocabulary that focuses on malicious behaviours on- and offline in order to enhance shared understanding, promote cataloguing and enable the disruption of hostile TTPs.

EXPANSION AND COLLABORATION

The G7 RRM welcomed NATO and Sweden as observers with a view to leveraging expertise and avoiding duplication. The G7 RRM coordinated with other international forums working to counter hostile information activities by foreign states, including disinformation. The Mechanism also worked with a range of stakeholders throughout the year to bring insight, increase public awareness of and resilience to disinformation, and coordinate research and capacity-building programming for maximum effect.

IN-FOCUS FEATURES

Canada

Building resilience to disinformation through research and digital media and civic literacy

Canada builds societal resilience to disinformation through the Digital Citizen Contribution Program (DCCP), which funds third-party organizations to better understand disinformation in the Canadian context and undertake digital media and civic literacy activities. In 2021 to 2022, the DCCP funded 15 projects worth $1.3 million to understand the role of algorithms in spreading disinformation on mainstream and fringe platforms, to assess the transnational spread of disinformation through diaspora communities, and to study disproportionate impacts on Indigenous and non-English language communities. The DCCP also funded initiatives targeting COVID-19 disinformation through digital media and civic literacy, supported a Digital Media Literacy Week run by the Canadian organization MediaSmarts, and convened a Citizens' Assembly from across the country to debate and provide recommendations for Canada's approach to combatting disinformation.

France

A new agency to fight foreign digital interferences aimed at undermining our democratic institutions

Like many of its main European and international partners, France has chosen to strengthen its system for combating information manipulation by setting up a service designed to protect democracy against foreign digital interference. This service, established in July 2021, is called Viginum (Vigilance et Protection Contre les Ingérences Numériques Étrangères [Vigilance and Protection Against Foreign Digital Interference]) and was launched under the supervision of the Secretary General of Defense and Homeland Security (SGDSN), under the auspices of the Prime Minister's Office. Viginum has one clear mission: identifying disinformation campaigns that directly or indirectly involve a foreign state or a foreign non-state entity aimed at the artificial or automated, massive and deliberate dissemination, through an online public communication service, of manifestly inaccurate or misleading accusations aimed at harming the fundamental interests of the state. The agency will be operational by the end of 2022 and use information collected from publicly accessible sources only. A scientific and ethics committee will supervise the agency's work.

Germany

A nascent centre for strategy, analysis and resilience

The Federal Ministry of the Interior and Community (BMI) has been in charge of coordinating the whole-of-government approach to countering hybrid threats since July 2019. An interdepartmental management-level working group, chaired by the BMI Permanent Secretary responsible for countering hybrid threats, was set up to advance joint planning and coordination. A milestone for this interdepartmental cooperation in detecting and countering hybrid threats was achieved in January 2021 when a dedicated interdepartmental unit began testing and preparations for the launch of a future federal centre for strategy, analysis and resilience (SAR). Led by the BMI, the nascent SAR also includes representatives from the Federal Foreign Office and the Federal Ministry of Defence.

Italy

Conference on countering disinformation

The combined effects of disinformation, misinformation and mal-information pose an increasingly serious challenge to Italian national security. In the second half of 2021, the Italian Ministry of Foreign Affairs started to plan an event for the beginning of February 2022, devoted to the issue of preventing and countering disinformation at the national level. The aim is to reinforce the awareness and resilience of the public and private sectors and to enhance contributions to national and international

policies and strategies against disinformation. The sharing of information and lessons learned on current threats, how to react, and the reforms, including of the legal framework, necessary to be more effective in preventing, mitigating and countering disinformation will be part of the discussion. This multi-stakeholder event is the result of the cooperation established between the Italian MFA and the Italian Digital Media Observatory.

Japan

Detection of increasing sophistication of foreign influence operations

As a member of the Japanese intelligence community, the Public Security Intelligence Agency (PSIA) collects and analyzes information activities conducted by foreign countries, including possible operations aimed at Japan's democratic process. The Agency has observed that foreign external publicity activities using social networking services (SNS) have become more sophisticated and radical, including regarding issues related to the spread of COVID-19 infection.

United Kingdom

U.K. Shared Values Campaign (This is democracy)

The Shared Values campaign is a counter-brand campaign that brings together a global partnership of democratic governments and organizations to promote positive messages about the enduring strength and global leadership of the partnership and the commonly held liberal values that bind them together. Partners to the campaign, who have joined activity on a modular basis, are Canada, Denmark, Estonia, Finland, Germany, Lithuania, Latvia, Slovakia, Ukraine, United Kingdom and the United States, the Westminster Foundation for Democracy and the Community of Democracies. Since launch, the global level activity has achieved an organic reach of 33 million people across 163 countries, with 84 civil society organizations organically sharing the content. At local level, the campaign targeted "democracy-hesitant audiences" vulnerable to disinformation undermining democracy in Eastern Europe. Post-campaign results showed an 11% increase in audience perception of democracy as "quite important" a 2% increase in audience preference for democratic governments, a 16% increase in awareness of healthy democratic behaviours and an average campaign recognition rate of 20% across the region.

United States

Global Engagement Center publishes counter-disinformation dispatches

The GEC releases exposure reports and counter-disinformation dispatches that summarize lessons learned about disinformation and how to counter it based on the experiences of frontline counter-disinformation practitioners, for the benefit of those in other countries who are newly engaged in this issue. The dispatches' readership has grown to include a large community of government officials, civil society leaders and academics around the world. Previous dispatches have covered COVID disinformation, lessons on making debunking more effective, the underlying strategy and historical context of Russia's disinformation tactics, and the role of state-controlled agents of influence in disinformation operations. The dispatches are available on the website www.state.gov/disarming-disinformation, and here in English, and some issues are also available in Russian, Spanish, French and Arabic. To be added to the distribution list for future counter-disinformation dispatches, please email us.

Australia

ASIO disrupts a foreign interference plot

Recently, the Australian Security Intelligence Organisation (ASIO) detected and disrupted a foreign interference plot in the lead-up to an election in Australia. An individual who maintained direct and deep connections with a foreign government and its intelligence agencies sought to shape the political scene to benefit the foreign power. The deliberate deceit and secrecy about the foreign government connection took the case into the realm of foreign interference. ASIO's intervention ensured the plan was not executed, and harm was avoided.

New Zealand

Espionage and foreign interference threats: Security advice for members of the New Zealand Parliament and locally elected representatives

Raising awareness about the potential impact of foreign interference in New Zealand's economy, democracy and international reputation remains an area of high priority and focus for the New Zealand government. We have seen indicators concerning relationship-building and donation activity by state actors and their proxies spanning the political spectrum at both a central and local government level. In March 2021, a booklet entitled Espionage and Foreign Interference Threats: Security Advice for members of the New Zealand Parliament and Locally Elected Representatives was publicly released under the banner of the New Zealand Protective Security Requirements (PSR) Framework. The booklet has supported the New Zealand government's work to raise awareness of foreign interference, with briefings to central and local government politicians about how they may be targeted and exploited, and what they can do to protect themselves.

Sweden

Sweden establishes the Psychological Defence Agency

Sweden, who joined the RRM as an observer in 2021, has established a new government agency—the Swedish Psychological Defence Agency—tasked with identifying, analyzing, preventing and responding to undue information influence and other misleading information directed at Sweden or Swedish interests, both nationally and internationally. It will have an operational role, but, importantly, also the mandate to build capacity broadly in Swedish society.

European External Action Service

A multi-stakeholder approach to countering foreign information manipulation and interference

In 2021, the EEAS—in close cooperation with other EU institutions—has led work on a comprehensive framework to counter foreign information manipulation and interference (FIMI), based on 3 dimensions: a common conceptual definition of the threat with all its facets; a common analytical framework and methodology; and an updated toolbox to address foreign information manipulation and interference.[28] The Strategic Communications Team, with its dedicated task forces for the Eastern European neighbourhood, western Balkans and the South, has been working on improved situational awareness and exposing of FIMI activities, and contributed to strengthened societal resilience. The Rapid Alert System has proven its importance, making it possible to swiftly share with EU institutions, member states and international partners analysis, best practices and communications material. The EEAS has also intensified its work to help partners in the region to tackle the issue of information manipulation and interference—for example, in the western Balkans, which are currently being targeted through systematic FIMI campaigns by the pro-Kremlin ecosystem. It also worked on approaches and instruments allowing partners to impose costs on FIMI actors. Throughout 2021, the EEAS strengthened its activities to analyze and expose information manipulation and interference, including via its dedicated EUvsDisinfo website and the many awareness-raising and training activities as part of a broader campaign.

North Atlantic Treaty Organization (NATO)

NATO resilience grants program

NATO continues the implementation of its #NATO2030 agenda to be fit to deal with current and future security challenges. In 2020 and 2021, NATO's Public Diplomacy Division awarded grants aimed at building resilience to disinformation and hostile information activities among NATO countries. Non-governmental organizations, thinktanks and universities were invited to submit innovative projects. In 2020, 30 projects were supported with a total budget of 310,000 euros and in 2021, 35 project proposals were supported with NATO funding totalling 425,000 euros. Selected projects included initiatives focusing on media literacy, research and development of educational online games.

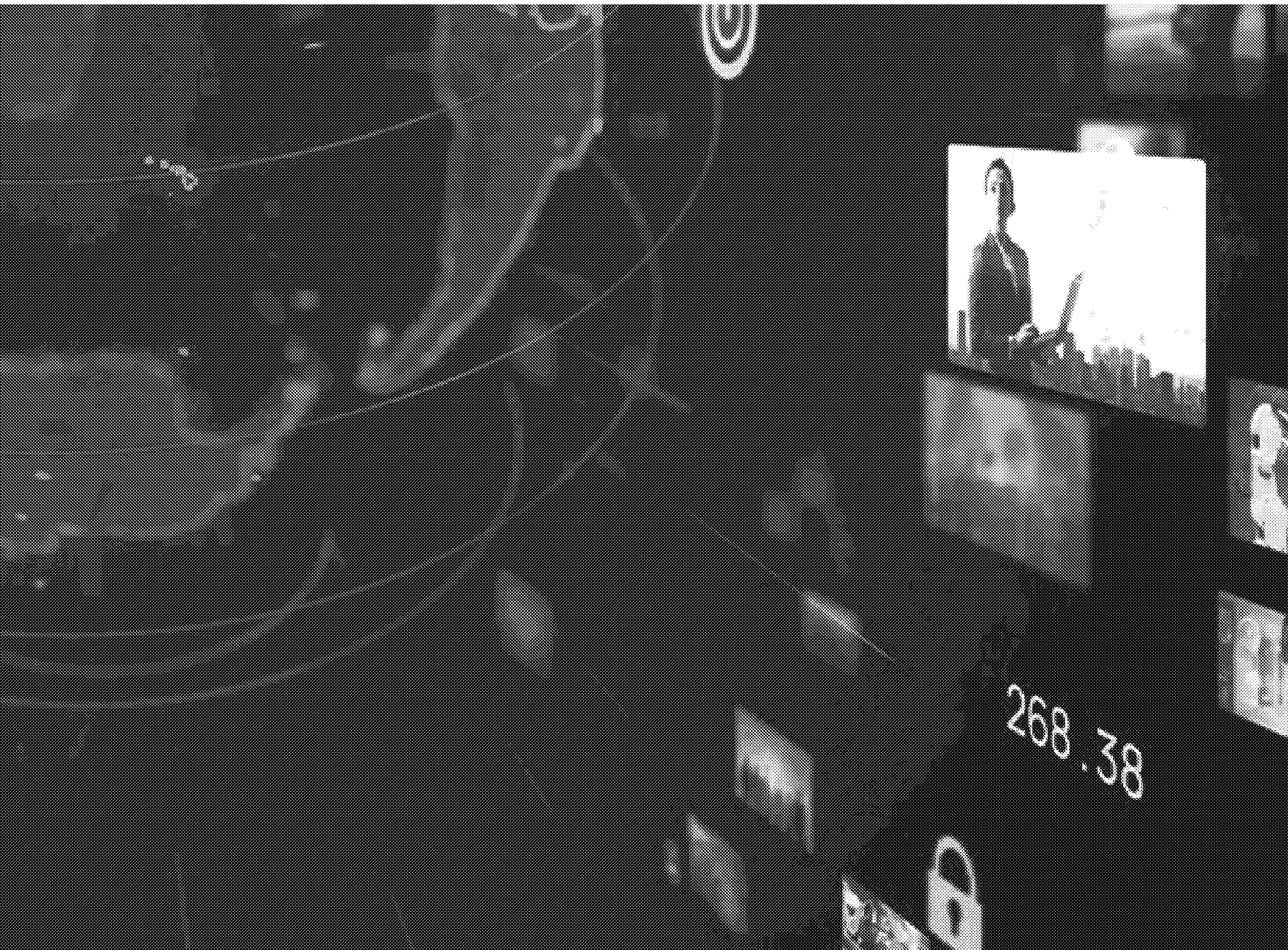
28 EEAS Stratcom Activity Report 2021: https://eeas.europa.eu/sites/default/files/report_stratcom_activities_2021.pdf

NEXT STEPS FOR THE G7 RRM

In 2022, the G7 RRM community will implement a broad array of activities aimed at enhancing collaboration in the following key areas:

- building knowledge and capacity to counter foreign threats within the G7 RRM and with key partners
- developing common data analytics tools and methods to identify foreign threats
- strengthening the G7 RMM's capacity for coordinated response to foreign threats
- supporting research to assess possible foundations for norms development with respect to foreign information manipulation and interference
- strengthening collaboration with other international organizations and initiatives, civil society, academia and industry to identify and counter foreign threats
- communicating the work of the G7 RRM to G7 publics through a second annual report on foreign threats to democracy

Under the auspices of the German G7 presidency, and while continuing to focus on countering disinformation, the G7 RRM will also explore opportunities for collaboration on addressing threats to democracy stemming from the introduction of new technologies or targeting economic and research security, including at local levels.



ANNEX I

G7

RAPID RESPONSE MECHANISM

PROTECTING DEMOCRACY

ACTION PLAN 2021

MANDATE

The mandate of the G7 Rapid Response Mechanism (RRM) is to strengthen G7 coordination to identify and respond to diverse and evolving foreign threats to G7 democracies, including through sharing information and analyses and identifying opportunities for coordinated responses. The G7 RRM's focus includes, but is not limited to, threats to: 1) democratic institutions and processes; 2) information ecosystems and media; and 3) fundamental freedoms and human rights.

PROGRESS IN 2020

The G7 RRM made its greatest progress in information sharing. The RRM commenced monthly meetings of G7+ RRM focal points[1], including national updates and lessons learned, as well as bi-weekly exchanges at the analyst level. The RRM established a secure, online information-sharing portal under the auspices of the United States, whereby G7+ reporting is shared and analytical exchanges take place. The RRM also continued to produce its monthly unclassified newsletter the Wire, highlighting original insight, sharing new developments and identifying potential partnerships in defence of democracy. Finally, the RRM established an information-sharing agreement with the EU Rapid Alert System.

G7 RRM information sharing was tested and proven in the context of the COVID-19 pandemic. The RRM quickly shifted its focus to the pandemic in the first quarter, supporting a real-time exchange of analyses of foreign threats that included industry and civil society organization partners, particularly with respect to evolving foreign-state-sponsored information manipulation. The G7 RRM also supported G7 political directors by leading a G7 proposal on protecting shared values to counter COVID-19-related state-sponsored disinformation, under the auspices of the United States' G7 presidency. Although the leaders' summit did not ultimately take place, elements of the proposal were re-purposed by G7 members and like-minded countries.

G7 members undertook collaborative initiatives, including a joint report by 2 members on new tactics in amplifying COVID-19-related narratives and combatting disinformation and a report on this dynamic across G7+ member states.

TARGETS FOR 2021

The focal points agree to the following targets for 2021:

1. Enhance common understanding of all foreign threats to democracy, including, but not limited to, elections and disinformation.
2. Maintain robust information-sharing platforms and continue to increase the exchange of national developments and lessons learned, assessments and real-time analyses.
3. Bolster respective ethical and methodological frameworks for open data monitoring and analysis in the context of evolving tactics and trends in online disinformation.
4. Develop a shared understanding of what constitutes foreign interference as opposed to foreign influence with a view to developing shared norms.
5. Strengthen the reporting relationship between the G7 RRM and G7 political directors to facilitate coordinated responses.

1. The G7+ RRM consists of G7 RRM members and observers. The G7 RRM members are Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and the European Union (EU). The G7 RRM observers are Australia, New Zealand and the Netherlands. Each member and each observer are represented by a focal point at the monthly meetings of the RRM.

6. Strengthen collaboration with other similarly mandated international organizations and initiatives to avoid duplication and leverage added value.
7. Strengthen collaboration with civil society organizations and academia to increase public awareness and resilience and coordinate research and capacity building programming for maximum effect.
8. Coordinate engagement, where appropriate, with social media companies.
9. Communicate the work of the G7 RRM to the publics of G7 states through annual reports on foreign threats to democracy.

COMMITMENTS FOR 2021

In order to meet RRM targets, the focal points agree to the following commitments for 2021:

- Increase information sharing, informed by national developments, lessons learned and assessments via contributions to monthly G7 RRM meetings, the GEC-IQ platform and Wire newsletter, including by engaging respective national government departments and agencies where relevant.
- Facilitate national participation in the Open Data Analytics Community of Practice biweekly meetings, undertaking joint open data analytics projects and developing common data analytics terminology, tools and methodologies.
- Support a working group, under the United States' leadership, on building open data monitoring and analysis capacity with a view to: 1) strengthening the analytic capacity of the G7 RRM; 2) synchronizing the analytic work of the G7 RRM to avoid duplication and achieve maximum effect; and 3) building the capacity of third countries.
- Support a working group, under EU leadership, to distinguish between influence (a legitimate activity) and interference (an illegitimate activity), with a focus on disinformation; the conceptual framework will serve as a basis for defining thresholds with a view to triggering potential coordinated responses.
- Engage respective G7 political directors in the work of the G7 RRM.
- Brief the G7 RRM on ongoing work in similarly mandated international organizations and initiatives—including NATO, the NATO Strategic Communications Centre of Excellence and the EU Centre of Excellence for Countering Hybrid Threats—and identify opportunities for collaboration and deconfliction, including by welcoming additional observers.
- Support and share research on foreign threats to democracy in partnership with academia and civil society organizations, doing so jointly with G7 RRM partners where appropriate.
- Identify and develop common positions for engagement with social media companies.
- Develop a G7 RRM report on disinformation to be shared with respective publics.

The Coordination Unit agrees to conduct the following activities in 2021:

- Convene RRM meetings.
- Facilitate the circulation and curation of relevant content across the RRM network, including through the GEC-IQ and the EU Rapid Alert System.
- Produce the RRM's Wire newsletter.
- Undertake open data analytics and produce reports on disinformation.
- Coordinate and facilitate RRM initiatives and partnerships.
- Support the United Kingdom's G7 presidency in the lead-up to ministerial meetings and the leaders' summit.