G7 GERMANY
2022

PROTÉGER LA DÉMOCRATIE

MÉCANISME DE RÉPONSE RAPIDE DU G7

Rapport annuel de 2021

L’équipe du Mécanisme de réponse rapide d’Affaires mondiales Canada (MRR Canada) sert de secrétariat permanent au Mécanisme de réponse rapide du G7 (MRR du G7). Le MRR Canada a préparé le présent rapport en partenariat avec les membres et les observateurs du MRR du G7, y compris l’Australie, la Nouvelle-Zélande, l’OTAN, les Pays-Bas et la Suède.

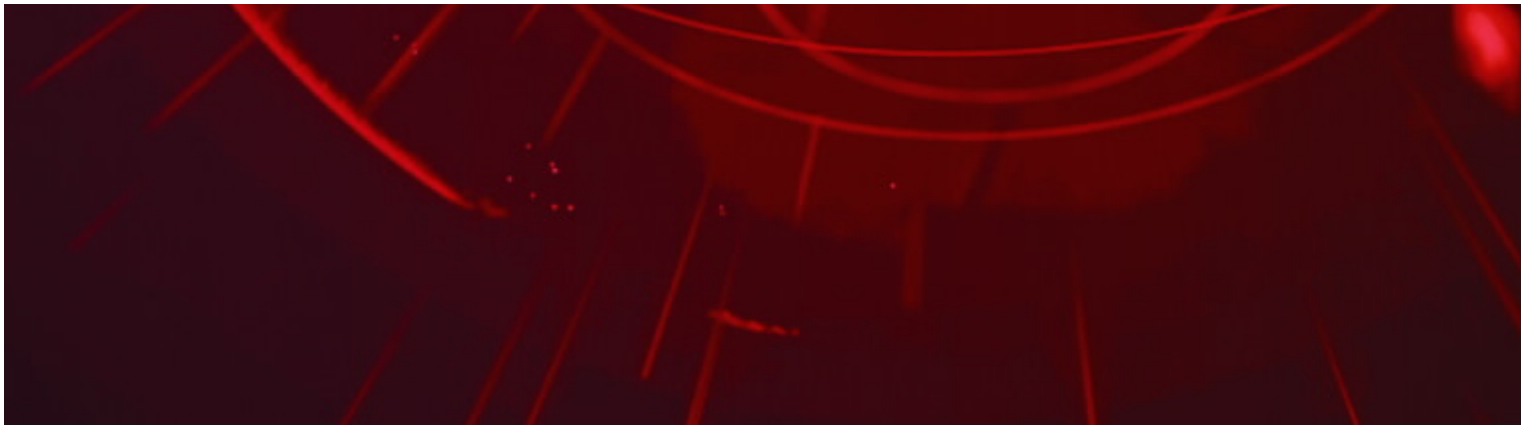

TABLE DES MATIÈRES

G7 GERMANY
2022

PROTÉGER LA DÉMOCRATIE

MÉCANISME DE RÉPONSE RAPIDE DU G7

INTRODUCTION

Au Sommet du G7 de Charlevoix en 2018, les dirigeants ont mis en place le Mécanisme de réponse rapide du G7 (MRR du G7) afin de renforcer la coordination qui permet de déceler les diverses menaces étrangères contre la démocratie et d'y répondre. Ces menaces, qui sont en constante évolution, comprennent les activités d'États hostiles visant nos institutions et nos processus démocratiques, notre environnement médiatique et informationnel, ainsi que l'exercice des droits de la personne et des libertés fondamentales.

Le MRR du G7 est composé d'agents de coordination de la communauté du G7, y compris l'Union européenne (UE), et compte l'Australie, la Nouvelle-Zélande, l'OTAN, les Pays-Bas et la Suède à titre d'observateurs. Les agents de coordination tirent parti de leurs structures et de leurs processus institutionnels respectifs pour favoriser une participation pangouvernementale. Le Canada dirige le Mécanisme de façon continue.

Pendant la réunion des ministres des Affaires étrangères et du Développement du G7 (en anglais) de 2021 à Londres, les ministres des Affaires étrangères se sont engagés à faire en sorte que le MRR du G7 présente des rapports annuels thématiques sur divers aspects des menaces en constante évolution et des réponses possibles pour favoriser la sensibilisation du public et la résilience.

À la demande des ministres des Affaires étrangères du G7, ce premier rapport annuel porte sur la désinformation, un vecteur de plus en plus important de l'ingérence étrangère qui menace les démocraties. Le rapport donne un aperçu du contexte de la menace que représente la désinformation, y compris les événements et les développements marquants de 2021, les tendances naissantes et les conséquences pour les possibilités de réponse qui comprennent des mesures de protection pour le respect de la liberté d'opinion et d'expression. Il décrit également les activités générales du MRR du G7 au cours de l'année écoulée et donne un aperçu des priorités de ce dernier en 2022. Enfin, le rapport donne divers exemples d'initiatives entreprises par les membres du MRR du G7, souvent éclairées par un échange d'information et de pratiques exemplaires, pour contrecarrer les menaces étrangères qui pèsent sur les démocraties.

CONTEXTE DE LA MENACE DE DÉSINFORMATION EN 2021

CONTEXTE

La menace que représentent les activités d'États hostiles pour les démocraties a persisté et évolué en 2021, et la désinformation constituait un vecteur essentiel[1]. Agissant directement, au moyen de médias et d'influenceurs étatiques et affiliés, ou indirectement, au moyen d'intermédiaires, un certain nombre d'États ont continué à créer, à diffuser ou à amplifier la désinformation pour faire avancer leurs objectifs stratégiques.

Bien qu'il n'existe pas de définition internationalement reconnue de la désinformation, celle-ci désigne généralement une information fausse ou trompeuse diffusée délibérément, par opposition à la mésinformation, qui désigne une information fausse ou trompeuse diffusée involontairement. La désinformation peut être utilisée par un acteur, étranger ou national, pour atteindre des objectifs politiques, idéologiques, économiques ou militaires. La désinformation est un terme souvent employé comme raccourci pour le défi plus large que représente la manipulation de l'information, qui, en plus des fausses nouvelles, comprend des tactiques telles que l'omission partielle ou totale de faits, le contenu audiovisuel trafiqué, l'amplification inauthentique de récits, les trolls et le recours à la censure ou à l'autocensure de l'information, visant toutes à déformer la perception de la réalité par le public[2]. Dans le cadre du présent rapport, nous utilisons le terme désinformation pour désigner l'ensemble des efforts visant à tromper dans le contexte de l'information, en insistant sur la désinformation propagée par les acteurs étatiques et leurs mandataires.

La désinformation a prospéré dans le contexte de la COVID-19, car la pandémie mondiale a fourni un terreau fertile aux acteurs étatiques hostiles, agissant directement ou par l'intermédiaire de mandataires, pour manipuler l'environnement informationnel[3]. La vie s'est poursuivie en ligne, plus de gens que jamais consultant les écrans et accédant à une quantité sans précédent d'information, exacte ou non, ce qui a donné lieu à ce que l'on a appelé communément une « infodémie[4] ». Il est donc devenu de plus en plus difficile de faire la distinction entre le contenu et les tactiques de manipulation employées par des acteurs étatiques hostiles ou leurs mandataires et l'information authentique. En outre, ces acteurs ont tiré parti des difficultés et des frustrations liées à la pandémie vécues par les personnes et les collectivités, y compris les répercussions sociales et économiques inégales, pour diffuser et amplifier des récits visant à saper la crédibilité des gouvernements démocratiques et à polariser davantage les sociétés démocratiques.

PRINCIPAUX ÉVÉNEMENTS ET DÉVELOPPEMENTS MARQUANTS

Les questions liées à la désinformation ont continué à faire les manchettes et à dominer les programmes politiques dans les pays du G7 et à l'échelle mondiale tout au long de l'année 2021, alors que les activités des États hostiles se sont manifestées en relation avec la pandémie en cours, les élections nationales et infranationales, et d'autres événements d'importance mondiale.

Les efforts déployés par les gouvernements et les autorités de santé publique pour faire face aux vagues successivesde **COVID-19** ont été contrariés par un flux constant de campagnes de désinformation hostiles parrainées par des États, qui ont souvent inspiré ou amplifié la désinformation nationale. Depuis le début de la pandémie, les acteurs étatiques hostiles ont manipulé l'information pour semer le doute sur les origines du virus et les moyens nécessaires pour le combattre, discréditer les réponses démocratiques, saper les mesures de santé publique et promouvoir leurs propres réponses comme étant supérieures[5].

1 Veuillez consulter les sources canadiennes suivantes : Menaces d'ingérence étrangère visant les processus démocratiques du Canada (juillet 2021) et Cybermenaces contre le processus démocratique du Canada (mise à jour de juillet 2021).
2 Combating Information Manipulation: A Playbook for Elections and Beyond, International Republican Institute, septembre 2021 (en anglais).
3 Par exemple, consulter la communication du Service européen pour l'action extérieure sur la désinformation dans le contexte de la COVID-19.
4 Pour un complément d'information, des outils et des lignes directrices pour lutter contre l'infodémie dans le domaine de la santé, consulter l'Organisation mondiale de la santé (en anglais).
5 Superspreaders of Malign and Subversive Information on COVID-19, Rand Corporation, 2021 (en anglais).

Nous avons vu des acteurs étatiques hostiles, s'inspirant de leurs campagnes respectives, amplifier les fausses allégations selon lesquelles la COVID-19 proviendrait d'un laboratoire d'armes biologiques américain ou aurait été inventée par Washington pour affaiblir d'autres pays[6]. Nous les avons également vus diffuser des messages trompeurs concernant la fourniture d'équipements de protection individuelle (EPI) à des pays tiers, afin d'affaiblir la cohésion et la solidarité des pays donateurs démocratiques et de minimiser l'importance de l'aide fournie par les pays démocratiques.

Depuis le début de l'année 2021, nous avons assisté à des campagnes de désinformation menées par des États étrangers visant à la fois à saper la confiance dans les vaccins produits dans les pays démocratiques et à promouvoir des produits de ces États[7]. Nous avons également vu des acteurs étatiques hostiles amplifier activement le sentiment antivaccin, particulièrement en accueillant des théoriciens du complot sur des chaînes de médias liées à l'État[8]. Par conséquent, ces campagnes de désinformation ont contribué à l'érosion de la confiance dans les mesures mises en œuvre par les gouvernements démocratiques et, dans la mesure où elles ont sapé la confiance du public dans les conseils des autorités de santé publique, elles ont également mis la vie de gens en danger.

Les campagnes de désinformation menées par des États étrangers ont également été une caractéristique importante de diverses **élections nationales et infranationales**, y compris dans les pays du G7, dans le but d'influer sur les résultats électoraux, de saper la confiance dans les processus et les institutions démocratiques et de favoriser la polarisation. Si la désinformation n'est pas propre aux élections, les campagnes électorales sont souvent les points chauds autour desquels s'intensifient les activités des États hostiles, y compris la désinformation. L'encadré ci-dessous donne un aperçu des mesures adoptées par les gouvernements du MRR du G7 pour protéger l'intégrité de leurs processus électoraux.

EFFORTS DÉPLOYÉS PAR LES GOUVERNEMENTS POUR PROTÉGER LES ÉLECTIONS NATIONALES EN 2021

En mars 2021, le gouvernement fédéral des **États-Unis** a publié 2 rapports sur l'ingérence étrangère dans l'élection présidentielle de 2020. The Intelligence Community Assessment on Foreign Threats to the 2020 U. S. Federal Elections (en anglais) a relevé que rien n'indique qu'un acteur étranger ait tenté de modifier des aspects techniques du processus de vote, mais que certains acteurs étrangers ont diffusé des affirmations fausses ou exagérées sur des compromissions présumées des systèmes de vote afin de saper la confiance du public dans les processus et les résultats électoraux. Les auteurs du rapport conjoint du département de la Justice et du département de la Sécurité intérieure sur l'ingérence étrangère (en anglais) n'ont trouvé aucune preuve qu'un acteur affilié à un gouvernement étranger a empêché le vote ou modifié des aspects techniques du processus électoral, malgré les vastes campagnes menées par la Russie et l'Iran contre de multiples secteurs d'infrastructures critiques qui ont compromis la sécurité de plusieurs réseaux gérant certaines fonctions électorales. Les agences fédérales de renseignement, d'application de la loi et de sécurité nationale ont continué à surveiller l'activité des menaces étrangères, à échanger de l'information et à fournir une assistance en matière de sécurité électorale aux autorités électorales étatiques et locales et au secteur privé, à l'approche des élections fédérales de mi-mandat en 2022.

Plusieurs élections régionales et l'élection fédérale ont eu lieu en **Allemagne** en 2021. Devant l'augmentation des activités hostiles dans le domaine de l'information et du cyberespace, le gouvernement fédéral allemand a mis en place une plateforme de coopération spécialisée afin de renforcer les capacités et les structures de coopération actuelles pour contrer la désinformation et d'autres formes d'ingérence étrangère. Au moyen de cette plateforme, le ministère fédéral de l'Intérieur a coordonné l'ensemble des mesures de prévention, de détection et de réponse liées aux activités hostiles. Le dialogue et l'échange d'information

6 Weaponized: How rumors about COVID-19's origins led to a narrative arms race, DFRLab, février 2021 (en anglais).
7 Par exemple, consulter les communications du site EUvsDisinfo.eu, qui font régulièrement le point sur l'évolution des discours de manipulation de l'information dans les médias pro-Kremlin.
8 Russia's Pillars of Disinformation and Propaganda, Global Engagement Center, août 2020 (en anglais).

avec les intervenants nationaux et les partenaires internationaux, ainsi qu'une coopération étroite au sein du G7, de l'UE et de l'OTAN, ont renforcé les mesures du gouvernement. Seules quelques activités d'influence malveillante de la part d'États étrangers se sont finalement concrétisées. Il y a eu, par exemple, un certain nombre de cyberattaques contre des hommes et des femmes politiques allemands au début de septembre 2021, que le gouvernement fédéral allemand a attribuées à la Russie. Plus précisément, une vaste campagne de sensibilisation auprès du grand public et de groupes cibles précis, ainsi que des mesures de communication gouvernementales coordonnées, ont contribué à la protection réussie de l'élection contre les menaces hybrides.

Le gouvernement du **Canada** a mis à jour et activé son Plan pour protéger la démocratie canadienne en vue de l'élection générale de 2021 au Canada. Ce plan comprenait le Protocole public en cas d'incident électoral majeur, un groupe non partisan de hauts fonctionnaires ayant pour mandat d'informer le public pendant la période d'application de la convention de transition, au cas où des opérations d'influence et d'ingérence menaceraient la capacité du Canada à tenir une élection libre et équitable. Il comprenait également la Déclaration du Canada sur l'intégrité électorale en ligne, un code volontaire entre le gouvernement et les entreprises de médias sociaux pour soutenir les principes d'intégrité, de transparence et d'authenticité. Tout au long de l'élection, le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections a activement surveillé les indicateurs de manipulation de l'information et d'ingérence étrangères, entre autres menaces étrangères. Les agences de sécurité et de renseignement du Canada ont averti à plusieurs reprises avant l'élection que des acteurs hostiles déployaient des efforts pour injecter et amplifier de l'information fausse et trompeuse sur des plateformes en ligne afin de faire avancer leurs programmes, y compris des tentatives de miner les processus démocratiques du Canada et de s'ingérer dans les élections. En fin de compte, le gouvernement du Canada n'a pas détecté d'activités d'ingérence qui ont compromis l'intégrité de l'élection.

Des élections générales à la Chambre des représentants ont eu lieu au **Japon** en octobre 2021. Le gouvernement japonais est resté vigilant face à d'éventuelles cyberactivités malveillantes menaçant la démocratie, telles que la diffusion de désinformation sur les élections par des acteurs étrangers. En parallèle, une initiative de vérification des faits a été mise en œuvre par une organisation non gouvernementale visant à protéger la société contre la mésinformation et la désinformation, qui a contribué à surveiller l'environnement informationnel pendant les élections et à sensibiliser le public au moyen de son site Web. En fin de compte, aucune activité d'influence malveillante de la part d'États étrangers n'a été signalée.

Tout au long de l'année 2021, nous avons observé d'autres exemples notables de désinformation : la crise fabriquée de la frontière biélorusse; les efforts de la République populaire de Chine (RPC)pour faire pression sur Taïwan; les récits sur le renforcement des restrictions de sécurité à Hong Kong et le portrait manipulateur de la situation des droits de la personne au Tibet et au Xinjiang par divers moyens, y compris en faisant taire des voix et en supprimant de l'information [9].

Depuis la révolution de Maïdan de 2014 en Ukraine et l'annexion illégale de la Crimée par la Russie, le Kremlin a mené des campagnes de désinformation incessantes contre l'Ukraine. Ces campagnes ont ciblé les populations russophones d'Ukraine, mais ont également été utilisées pour influencer les pays voisins et le public international en général [10]. Après novembre 2021, la campagne du Kremlin s'est intensifiée pour soutenir le renforcement militaire sur le terrain et ouvrir la voie à une escalade de l'agression. Cette campagne a faussement caractérisé le gouvernement ukrainien comme étant faible, corrompu et une marionnette de l'Occident. Elle prétendait que le gouvernement ukrainien commettait des atrocités contre des civils dans le Donbass et que l'Ukraine était une partie historique de la Russie. Elle a mis de l'avant un faux récit qui présentait les démocraties occidentales comme les agresseurs responsables du

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

10 Russian Hybrid Threats Report: Kremlin pushes claims about Ukrainian offensive, 'junk' weapons from West, DFRLab, janvier 2022 (en anglais).

renforcement sans précédent des troupes russes aux frontières de l'Ukraine et la Russie comme une partie innocente agissant en état de légitime défense, ouverte à la diplomatie. Le Kremlin a continué à diffuser toute une série de fausses affirmations pour faire avancer ses objectifs, de pair avec son empiétement militaire, y compris en ce qui concerne la capacité et l'intention du gouvernement ukrainien de développer et d'utiliser des armes chimiques, bactériologiques, radiologiques et nucléaires.

En réponse, le G7 et les démocraties partenaires se sont efforcés de contrer la désinformation de la Russie[11] en renforçant le soutien au MRR du G7, en échangeant des évaluations en temps réel, en coordonnant les approches en matière de communication, en imposant des sanctions aux personnes et aux entités liées aux violations du droit international par la Russie, et en dénonçant ceux qui diffusent la désinformation de la Russie à la demande de ses services de renseignement [12]. Certains pays ont également apporté un soutien au renforcement des capacités des organisations de la société civile ukrainienne qui luttent contre la désinformation russe et protègent l'intégrité de l'environnement informationnel ukrainien.

ÉVOLUTION DES TENDANCES

Le MRR du G7 a cerné les 12 tendances notables suivantes dans les activités de manipulation de l'information parrainées par des États étrangers en 2021, dans lesquelles les tactiques de désinformation ont joué un rôle clé. Ces tendances ont été retenues à la suite de recherches dans les sources primaires et secondaires dans l'ensemble de la communauté du MRR du G7 et ont des conséquences importantes pour nos efforts stratégiques et législatifs visant à répondre aux menaces étrangères.

1. Les acteurs étatiques étrangers, tels que la Russie et la RPC en particulier, et, dans une certaine mesure, la République islamique d'Iran, entre autres, ont exploité **les sujets de discorde et les clivages sociaux** pour polariser les sociétés, influer sur les résultats politiques et saper les institutions et les processus démocratiques [13]. Ces questions et ces divisions ont été exacerbées par les tensions liées aux répercussions et à la gestion de la pandémie de COVID-19.
2. Dans une volonté de conférer une légitimité à leurs messages dans différents contextes, les acteurs étatiques étrangers ont souvent coopté ou utilisé des **influenceurs clés**, tels que des vedettes, des médias traditionnels et des personnalités publiques, pour valider ou amplifier leur contenu [14].
3. Une série **d'acteurs non étatiques perturbateurs** ont joué un rôle croissant dans la diffusion de la désinformation parrainée par des États étrangers[15]. Ces acteurs non étatiques perturbateurs comprennent des mouvements extrémistes transnationaux, des mandataires affiliés à des États étrangers et des acteurs privés motivés par le profit qui diffusent de la désinformation contre rémunération [16]. Ces acteurs manipulent souvent l'information et amplifient les faussetés, parallèlement aux acteurs étatiques étrangers ou à leur demande.
4. Différentes **collectivités de la diaspora** ont continué à subir des pressions directes et indirectes au moyen de la censure, de campagnes de désinformation et de la manipulation secrète de l'information

11 Fact vs. Fiction: Russian Disinformation on Ukraine, Département d'État des États-Unis, janvier 2022 (en anglais); Disinformation About the Current Russia-Ukraine Conflict – Seven Myths Debunked, East StratCom Task Force, janvier 2022 (en anglais); OTAN-Russie : mise au point, Division de la diplomatie publique de l'OTAN, janvier 2022.

12 Taking Action to Expose and Disrupt Russia's Destabilization Campaign in Ukraine, Département d'État des États-Unis, janvier 2022 (en anglais).

13 Threat Report: Combating Influence Operations, Meta, mai 2021 (en anglais). Consulter aussi Pinault, Nicolas (25 mars 2021), « Macron Warns Turkey Not to Interfere in French Elections » (en anglais), Voice of America. Consulter Foreign Threats to the 2020 US Federal Elections, U.S. National Intelligence Council, mars 2021 (en anglais) pour une analyse des campagnes d'influence secrètes menées par la Russie et l'Iran visant l'intégrité des élections. En ce qui concerne les activités de la RPC, consulter Superspreaders of Malign and Subversive Information on COVID-19, Rand Corporation, 2021 (en anglais) et China's Influence in Southeastern, Central, and Eastern Europe: Vulnerabilities and Resilience in Four Countries, Carnegie Endowment, 13 octobre 2021 (en anglais). Pour d'autres références sur les activités de l'Iran, consulter Iranian Influence Networks in the United Kingdom: Audit and Analysis, Henry Jackson Society, 7 juin 2021 (en anglais) et Designation of Iranian Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election, Département d'État des États-Unis, 18 novembre 2021 (en anglais).

14 Culliford, Elizabeth (10 août 2021), « Facebook removes Russian network that targeted influencers to peddle anti-vax messages », Reuters (en anglais). Consulter aussi le rapport de Meta sur la suppression du réseau : July 2021 Coordinated Inauthentic Behaviour Report (en anglais).

15 Bien que le mandat du MRR du G7 se concentre sur la surveillance des menaces à la démocratie provenant d'acteurs étatiques étrangers et la lutte contre celles-ci, nous soulignons le réseau complexe d'acteurs agissant au-delà des frontières et des enjeux.

16 Disinformation-For-Hire: The Pollution of News Ecosystems and Erosion of Public Trust, Center for International Media Assistance, décembre 2021 (en anglais).

par des acteurs étatiques dans leur pays d'origine, dans le but de réduire la dissidence ou de soutenir les politiques du pays d'origine [17].

5. Les acteurs étatiques et non étatiques diffusent de la **désinformation fondée sur le genre et l'identité** (race, origine ethnique, orientation sexuelle, etc.) sur des dirigeants politiques, des journalistes et d'autres personnalités publiques. Parmi les exemples récents de ces attaques, citons les campagnes de désinformation contre la ministre des Affaires étrangères allemande, Annalena Baerbock [18], la vice-présidente des États-Unis, Kamala Harris[19], et la dirigeante prodémocratie biélorusse, Sviatlana Tsikhanouskaya[20]. Les messages trompeurs de ces campagnes comprenaient souvent des récits dégradants, un langage codé visant à contourner les systèmes de modération, ainsi que des textes inexacts ou des images et des vidéos trafiquées ou mal attribuées, destinés à décourager les cibles de participer à la vie publique.

6. Les acteurs étatiques étrangers ont ciblé des **organismes et des forums non étatiques au niveau infranational**,notamment des entreprises, la société civile, des établissements d'enseignement et des instituts scientifiques ou de recherche, afin d'exercer une influence indue, d'obtenir des renseignements essentiels et d'orienter les publics cibles vers les campagnes de désinformation en cours [21].

7. Les acteurs étatiques étrangers, tels que la Russie,ont continué à utiliser des **médias contrôlés par l'État ou affiliés à l'État** et des sites d'information par procuration, également connus sous le nom de « **sites d'information grise**[22] », pour manipuler le discours public et s'adresser à des publics cibles. Ils ont déployé cette tactique dans les pays démocratiques, en particulier pendant les élections. Ce faisant, ils ont brouillé la frontière entre la diplomatie ouverte et la manipulation secrète de l'information.

8. La « **diplomatie du loup guerrier** » de la RPC est apparue au grand jour ces dernières années, avec de hauts dirigeants diffusant des points de vue agressifs, et parfois de la désinformation, sur les médias sociaux. Ces « loups guerriers » ont créé du contenu ou amplifié le contenu des médias d'État et des médias affiliés dans leurs flux de médias sociaux. À leur tour, ces médias étatiques et affiliés ont également utilisé des messages des « loups guerriers » pour alimenter des campagnes d'influence, augmentant ainsi les sources de contenu pour l'amplification et le trollage par des réseaux coordonnés de comptes de médias sociaux [23].

9. Si les tactiques et les techniques de désinformation déployées par les acteurs étatiques étrangers diffèrent dans leur degré de complexité, une imitation croissante des tactiques russes a été observée, particulièrement de la part de la RPC.Le modèle russe se caractérise par la coordination des campagnes de désinformation et d'autres actions déstabilisantes en recourant à un éventail de moyens et de capacités hybrides [24].

10. Les acteurs étatiques étrangers ont mené des campagnes d'influence sur **des plateformes et des réseaux de médias sociaux divers**,y compris des réseaux fermés et chiffrés. Cela a posé de nombreux défis aux gouvernements, à la société civile, aux plateformes en ligne et aux chercheurs universitaires dans leur volonté de détecter, de coordonner et de combattre la diffusion de la désinformation, et de mesurer son ampleur et son intention.

11. **Les plateformes alternatives de médias sociaux** ont continué à offrir un refuge aux acteurs non étatiques, motivés par l'idéologie, qui ont été retirés des plateformes principales ou « déplateformés » pour violation des conditions de service. Certaines de ces plateformes alternatives sont directement liées à des acteurs étatiques hostiles ou influencées par eux [25]. Sur ces plateformes, l'information exacte et fiable est souvent noyée dans des discours de haine, la désinformation et de faux récits de nature

17 Disinformation, stigma and Chinese diaspora: policy guidance for Australia, First Draft News, août 2021 (en anglais).
18 Targeting Baerbock: Gendered Disinformation in Germany's 2021 Federal Election, Alliance for Securing Democracy, août 2021 (en anglais).
19 Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, Wilson Center, janvier 2021 (en anglais).
20 Voir les analyses d'EUvsDisinfo (en anglais) sur les attaques de désinformation contre Sviatlana Tsikhanouskaya.
21 Big fish in small ponds: China's subnational diplomacy in Europe, Merics et Heinrich Böll-Stiftung, novembre 2021 (en anglais).
22 Ces sites Web peuvent donner l'impression d'être des sources d'information alternatives légitimes dans le but de brouiller l'attribution de la source ultime ou l'affiliation à un État. Souvent, afin d'augmenter la perception de crédibilité, ils publient de l'information exacte à côté de la désinformation. Consulter le rapport du Global Engagement Center des États-Unis sur Pillars of Russia's Disinformation and Propaganda Ecosystem (août 2020; mis à jour en janvier 2022).
23 Growling Back at the West, China Media Project, University of Hong Kong Journalism and Media Studies Centre, août 2021 (en anglais).
24 Les opérations d'influence chinoises : un moment machiavélien, Institut de Recherche Stratégique de l'École Militaire, octobre 2021.
25 Posing as Patriots, Graphika, juin 2021 (en anglais).

complotiste qui sont amplifiés par des États hostiles, des groupes politiques marginaux et des gens à la recherche de profit ou d'influence.

12. En 2021, les gouvernements étrangers ont continué à développer une technologie avancée appelée **hypertrucage** ou deepfake, qui permet de générer rapidement des vidéos, des sons et des textes de synthèse, et peut être utilisée à des fins malveillantes. L'hypertrucage a été employé à petite échelle pour soutenir les campagnes d'influence étrangères pendant les élections américaines de 2020, et les progrès de la recherche rendront probablement ces technologies plus perfectionnées dans les années à venir[26].

CONSÉQUENCES

Les tendances démontrent que la désinformation en ligne et hors ligne parrainée par des États étrangers, qui n'est qu'un outil parmi d'autres dans l'arsenal plus large des activités des États hostiles, est un défi de plus en plus transnational, multidimensionnel et multiplateforme. Dans ce contexte, il est difficile de faire la distinction entre les acteurs étrangers et nationaux; les uns et les autres sont de plus en plus nombreux et leurs tactiques sont de plus en plus complexes. Parallèlement, la frontière entre la diplomatie ouverte, d'une part, et la manipulation d'information malveillante, d'autre part, s'estompe également.

Ces défis compliquent les efforts visant à lutter contre la manipulation de l'information par des acteurs étatiques hostiles, allant de la détermination et de l'évaluation des menaces à la conception d'options de réponse efficaces tout en respectant la liberté d'expression. Par exemple, l'attribution est de plus en plus difficile à réaliser avec un degré élevé de certitude. Il est également difficile de mesurer les effets réels ou possibles de la désinformation. Ceci, à son tour, met à l'épreuve notre capacité à élaborer des options de réponse efficaces et responsables. Et étant donné que les auteurs de campagnes de désinformation mènent une multitude d'activités dans le temps et dans l'espace, il n'est pas pertinent de répondre à la désinformation comme s'il s'agissait d'un événement unique. Cela met également en évidence le défi sociétal plus large qui consiste à encourager la résilience et un scepticisme sain à l'égard des affirmations non vérifiées, tout en garantissant le respect de l'intégrité des faits et de la science.

Entretemps, de nombreux États étrangers responsables de la désinformation investissent de plus en plus de ressources pour exercer un contrôle sur leurs propres environnements d'information nationaux; une législation draconienne consacre le contrôle de l'État sur la libre circulation et le contenu de l'information, et limite l'exercice d'une série de libertés fondamentales et de droits de la personne, dont la liberté d'expression. L'exemple le plus récent et le plus flagrant de cette tendance est la répression exercée par le Kremlin à l'encontre des médias indépendants en Russie, accompagnée de restrictions et de blocages des plateformes de médias sociaux et de la criminalisation de l'opposition à la guerre. Ces États, avec la Russie en tête, cherchent aussi activement à façonner les initiatives multilatérales, aux Nations Unies et ailleurs[27], afin de s'assurer que tout cadre normatif et juridique portant sur l'environnement informationnel mondial qui est adopté correspond à leur propre vision des choses.

Au fur et à mesure que nous comprenons mieux l'évolution des menaces liées à la désinformation, les démocraties se mobilisent pour coordonner leurs actions au moyen de mécanismes tels que le MRR du G7. Cet élan s'appuie sur une compréhension approfondie du fait que les réponses politiques doivent être fondées sur des données probantes et doivent être proportionnelles, et que la lutte efficace contre la manipulation de l'information sous toutes ses formes nécessite une approche en réseau fondée sur les valeurs et les principes démocratiques.

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

27 Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales, résolution de l'Assemblée générale des Nations Unies A/RES/76/227, novembre 2021.

ACTIVITÉS DU MRR DU G7 EN 2021

Les activités du MRR du G7 ont été orientées par son plan d'action de 2021 (voir l'annexe 1). Ce plan visait à renforcer la compréhension commune des membres et des observateurs du MRR du G7 des menaces étrangères contre la démocratie et de la réponse à celles-ci. Tout au long de l'année 2021, le Mécanisme a continué à permettre l'échange d'information en temps réel sur la désinformation et les autres tactiques et menaces d'influence malveillante étrangères, et a servi de plateforme pour discuter des approches nationales et des réponses coordonnées.

ÉCHANGE D'INFORMATION

Les agents de coordination du MRR du G7 se sont réunis tous les mois pour échanger de l'information, des pratiques exemplaires et des leçons retenues. Les priorités thématiques comprenaient les registres d'agents étrangers, les menaces étrangères contre les droits et libertés de nos citoyens, le dialogue avec les plateformes de médias sociaux et la sécurité des élections. Plusieurs réunions ont permis aux universitaires et à la société civile de parler de menaces en évolution, telles que la désinformation liée à la COVID-19, la convergence des pratiques et des messages parmi les acteurs étatiques hostiles et, en préparation du plan d'action du MRR du G7 de 2022, les principales tendances et les grandes priorités dans la lutte contre les menaces étrangères à la démocratie. Ces discussions ont contribué à une compréhension commune de l'évolution des menaces étrangères, actuelles et à venir, et ont éclairé les approches nationales en vue de les contrer. Le Canada a continué de produire un fil d'actualité mensuel qui a pour but d'échanger des idées et des renseignements sur les nouveaux développements et les nouveaux projets, et à repérer des partenaires potentiels qui s'emploient à contrer les opérations d'influence malveillante et d'ingérence étrangère.

RENFORCEMENT DES CAPACITÉS D'ANALYSE

Les analystes du MRR du G7 se sont réunis régulièrement pour échanger des idées et des analyses en temps réel, notamment sur la désinformation liée à l'actualité telle que la crise migratoire au Bélarus. Ils ont également participé systématiquement à des analyses en ligne et à des échanges d'information facilités par le Global Engagement Center du Département d'État américain. Afin de renforcer la capacité analytique du MRR du G7 à évaluer et à contrer la désinformation, un groupe de travail sur l'analyse, dirigé par les États-Unis, a été créé. Il a commencé à élaborer une typologie pour évaluer le niveau d'affiliation entre les acteurs étatiques et les médias. Ce cadre commun permettra ultérieurement aux membres et aux observateurs du G7 d'employer une terminologie commune dans les rapports analytiques et contribuera à orienter les approches de contre-discours. Ces travaux se poursuivront en 2022.

MANIPULATION DE L'INFORMATION ET INGÉRENCE ÉTRANGÈRES

En 2021, le MRR du G7 a mis en place un groupe de travail sur la terminologie, en vue de distinguer les comportements légitimes et les comportements illégitimes des États et des organisations étatiques dans l'environnement informationnel. Sous la direction du Service européen pour l'action extérieure (SEAE), les membres ont discuté du concept de manipulation de l'information et d'ingérence étrangères afin de saisir les tactiques, les techniques et les procédures (TTP) en constante évolution déployées par les acteurs étatiques et leurs mandataires pour exercer une influence malveillante dans l'environnement de l'information.

Le concept de manipulation de l'information et d'ingérence étrangères décrit des modèles de comportement qui ont un effet négatif ou qui peuvent avoir un effet négatif sur les valeurs, les procédures et les processus politiques. Ces activités ont un caractère manipulateur et sont menées de manière intentionnelle et coordonnée par une série d'acteurs, étatiques ou non, y compris leurs mandataires, à l'intérieur et à l'extérieur de leur propre territoire. Elles comprennent l'ensemble des tactiques utilisées pour manipuler l'information. L'adoption du concept de manipulation de l'information et d'ingérence étrangères comme définition de référence permet aux membres du MRR du G7 d'élaborer un vocabulaire opérationnel commun axé sur les comportements malveillants en ligne et hors ligne, afin d'améliorer la compréhension commune des TTP hostiles, de les répertorier et de les perturber.

RENFORCER LE DISPOSITIF DE RÉPONSE

Le Service européen pour l'action extérieure (SEAE)a dirigé un groupe de travail sur la terminologie en vue de favoriser une compréhension conceptuelle commune des menaces pesant sur l'environnement informationnel et d'établir une base permettant de coordonner les réponses. Ce groupe de travail a défini les caractéristiques essentielles de la manipulation de l'information et de l'ingérence étrangères, en mettant l'accent sur le comportement manipulateur coordonné, intentionnel et nuisible d'acteurs étrangers et de leurs mandataires. Ces travaux se poursuivront en 2022, en collaboration avec le groupe de travail sur l'analyse, dans le but de mettre en place un vocabulaire commun et une méthode d'analyse correspondante dans l'ensemble du MRR du G7. En outre, le Canada a lancé un projet de recherche visant à répertorier les cadres nationaux et internationaux actuels de lutte contre la désinformation afin d'évaluer les fondements possibles de travaux ultérieurs sur l'élaboration de normes relatives à la manipulation de l'information et à l'ingérence étrangères.

EXPANSION ET COLLABORATION

Le MRRdu G7 a accueilli l'OTAN et la Suède en tant qu'observateurs dans le but de tirer parti de l'expertise et d'éviter les dédoublements. Le MRR du G7 a coordonné son action avec celle d'autres instances internationales qui s'efforcent de lutter contre les activités d'information hostiles menées par des États étrangers, dont la désinformation. Tout au long de l'année, le Mécanisme a également collaboré avec diverses parties intéressées afin de fournir des observations, d'accroître la sensibilisation du public à la désinformation et sa résilience face à celle-ci, et de coordonner les programmes de recherche et de renforcement des capacités pour en optimiser les effets.

PLEINS FEUX SUR LES PAYS ET LES ORGANISMES

Canada

Renforcer la résilience face à la désinformation grâce à la recherche, aux médias numériques et à l'éducation civique

Le Canada renforce la résilience de la société face à la désinformation grâce au Programme de contributions en matière de citoyenneté numérique (PCCN), qui finance des organismes tiers pour mieux comprendre la désinformation dans le contexte canadien et entreprendre des activités liées aux médias numériques et à l'éducation civique. En 2021 et 2022, le PCCN a financé 15 projets d'une valeur de 1,3 million de dollars pour comprendre le rôle des algorithmes dans la diffusion de la désinformation sur les plateformes grand public et marginales, la diffusion transnationale de la désinformation auprès des collectivités de la diaspora, et les répercussions disproportionnées sur les communautés autochtones et les collectivités non anglophones. Le PCCN a également financé des initiatives ciblant la désinformation sur la COVID19 au moyen des médias numériques et de l'éducation civique, soutenu une semaine d'éducation aux médias dirigée par l'organisation canadienne HabiloMédias et convoqué une assemblée de citoyens de tout le pays pour débattre et fournir des recommandations sur l'approche du Canada en matière de lutte contre la désinformation.

France

Un nouvel organisme de lutte contre les ingérences numériques étrangères qui visent à miner nos institutions démocratiques

Comme bon nombre de ses principaux partenaires européens et internationaux, la France a choisi de renforcer son dispositif de lutte contre la manipulation de l'information en créant un service destiné à protéger la démocratie contre les ingérences numériques étrangères. Ce service, mis en place en juillet 2021, s'appelle Viginum (Service de vigilance et de protection contre les ingérences numériques étrangères) et relève du secrétariat général de la défense et de la sécurité nationale (SGDSN), sous l'égide du cabinet du premier ministre. Viginum a une mission claire : repérer les campagnes de désinformation impliquant directement ou indirectement un État étranger ou une entité étrangère non étatique dont le but est la diffusion artificielle ou automatisée, massive et délibérée, par l'intermédiaire d'un service de communication public en ligne, d'accusations manifestement inexactes ou trompeuses visant à porter atteinte aux intérêts fondamentaux de l'État. L'organisme sera en activité d'ici la fin de 2022 et utilisera uniquement de l'information recueillie auprès de sources accessibles au public. Un comité scientifique et éthique supervisera les travaux de l'organisme.

Allemagne

Un nouveau centre pour la stratégie, l'analyse et la résilience

Le ministère fédéral de l'Intérieur et de la Patrie (BMI) est chargé de coordonner l'approche pangouvernementale de la lutte contre les menaces hybrides depuis juillet 2019. Un groupe de travail interministériel au niveau de la direction, présidé par le secrétaire permanent du BMI chargé de la lutte contre les menaces hybrides, a été mis en place pour faire progresser la planification et la coordination conjointes. Une étape importante de cette coopération interministérielle en matière de détection des menaces hybrides et de lutte contre celles-ci a été franchie en janvier 2021, lorsqu'une unité interministérielle spécialisée a commencé les essais et les préparatifs en vue du lancement d'un futur centre fédéral de stratégie, d'analyse et de résilience (SAR).Dirigé par le BMI, le SAR naissant comprend également des représentants du ministère fédéral des Affaires étrangères et du ministère fédéral de la Défense.

Italie

Conférence sur la lutte contre la désinformation

Les effets combinés de la désinformation, de la mésinformation et de l'information malveillante posent un défi de plus en plus sérieux à la sécurité nationale italienne. Au cours du second semestre de 2021, le ministère italien des Affaires

étrangères a commencé à planifier un événement pour le début du mois de février 2022, consacré à la question de la prévention de la désinformation et de la lutte contre celle-ci au niveau national. L'objectif est de renforcer la sensibilisation et la résilience des secteurs public et privé, et d'améliorer les contributions aux politiques et aux stratégies nationales et internationales contre la désinformation. L'échange d'information et d'enseignements sur les menaces actuelles, la manière de réagir et les réformes, y compris du cadre juridique, nécessaires pour être plus efficaces dans la prévention, l'atténuation et la répression de la désinformation feront partie de la discussion. Cet événement multipartite est le résultat de la coopération établie entre le ministère italien des Affaires étrangères et l'Observatoire italien des médias numériques.

Japon

Détection des opérations d'influence étrangère de plus en plus perfectionnées

En tant que membre de la communauté japonaise du renseignement, l'Agence de renseignement de la sécurité publique (PSIA)recueille et analyse les activités d'information menées par des pays étrangers, y compris les éventuelles opérations visant le processus démocratique du Japon. L'Agence a observé que les activités de publicité externe étrangères utilisant les services de réseaux sociaux sont devenues plus complexes et radicales, notamment en ce qui concerne les questions liées à la propagation de l'infection par la COVID-19.

Royaume-Uni

Campagne « Shared Values » (Valeurs communes) du Royaume-Uni

La campagne Shared Values est une campagne de contremarque qui rassemble un partenariat mondial de gouvernements et d'organisations démocratiques afin de promouvoir des messages positifs sur la force durable et le leadership mondial du partenariat, ainsi que sur les valeurs libérales communes qui les lient. Les partenaires de la campagne, qui se sont joints à l'activité sur une base modulaire, sont le Canada, le Danemark, l'Estonie, la Finlande, l'Allemagne, la Lituanie, la Lettonie, la Slovaquie, l'Ukraine, le Royaume-Uni et les États-Unis d'Amérique, la Fondation Westminster pour la démocratie et la Communauté des démocraties. Depuis son lancement, l'activité au niveau mondial a atteint une portée organique de 33 millions de personnes dans 163 pays, alors que 84 organisations de la société civile diffusent organiquement le contenu. Au niveau local, la campagne a ciblé les « publics réticents à la démocratie », vulnérables à la désinformation qui mine la démocratie en Europe de l'Est. Le bilan de l'après-campagne a montré une augmentation de 11 % de la perception de la démocratie comme « assez importante », une augmentation de 2 % de la préférence du public pour les gouvernements démocratiques, une augmentation de 16 % de la sensibilisation aux comportements démocratiques sains et un taux moyen de reconnaissance de la campagne de 20 % dans toute la région.

États-Unis

*Le Global Engagement Center publie des **dépêches anti-désinformation***

Le GEC publie des rapports d'exposition et des dépêches anti-désinformation qui résument les leçons retenues sur la désinformation et la manière de lutter contre celle-ci, à partir des expériences des praticiens de première ligne, au profit de ceux qui, dans d'autres pays, sont nouvellement actifs dans ce domaine. Le lectorat des dépêches s'est élargi pour inclure une vaste communauté de fonctionnaires, de dirigeants de la société civile et de chercheurs universitaires du monde entier. Les dépêches précédentes ont traité de la désinformation sur la COVID-19, des leçons à tirer pour rendre la démystification plus efficace, de la stratégie sous-jacente et du contexte historique des tactiques de désinformation de la Russie,ainsi que du rôle des agents d'influence contrôlés par l'État dans les opérations de désinformation. Les dépêches sont disponibles sur le site www.state.gov/disarming-disinformation, et ici en anglais. Certains numéros sont également disponibles en russe, en espagnol, en français et en arabe. Pour ajouter votre nom à la liste de distribution des futures dépêches anti-désinformation, veuillez leur envoyer un courriel.

Australie

ASIO met au jour un complot d'ingérence étrangère

Récemment, l'Australian Security Intelligence Organisation (ASIO) (service de renseignements intérieur australien) a détecté et démantelé un complot d'ingérence étrangère à l'approche d'une élection en Australie. Un individu qui entretenait des liens directs et profonds avec un gouvernement étranger et ses agences de renseignement a cherché à façonner la scène politique au profit de la puissance étrangère. La tromperie et le secret délibérés concernant les liens avec le gouvernement étranger ont fait entrer l'affaire dans le domaine de l'ingérence étrangère. L'intervention de l'ASIO a permis de s'assurer que le plan n'était pas exécuté et d'éviter tout préjudice.

Nouvelle-Zélande

Menaces d'espionnage et d'ingérence étrangère : conseils de sécurité pour les députés néo-zélandais et les élus locaux

La sensibilisation à l'incidence possible de l'ingérence étrangère sur l'économie, la démocratie et la réputation internationale de la Nouvelle-Zélande reste un domaine hautement prioritaire pour le gouvernement néo-zélandais. Nous avons observé des indicateurs concernant l'établissement de relations et le versement de dons par des acteurs étatiques et leurs mandataires, couvrant l'ensemble de l'éventail politique tant au niveau du gouvernement central qu'au niveau des administrations locales. En mars 2021, un livret intitulé Espionage and Foreign Interference Threats: Security Advice for members of the New Zealand Parliament and Locally Elected Representatives a été rendu publique sous la bannière du cadre des exigences en matière de sécurité et de protection de la Nouvelle-Zélande. Le livret (en anglais) appuie le travail de sensibilisation du gouvernement néo-zélandais à l'ingérence étrangère, en informant les élus du gouvernement central et des administrations locales de la manière dont ils peuvent être ciblés et exploités, et de ce qu'ils peuvent faire pour se protéger.

Suède

La Suède met sur pied l'Agence de défense psychologique

La Suède, qui a adhéré au MRR en tant qu'observatrice en 2021, a créé une nouvelle agence gouvernementale, à savoir l'Agence suédoise de défense psychologique, chargée de déceler, d'analyser, de prévenir et de combattre les influences indues dans l'information et d'autres renseignements trompeurs visant la Suède ou les intérêts suédois, tant au niveau national qu'au niveau international. L'Agence jouera un rôle opérationnel, mais en plus, ce qui est important, elle aura aussi le mandat de renforcer les capacités au sein de la société suédoise.

Service européen pour l'action extérieure

Une approche multipartite pour lutter contre la manipulation de l'information et l'ingérence étrangères

En 2021, le SEAE, en étroite collaboration avec d'autres institutions de l'UE, a dirigé les travaux sur un cadre global de lutte contre la manipulation de l'information et l'ingérence étrangères fondé sur 3 aspects : une définition conceptuelle commune de la menace et de toutes ses facettes, un cadre analytique et une méthode communs, et une boîte à outils actualisée pour lutter contre la manipulation de l'information et l'ingérence étrangères[28]. L'équipe de la communication stratégique, avec ses groupes de travail spécialisés sur les pays voisins d'Europe de l'Est, les Balkans occidentaux et le Sud, s'est employée à améliorer la connaissance de la situation et à dénoncer les activités de manipulation de l'information et d'ingérence étrangères, et a contribué à renforcer la résilience de la société. Le système d'alerte rapide a démontré son importance, en permettant d'échanger rapidement avec les institutions de l'UE, les États membres et les partenaires internationaux des analyses, des pratiques exemplaires et du matériel de communication. Le SEAE a également intensifié son travail pour aider les partenaires de la région à s'attaquer au problème de la manipulation de l'information et de l'ingérence, par exemple dans les Balkans

28 Rapport d'activités de la communication stratégique du SEAE 2021 : https://www.eeas.europa.eu/sites/default/files/documents/Report%20Stratcom%20activities%202021.pdf (en anglais)

occidentaux, qui sont actuellement la cible de campagnes systématiques de manipulation de l'information et d'ingérence étrangères menées par l'écosystème pro-Kremlin. Il a également élaboré des approches et des outils permettant aux partenaires d'imposer des coûts aux acteurs de la manipulation de l'information et de l'ingérence étrangères. Tout au long de l'année 2021, le SEAE a renforcé ses activités d'analyse et de dénonciation de la manipulation de l'information et de l'ingérence, notamment par son site Web sur la question, EUvsDisinfo, et les nombreuses activités de sensibilisation et de formation dans le cadre d'une campagne plus large.

Organisation du Traité de l'Atlantique Nord (OTAN)

Programme de subventions de l'OTAN pour la résilience

L'OTAN poursuit la mise en œuvre de son programme #OTAN2030 afin d'être en mesure de faire face aux défis de sécurité actuels et à venir. En 2020 et 2021, la Division Diplomatie publique de l'OTAN a attribué des subventions visant à renforcer la résilience face à la désinformation et aux activités d'information hostiles dans les pays de l'OTAN. Des organisations non gouvernementales, des groupes de réflexion et des universités ont été invités à présenter des projets novateurs. En 2020, 30 projets ont obtenu un appui avec un budget total de 310 000 euros, et en 2021, 35 propositions de projet ont été soutenues avec un financement total de 425 000 euros. Les projets sélectionnés comprenaient des initiatives axées sur l'éducation aux médias, la recherche et le développement de jeux éducatifs en ligne.

PROCHAINES ÉTAPES POUR LE MRR DU G7

En 2022, la communauté du MRR du G7 mettra en œuvre un large éventail d'activités visant à renforcer la collaboration dans les domaines clés suivants :

- renforcer les connaissances et les capacités pour lutter contre les menaces étrangères au sein du MRR du G7 et avec les partenaires clés;
- élaborer des méthodes et des outils communs d'analyse de données pour repérer les menaces étrangères;
- renforcer la capacité du MRR du G7 à répondre de manière coordonnée aux menaces étrangères;
- soutenir la recherche pour évaluer les fondements possibles de l'élaboration de normes en matière de manipulation de l'information et d'ingérence étrangères;
- renforcer la collaboration avec d'autres organisations et initiatives internationales, la société civile, le milieu universitaire et l'industrie pour repérer les menaces étrangères et lutter contre celles-ci;
- communiquer les travaux du MRR du G7 aux divers publics du G7 au moyen d'un deuxième rapport annuel portant sur les menaces étrangères à la démocratie.

Sous les auspices de la présidence allemande du G7, et tout en continuant à se concentrer sur la lutte contre la désinformation, le MRR du G7 étudiera également les possibilités de collaboration pour faire face aux menaces à la démocratie découlant de l'avènement de nouvelles technologies ou visant la sécurité économique et de la recherche, y compris à l'échelle locale.

ANNEXE I

PROTÉGER LA DÉMOCRATIE

MÉCANISME DE RÉPONSE RAPIDE DU G7

PLAN D'ACTION

2021

MANDAT

Le mandat du MRR du G7 consiste à renforcer la coordination du G7 dans le but de cerner les menaces étrangères diverses et en constante évolution qui pèsent sur les démocraties du G7 et y réagir, notamment en mettant en commun l'information et les analyses, et en déterminant des possibilités de réponse coordonnée. Les responsables du MRR du G7 axent leurs efforts, sans toutefois s'y limiter, sur les menaces qui pèsent sur 1) les institutions et les processus démocratiques; 2) les écosystèmes d'information et les médias; 3) les libertés fondamentales et les droits de la personne.

PROGRÈS RÉALISÉS EN 2020

Le MRR du G7 a fait de très grands progrès en matière d'échange d'information. Les responsables du Mécanisme ont commencé à tenir des réunions mensuelles regroupant les agents de coordination du MRR du G7+1 [1], qui concernent aussi les mises à jour nationales et les leçons retenues, ainsi que des échanges bihebdomadaires au niveau des analystes. Grâce au Mécanisme, on a pu mettre en place un portail en ligne sécurisé d'échange d'information sous les auspices des États-Unis, au moyen duquel les rapports du G7+ sont communiqués et des échanges analytiques ont lieu. Le Mécanisme a aussi continué à produire son fil d'actualité mensuel non classifié, qui met en lumière des idées originales, diffuse les nouveaux développements et cerne les partenariats potentiels pour la défense de la démocratie. Enfin, les responsables du Mécanisme ont conclu un accord en matière d'échange d'information avec les intervenants du système d'alerte rapide de l'Union européenne.

L'échange d'information dans le cadre du MRR du G7 a été mis à l'essai et a fait ses preuves dans le contexte de la COVID-19. Les responsables du Mécanisme se sont rapidement concentrés sur la pandémie au cours du premier trimestre, en soutenant un échange d'analyses en temps réel des menaces étrangères, qui comprenait les partenaires de l'industrie et des organisations de la société civile, en particulier pour ce qui est de l'évolution de la manipulation de l'information par des États étrangers. Les responsables du MRR du G7 ont également soutenu les directeurs politiques du G7 en pilotant une proposition du G7 sur la protection des valeurs communes pour contrer la désinformation parrainée par l'État relative à la COVID-19, sous les auspices de la présidence américaine du G7. Bien que le Sommet des dirigeants de 2020 n'ait finalement pas eu lieu, des éléments de la proposition ont été repris par des membres du G7 et des partenaires aux vues similaires.

Les membres du G7 ont mis de l'avant des initiatives de collaboration, y compris un rapport conjoint rédigé par 2 membres et portant sur les nouvelles tactiques d'amplification des discours et de désinformation liées à la COVID-19, et un autre rapport sur cette dynamique destiné à tous les États membres du G7+.

1 Le MRR du G7+ regroupe les membres et les observateurs du MRR du G7. Les membres du MRR du G7 sont le Canada, la France, l'Allemagne, l'Italie, le Japon, le Royaume-Uni, les États-Unis et l'Union européenne. Les observateurs du MRR du G7 sont l'Australie, la Nouvelle-Zélande et les Pays-Bas. Chaque membre et chaque observateur est représenté par un agent de coordination lors des réunions mensuelles du Mécanisme.

OBJECTIFS POUR 2021

Les agents de coordination ont convenu des objectifs suivants pour 2021 :

1. Améliorer la compréhension commune de toutes les menaces étrangères à la démocratie, y compris, mais sans s'y limiter, les élections et la désinformation.
2. Maintenir de solides plateformes d'échange d'information et continuer à accroître l'échange d'information sur l'évolution de la situation et les leçons retenues au niveau national, les évaluations et les analyses en temps réel.
3. Renforcer les cadres éthiques et méthodologiques respectifs aux fins du suivi et de l'analyse des données ouvertes dans le contexte de l'évolution des tactiques et des tendances au chapitre de la désinformation en ligne.
4. Acquérir une compréhension commune de ce qui constitue une ingérence étrangère par opposition à une influence légitime dans le but d'élaborer des normes communes.
5. Renforcer la relation hiérarchique entre le MRR du G7 et les directeurs politiques du G7 afin de faciliter une réponse coordonnée.
6. Renforcer la collaboration touchant d'autres organisations et initiatives internationales dotées d'un mandat similaire, afin d'éviter les dédoublements et de tirer parti de la valeur ajoutée.
7. Renforcer la collaboration avec les organisations de la société civile et les milieux universitaires afin d'accroître la sensibilisation et la résilience du public, et coordonner les programmes de recherche et de renforcement des capacités afin d'en optimiser les effets.
8. Coordonner, le cas échéant, la collaboration avec les entreprises de médias sociaux.
9. Communiquer les travaux du MRR du G7 aux publics du G7 au moyen de rapports annuels sur les menaces étrangères pesant sur la démocratie.

ENGAGEMENTS POUR 2021

Afin d'atteindre les objectifs du MRR, les agents de coordination ont convenu des engagements suivants pour 2021 :

- Accroître l'échange d'information fondée sur l'évolution de la situation, les leçons retenues et les évaluations à l'échelle nationale en contribuant aux réunions mensuelles du MRR du G7, à la plateforme IQ du Global Engagement Center des États-Unis et au Fil d'actualité, y compris en mobilisant, s'il y a lieu, les ministères et les organismes des gouvernements nationaux respectifs.
- Faciliter la participation nationale aux réunions bihebdomadaires de la communauté de pratique d'analyse des données ouvertes, en entreprenant des projets conjoints d'analyse des données ouvertes et en élaborant une terminologie, des outils et des méthodes d'analyse des données communs.
- Soutenir un groupe de travail, sous la direction des États-Unis, sur le renforcement des capacités de suivi et d'analyse des données ouvertes en vue de 1) renforcer la capacité d'analyse du MRR du G7; 2) synchroniser le travail d'analyse du MRR du G7 afin d'éviter le double emploi et d'optimiser les effets; 3) renforcer les capacités des pays tiers.
- Soutenir un groupe de travail, sous la direction de l'Union européenne, afin de faire la distinction entre l'influence (activité légitime) et l'ingérence (activité illégitime), en mettant l'accent sur la désinformation; le cadre conceptuel servira de base pour définir des seuils qui permettront de déclencher d'éventuelles réponses coordonnées.
- Faire participer les directeurs politiques respectifs du G7 au travail des responsables du MRR du G7.
- Informer les responsables du MRR du G7 des travaux actuellement exécutés dans les organisations et les initiatives internationales ayant un mandat similaire, y compris l'OTAN et le Centre d'excellence

pour la communication stratégique de l'OTAN, et le Centre d'excellence européen pour la lutte contre les menaces hybrides, et recenser les possibilités de collaboration et de règlement des conflits, notamment en accueillant des observateurs supplémentaires.

- Soutenir et diffuser la recherche sur les menaces étrangères à la démocratie en partenariat avec le milieu universitaire et les organisations de la société civile, de concert avec les partenaires du MRR du G7, le cas échéant.
- Dégager et élaborer des positions communes aux fins d'une collaboration avec les entreprises de médias sociaux.
- Rédiger un rapport du MRR du G7 sur la désinformation qui sera diffusé auprès des publics respectifs.

L'Unité de coordination a convenu d'effectuer les activités suivantes en 2021 :

- Convoquer les réunions du MRR.
- Faciliter la circulation et la gestion du contenu pertinent à l'échelle du réseau du MRR, notamment par le truchement de la plateforme du Global Engagement Center (GEC-IQ) et du système d'alerte rapide.
- Produire le fil d'actualité du MRR.
- Entreprendre des analyses de données ouvertes et rédiger des rapports sur la désinformation.
- Coordonner et faciliter les initiatives et les partenariats du MRR.
- Soutenir la présidence britannique du G7 en vue des préparatifs aux réunions ministérielles et au Sommet.