Rapport annuel 2022

PROTÉGER LA DÉMOCRATIE

MÉCANISME DE RÉPONSE RAPIDE DU

G7

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 étroite collaboration avec l'Allemagne, en tant que pays hôte du G7 en 2022, et 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

PROTÉGER LA DÉMOCRATIE

MÉCANISME DE RÉPONSE RAPIDE DU

G7

INTRODUCTION

Lors du Sommet du G7 à Charlevoix, en 2018, les dirigeants ont mis en place le Mécanisme de réponse rapide du G7 (MRR du G7), qui renforce la coordination entre les pays du G7 afin de déceler les diverses menaces étrangères contre la démocratie et d'y répondre. Ces menaces, en constante évolution, comprennent les activités d'États hostiles visant nos institutions et nos processus démocratiques, notre environnement médiatique et de l'information, 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 processus institutionnels respectifs pour favoriser une participation pangouvernementale. Le Canada dirige le MRR du G7 de façon permanente.

Lors de la réunion des ministres des Affaires étrangères et du Développement du G7 à Londres, en 2021, les ministres des affaires étrangères se sont engagés à produire des rapports annuels du MRR du G7. Ces rapports abordent différents aspects du paysage changeant des menaces et proposent des possibilités de réponses, certaines proactives, qui pourraient être prises par les membres et les observateurs afin de sensibiliser le public et renforcer sa résilience. Alors que le rapport de 2021 se concentrait sur la désinformation en tant que vecteur spécifique des activités de manipulation de l'information et d'ingérence étrangères, le rapport de 2022 se concentre sur le phénomène plus large des menaces hybrides, y compris des exemples spécifiques rencontrés par la communauté du MRR du G7 en 2022.[1]

Le rapport de 2022 est structuré comme suit :

1. Vue d'ensemble des menaces hybrides auxquelles le MRR du G7 a été confronté en 2022
2. Mises à jour sur les menaces posées par les activités de manipulation de l'information et d'ingérence étrangères et les mesures prises par les gouvernements pour protéger leurs élections nationales contre ces menaces
3. Description des activités du MRR du G7 au cours de l'année passée
4. Exemples d'initiatives prises par les membres du MRR du G7 en réponse à des menaces étrangères

1 Selon le Centre d'excellence européen pour la lutte contre les menaces hybrides (Hybrid CoE), l'expression « menace hybride » désigne une action menée par des acteurs étatiques ou non étatiques, dans le but de saper ou de nuire à une cible en influençant sa prise de décision aux niveaux local, régional, étatique ou institutionnel. Ces actions sont coordonnées et synchronisées et ciblent délibérément les vulnérabilités des États et des institutions démocratiques dans les domaines politique, économique, militaire, civil ou de l'information. Pour plus d'information, voir le site Web du Centre d'excellence européen pour la lutte contre les menaces hybrides (en anglais).

LES MENACES HYBRIDES AU CENTRE DE L'ATTENTION EN 2022

En 2022, la guerre de la Russie contre l'Ukraine a dominé le paysage des menaces internationales. Alors que le monde entier commençait à se relever de la pandémie de COVID-19, la guerre d'agression menée par la Russie contre l'Ukraine a retenu l'attention des gouvernements démocratiques et a contesté l'ordre international fondé sur des règles. En juin 2022, le communiqué des dirigeants du G7 a défini la situation comme un « moment crucial pour la communauté internationale »[2]. Le chancelier allemand, Olaf Scholz, l'a quant à lui qualifiée de *Zeitenwende*, un « tournant historique »[3].

Dans le contexte de cette invasion à grande échelle, les menaces hybrides sont devenues une préoccupation majeure pour les démocraties du monde entier. On peut considérer ces menaces comme un mélange d'activités coercitives et subversives réalisées à l'aide de méthodes conventionnelles et non conventionnelles dans différents domaines, notamment diplomatique, militaire, économique et technologique. Les acteurs étatiques et leurs mandataires peuvent utiliser les activités hybrides de manière coordonnée afin de poursuivre des objectifs spécifiques, tout en restant en deçà du seuil de la guerre formelle[4].

En raison de leur nature nébuleuse et de leur vaste portée, les activités hybrides peuvent être difficiles à reconnaître et à contrer. Ce rapport met en lumière plusieurs menaces hybrides qui ont retenu l'attention du MRR du G7 en 2022, notamment :

1. Les tentatives de manipulation de l'information visant à saper les processus et institutions démocratiques, y compris au niveau infranational
2. La désinformation et les cyberattaques survenues lors de l'invasion massive de l'Ukraine
3. La coercition économique et l'espionnage scientifique pour poursuivre des objectifs stratégiques

LES TENTATIVES DE SAPER LES PROCESSUS ET INSTITUTIONS DÉMOCRATIQUES

Pour atteindre leurs objectifs, les acteurs étatiques étrangers et leurs mandataires exploitent les vulnérabilités des sociétés ouvertes. Ils le font à la fois au niveau national et infranational (sous le niveau fédéral), affectant ainsi les institutions publiques, les entreprises privées, les communautés et les personnes. Ils tentent d'influencer l'opinion publique et les comportements, de modifier les politiques et de perturber les processus démocratiques, et comprennent les tentatives d'ingérence des gouvernements russe et chinois dans les élections[5]. Ces acteurs déploient un large éventail d'activités hybrides, dont la manipulation de l'information, afin de supprimer les voix indépendantes ou critiques, fomenter la division ou promouvoir des messages favorables à leurs intérêts nationaux tout en érodant l'intégrité de nos environnements d'information et de l'ordre international fondé sur des règles[6].

INFORMATION ET CYBERATTAQUES

L'agression militaire de la Russie contre l'Ukraine s'est accompagnée d'un large éventail d'activités hybrides, notamment des attaques basées sur l'information. Les acteurs alignés sur l'État russe et leurs intermédiaires se sont livrés à une ingérence et à une manipulation de l'information à l'échelle mondiale

2 Communiqué des dirigeants du G7, Elmau, 28 juin 2022 (en anglais).
3 Voir Scholz, Olaf The Global Zeitenwende, publié à l'origine en allemand le 5 décembre 2022 (en anglais).
4 Voir la Communication conjointe au Parlement européen et au Conseil, intitulée Cadre commun en matière de lutte contre les menaces hybrides, une réponse de l'Union européenne, Commission européenne, juin 2016.
5 China's Growing Attempts to Influence U.S. Politics, Council on Foreign Relations, 31 octobre 2022 (en anglais) ; Chinese interference: What government documents tell us about election meddling, Global News, 16 décembre 2022 (en anglais); Rapport sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, A9-0022/2022, Parlement européen, 9 février 2022.
6 Voir notamment The Landscape of Hybrid Threats: A Conceptual Mode et Hybrid Threats: A Comprehensive Resilience Ecosystem, Centre d'excellence européen pour la lutte contre les menaces hybrides, Hybrid CoE (Hybrid CoE), "

afin de légitimer la guerre illégale menée par la Russie, de saper le soutien de l'opinion publique à l'Ukraine et de détourner la responsabilité de l'insécurité alimentaire et des perturbations économiques et énergétiques.

Selon toute vraisemblance, ces fausses informations visaient à saper la cohésion entre les partenaires d'optique commune et au sein de la communauté internationale. Ils ont cherché à alimenter le ressentiment entre les pays industrialisés et les pays émergents et en développement. Ces activités ont eu un effet négatif sur les conditions politiques et économiques en Afrique, en Asie et en Amérique latine, où la Russie et la Chine ont toutes deux cherché à créer des dépendances[7]. Les cyberattaques généralisées et continuelles de la Russie contre des infrastructures civiles critiques et des organismes gouvernementaux ukrainiens, qui fournissent des services essentiels, sont contraires aux attentes de tous les États membres des Nations Unies en matière de comportement responsable des États dans le cyberespace[8].

COERCITION ÉCONOMIQUE, ESPIONNAGE SCIENTIFIQUE ET SABOTAGE

Ces défis mondiaux ont mis l'accent sur la nécessité de protéger les entreprises privées, en particulier leur valeur et leurs chaînes d'approvisionnement, ainsi que les établissements de recherche contre l'influence illégitime, l'espionnage, les fuites illicites de connaissances et le sabotage, tant en ligne que hors ligne[9]. En outre, la coercition économique et diplomatique, notamment sous forme de menaces implicites ou explicites visant à restreindre le commerce ou les discussions sur les droits de la personne, est de plus en plus utilisée comme tactique hybride dans la poursuite d'objectifs stratégiques.

Dans ce contexte, les États étrangers hostiles et les acteurs affiliés cherchent à acquérir de l'information sur des questions d'importance économique et politique[10]. Ces activités font appel à des ressources humaines et financières, ouvertement ou secrètement, pour obtenir un avantage en matière de connaissances et combler leurs lacunes en matière de compétences ou d'expertise. Elles peuvent également servir à détecter les vulnérabilités existantes en vue d'une exploitation future au moyen d'attaques hybrides.

Ainsi, les investissements contrôlés par l'État ou l'envoi de scientifiques parrainés par l'État pour travailler dans des secteurs d'intérêt dans le pays cible peuvent être utilisés pour obtenir des technologies, de l'expertise ou de la propriété intellectuelle. Bien que prétendument légales, ces activités peuvent se traduire par des risques accrus pour nos économies et nécessitent des réponses soigneusement calibrées qui combinent la prévention, la détection et l'imposition de conséquences plus sévères pour les auteurs d'activités hostiles, tout en maintenant les possibilités de collaboration et d'innovation et en assurant la promotion de celles-ci.

7 En ce qui concerne l'influence à long terme sur les structures locales et la création de dépendances à long terme, voir par exemple le rapport d'experts de Gelpern, Horn, Morris et al. intitulé How China lends, Kiel Institute for the World Economy, mai 2021 (en anglais).

8 Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless, Wired, 18 novembre 2022 (en anglais); Cyberopérations russes contre l'Ukraine : déclaration du haut représentant au nom de l'Union européenne, Conseil de l'Union européenne, 10 mai 2022.

9 À titre de référence seulement, voir le communiqué des dirigeants du G7 à Hiroshima lors du sommet du G7 à Hiroshima, mai 2023 (en anglais).

10 Voir Hunter, Impiombato et al, Countering China's coercive diplomacy, Australian Strategic Policy Institute (ASPI), février 2023 (en anglais) ; Adachi, Brown, Zenglein, Fasten your seatbelts: How to manage China's economic coercion , MERICS China Monitor, août 2022 (en anglais) ; Hackenbroich, Jonathan, Tough Trade: The hidden costs of economic coercion, Conseil européen pour les relations internationales, février 2022 (en anglais).

RETOMBÉES ET RÉPONSE

L'utilisation par la Russie de la manipulation de l'information en tant qu'instrument crucial de sa guerre d'agression contre l'Ukraine est d'une intensité sans précédent. De façon plus générale, les gouvernements autoritaires utilisent la manipulation de l'information et l'ingérence comme vecteurs clés pour exercer une influence politique illégitime. D'autres formes de menaces hybrides, dont la coercition économique, l'espionnage scientifique et le sabotage, s'étendent dans la communauté du MRR du G7 et se manifestent au niveau infranational, communautaire ou individuel.

La lutte contre ces menaces nécessite une coordination entre les gouvernements, les secteurs, les niveaux de gouvernement et les politiques. Si des structures visant à contrer les menaces hybrides au niveau national ont été mises en place dans certains pays du G7 et dans des pays observateurs[11], l'ingérence étrangère au niveau infranational reste un défi de taille. Il nous incombe de continuer à travailler au-delà des frontières de la politique intérieure et étrangère et de renforcer la collaboration avec les partenaires de l'industrie, du milieu universitaire et de la société civile.

Conscients de cette réalité, les pays du MRR du G7 ont commencé en 2022, sous la présidence de l'Allemagne, à échanger de l'information et des pratiques exemplaires afin de mieux comprendre comment les menaces infranationales se manifestent.

Ainsi, vers la fin de l'année 2022, la question de la répression transnationale a été propulsée sur le devant de la scène à la suite d'une série de rapports de la société civile sur les activités policières transnationales de la République populaire de Chine (RPC) dans le monde entier[12]. La répression transnationale – y compris, mais pas uniquement, ces «stations d'outre-mer» – est devenue une préoccupation majeure pour les gouvernements démocratiques, y compris pour les membres du MRR du G7, en raison de la multiplication de cas d'acteurs étatiques étrangers intimidant les communautés de la diaspora, les défenseurs des droits de la personne et d'autres voix critiques ayant fui des régimes répressifs, et en raison d'autres risques qu'ils peuvent faire peser sur les sociétés démocratiques.

En 2023, l'identification d'approches efficaces pour contrer la répression transnationale et autres menaces infranationales sera au centre des préoccupations des membres du MRR du G7 et de leur collaboration renforcée.

11 Voir la stratégie de sécurité nationale des États-Unis, octobre 2022 (en anglais); la Revue nationale stratégique 2022 de la France, novembre 2022; la stratégie de sécurité nationale du Japon, décembre 2022 (en anglais); la stratégie de sécurité des Pays-Bas, avril 2023 (en anglais); la stratégie de sécurité nationale de l'Allemagne, juin 2023 (en anglais). Voir également le rapport de l'UE A9-0022/2022, intitulé Rapport sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, février 2022, qui appelle à une stratégie de l'UE sur l'ingérence étrangère, y compris la désinformation.

12 110 Overseas: Chinese Transnational Policing Gone Wild, Safeguard Defenders, septembre 2022 (en anglais), et Patrol and Persuade: A follow-up investigation to 110 Overseas, Safeguard Defenders, décembre 2022 (en anglais).

MESURES PRISES PAR LES GOUVERNEMENTS POUR PROTÉGER LES ÉLECTIONS NATIONALES EN 2022

En 2022, les préoccupations relatives à la manipulation de l'information et à l'ingérence étrangères par des États étrangers ont constitué un vecteur de menace important pour les élections nationales et infranationales dans le monde entier, y compris dans les pays membres et observateurs du MRR du G7. Bien que les cas de manipulation de l'information et d'ingérence étrangères ne soient pas propres aux élections, les campagnes électorales sont souvent les points d'appui autour desquels les activités de certains États hostiles s'intensifient dans le but probable d'influencer les résultats électoraux, de saper la confiance dans les processus et les institutions démocratiques, ou de favoriser la polarisation.

À l'automne 2021, le Service français de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a lancé des opérations visant à protéger les élections présidentielles et législatives de 2022 en **France** contre la manipulation de l'information et l'ingérence étrangères. Le Service a travaillé en étroite collaboration avec les principaux intervenants nationaux chargés de préserver l'intégrité des élections, notamment le ministère de l'Intérieur, la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle et le Conseil constitutionnel. Le Service a également établi des collaborations avec des plateformes numériques et organisé des séances de sensibilisation à l'intention des partis politiques. Tout au long de ces élections, VIGINUM a travaillé en étroite coordination avec ses partenaires pour garantir des réponses rapides et souples aux éventuels incidents. Il a accordé une attention particulière aux messages qui risquaient de saper la crédibilité du processus électoral, tant avant qu'après les élections. Dans l'ensemble, bien qu'aucune campagne malveillante majeure n'ait été identifiée, VIGINUM a détecté 60 cas d'activité inauthentique sur des plateformes numériques, dont cinq ont été classés comme ingérence numérique étrangère.

En 2022, l'Agence suédoise de défense psychologique (PDA) a collaboré avec des partenaires nationaux, notamment l'administration électorale, la police, les services numériques et les services de renseignement, afin de protéger la **Suède** contre toute ingérence étrangère lors de l'élection générale de septembre. L'agence s'est préparée à un scénario catastrophe basé sur une évaluation des capacités et des intentions des acteurs de la menace étrangère de s'ingérer dans l'élection ou les infrastructures critiques au niveau local, régional et national. L'agence a présenté un rapport sur les menaces et les vulnérabilités au gouvernement et aux intervenants concernés afin d'accroître la sensibilisation et la résilience. Afin de sensibiliser le public, l'agence a également lancé une campagne d'information « Ne vous laissez pas berner », à l'été 2022. La campagne a décrit les méthodes et les outils des adversaires afin d'aider les citoyens à rester vigilants face aux ingérences malveillantes. L'agence a organisé des séances de formation pour le personnel clé de l'administration électorale et sur demande, pour les journalistes et les représentants des partis politiques. En fin de compte, bien que des tentatives d'influence de l'opinion politique par des acteurs étrangers aient été détectées, l'APD a estimé que l'ingérence étrangère n'avait pas affecté l'élection ou le processus électoral suédois.

En **Italie**, les autorités nationales ont surveillé de près les médias sociaux et traditionnels pendant la campagne électorale en vue des élections législatives de septembre. Elles ont détecté une campagne de désinformation russe ciblant les dirigeants politiques et les candidats avec des messages favorables à l'invasion illégale de l'Ukraine par la Russie, mais elle n'a pas eu d'impact significatif.

Avant son élection fédérale de mai 2022, l'**Australie** avait créé l'*Electoral Integrity Assurance Taskforce* (EIAT) pour conseiller le commissaire aux élections sur les questions susceptibles de compromettre l'intégrité des élections. L'EIAT est un mécanisme intergouvernemental chargé d'évaluer, de comprendre et d'atténuer les menaces qui pèsent sur l'intégrité électorale et, le cas échéant, de conseiller le commissaire aux élections sur la façon de gérer ces menaces. Après l'élection, le commissaire aux élections australien, Tom Rogers, a déclaré que l'EIAT n'avait pas détecté d'ingérence étrangère, ou toute autre ingérence, susceptibles de compromettre l'organisation de l'élection fédérale de 2022 ou d'ébranler la confiance du peuple australien dans les résultats de l'élection.

Avant les élections de mi-mandat en 2022 aux **États-Unis**, la *Cybersecurity and Infrastructure Security Agency* (CISA) a procédé à des évaluations de la sécurité des infrastructures électorales et à une analyse des vulnérabilités en matière de cybersécurité dans des centaines d'administrations électorales américaines. La CISA a facilité l'échange d'information par l'intermédiaire de l'*Election Infrastructure Information Sharing and Analysis Center*, qui compte 3 400 membres et qui constitue une source d'information en temps réel sur les menaces et les mesures d'atténuation, afin d'aider les administrateurs électoraux locaux et des États à comprendre l'environnement des risques en matière de sécurité électorale. La CISA a également organisé des séances de formation, des exercices, des tables rondes et des discours dans l'ensemble des États-Unis, touchant plus de 5 000 entités locales, étatiques, fédérales, internationales et privées ayant un rôle à jouer dans la sécurité et la fiabilité des élections. En outre, les organismes fédéraux américains chargés de l'application de la loi et du renseignement ont surveillé les menaces étrangères, échangé de l'information et fourni une assistance en matière de sécurité électorale aux autorités électorales locales et étatiques, ainsi qu'au secteur privé. À la suite des élections, la directrice de la CISA, Jen Easterly, a publié une déclaration indiquant qu'il n'y avait aucune preuve indiquant qu'un système de vote « ait supprimé ou perdu des votes, modifié des votes ou ait été compromis de quelque manière que ce soit lors d'une élection dans le pays. »

TENDANCES EN MATIÈRE DE MANIPULATION DE L'INFORMATION ET D'INGÉRENCE ÉTRANGÈRES

Le rapport annuel 2021 du MRR du G7 mettait l'accent sur la désinformation en tant que vecteur de la manipulation de l'information et de l'ingérence étrangères, et cela a continué à être le cas tout au long de l'année 2022[13] La désinformation était le sujet principal de la conférence du G7 sur le MRR qui s'est tenue à Berlin en 2022[14].

Au cours de l'année, les tactiques et méthodes de manipulation de l'information employées par les acteurs étatiques étrangers se sont élargies en termes de cibles et de sophistication. Ainsi, la Russie s'en prend de plus en plus aux femmes ou aux personnes LGBTQI+ en Italie, en Tunisie, au Brésil et en Hongrie, tandis que l'Iran se livre à des opérations de cyberinfluence et de harcèlement en ligne[15]. La Russie cherche de plus en plus à manipuler l'environnement mondial de l'information, notamment en utilisant des sites Web «clonés» de médias internationalement connus (par exemple, *Der Spiegel* ou CNN)[16] ou en soutenant la croissance d'une «industrie de la désinformation» commerciale[17]. Nous pensons que ces phénomènes vont probablement s'amplifier dans les années à venir, affectant ainsi les institutions et les sociétés plus sensibles, en particulier celles où la résilience à la manipulation de l'information et l'ingérence étrangères reste faible, comme l'Allemagne[18].

Dans ce contexte, l'évolution continue des technologies de l'intelligence artificielle (IA) générative et des médias synthétiques – dont les grands modèles de langage, les puissants robots conversationnels, la génération d'images et de vidéos, et les logiciels de simulation vocale – présente de nouveaux défis. Ces avancées technologiques permettent de créer, en quelques secondes, des contenus complexes, de haute qualité et inquiétants. Ainsi, les outils de génération d'images peuvent créer des photos et des vidéos d'apparence authentique d'événements qui n'ont jamais eu lieu, tandis que les logiciels de génération de voix peuvent imiter de manière convaincante la voix d'une personne à partir d'un bref échantillon de voix[19]. Ces capacités médiatiques synthétiques, en particulier lorsqu'elles sont automatisées, pourraient accroître considérablement la production et la propagation de campagnes de désinformation ou présenter des «réalités» manipulées à grande échelle et dans le monde entier[20].

En 2022, le MRR du G7 a identifié les huit tendances notables suivantes grâce à des recherches primaires et secondaires au sein de la communauté du MRR du G7.

13 Voir le premier rapport du SEAE sur les tentatives étrangères visant à influencer les processus démocratiques européens, février 2023 (en anglais).

14 Voir le communiqué des dirigeants du G7, juin 2022 (en anglais), la déclaration des ministres de l'Intérieur et de la Sécurité du G7, novembre 2022 (en anglais), le communiqué des ministres des Affaires étrangères du G7, mai 2022 (en anglais), et le communiqué des ministres des Médias du G7, juin 2022 (en anglais).

15 Voir Di Meco, Monetizing Misogyny – Gendered Disinformation and the Undermining of Women's Rights and Democracy Globally, ShePersisted, février 2023 (en anglais), et Jankowicz, Hunchak et al, Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, Wilson Center, janvier 2021 (en anglais). En ce qui concerne l'Iran, voir Watts, Rinse and repeat: Iran accelerates its cyber influence operations worldwide, Microsoft, 2 mai 2023 (en anglais).

16 Voir par exemple Alaphilippe, A. et al, Doppelgänger – Media clones serving Russian propaganda, EU Disinfo Lab, septembre 2022 (en anglais). Voir le rapport de VIGINUM intitulé RRN: une campagne numérique de manipulation de l'information complexe et persistante, 13 juin 2023.

17 Voir le rapport du laboratoire d'innovation d'Europol intitulé Facing reality? Law enforcement and the challenge of deepfakes, avril 2022 (en anglais); Kwon H., The Disinformation Business is Booming, Defence One, 15 novembre 2021 (en anglais); Christoph, Diehl, Hopoenstedt et al, So funktioniert das System der Lügenindustrie Der Spiegel, 14 février 2023 (en allemand). Voir également Forbidden Stories (en anglais), une collection de reportages sur l'industrie de la désinformation.

18 Voir Lamberty et Frühwirth, Ein Jahr russischer Angriffskrieg: Die Rolle von Desinformation in Deutschland document de recherche du CEMAS, février 2023 (en allemand); Brandt, Ichihara, Jalli et.al, Impact of Disinformation democracy in Asia, Brookings Institution, décembre 2022 (en anglais).

19 Voir Helmus, Todd C., Artificial Intelligence, Deepfakes, and Disinformation, RAND Corporation, juillet 2022 (en anglais); Sadeghi M. et Arvanitis L., Les "newsbots" montent au front : des sites d'actualité générés par l'IA se multiplient en ligne, Newsguard, 1er mai 2023.

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

LES CAS DE MANIPULATION DE L'INFORMATION ET D'INGÉRENCE RUSSES ET LA DÉSINFORMATION

1. Manipulation continuelle de l'information visant l'Ukraine

La Russie a continué de s'adonner à des activités de manipulation de l'information pour légitimer sa conquête territoriale de l'Ukraine. Les thèmes de la désinformation russe sont passés de la propagande d'avant-guerre (par exemple, « l'Occident » en tant qu'agresseur, la « nazification » de l'Ukraine) à la propagande de guerre (par exemple, la reddition des troupes ukrainiennes sur des théâtres de guerre cruciaux, les échecs militaires ou les « crimes de guerre » ukrainiens, les opérations de « nettoyage ethnique » dans le Donbass). Au fur et à mesure que le conflit se poursuivait, les principaux messages comportaient également de fausses allégations en ce qui concerne l'impact des sanctions occidentales sur la sécurité alimentaire et la crise énergétique. Certains messages alimentés par la désinformation russe (notamment sur les laboratoires présumés d'armes biologiques en Ukraine, sur les effets démoralisants des sanctions et sur la « russophobie » rampante) ont été amplifiés par des groupes conspirationnistes, anti-vaccination et anti-Union européenne à l'Ouest.

2. Usurpation de l'identité des médias de l'Union européenne et de l'Occident

Dans le contexte de la guerre d'agression de la Russie contre l'Ukraine, on assiste à la multiplication d'incidents d'usurpation de l'image et de marques de commerce des grands médias sur les plateformes de médias sociaux et la production de contenus d'information falsifiés et d'imitations de sites Web faisant la promotion des messages prorusses. Cette tendance a commencé à l'été 2022 et elle comprenait des imitations de *Der Spiegel* et *Deutsche Welle* (Allemagne), de la BBC (Royaume-Uni) et de CNN (États-Unis[21]. Des acteurs malveillants ont également acheté des noms de domaine Internet presque identiques à des sites Web de médias établis et authentiques, créant des « clones » d'au moins 17 fournisseurs de médias, et ciblant ainsi les utilisateurs avec de faux articles[22]. En outre, des acteurs proKremlin ont créé de fausses couvertures de magazines satiriques en Espagne, en Allemagne et en France, qui ont ensuite été promues par l'écosystème russe de manipulation de l'information et d'ingérence étrangères[23]. Cette confusion entre médias traditionnels authentiques et médias clonés a posé des problèmes au secteur des noms de domaine et a eu pour effet de brouiller encore davantage la confiance du public dans les sources médiatiques crédibles et reconnaissables.

3. Hausse de la désinformation fondée sur le genre et l'identité

Tout au long de la période visée par le rapport, la Russie a diffusé des mensonges à caractère sexuel sur les femmes ukrainiennes et la communauté LGBTQI+ afin d'attiser le sexisme et l'homophobie[24], tandis que des acteurs liés à l'État chinois ont harcelé des femmes journalistes[25]. La désinformation basée sur l'identité a pour effet de réduire les cibles au silence. De plus, cette forme de désinformation, en renforçant les hiérarchies de pouvoir institutionnel qui placent les femmes, la communauté LGBTQI+, les personnes de couleur et d'autres communautés vulnérables au bas de l'échelle, ne fait que polariser davantage les sociétés occidentales[26].

4. Vidéos professionnelles se moquant des citoyens de l'UE

L'écosystème russe de manipulation de l'information et d'ingérence étrangères a produit et diffusé des vidéos satiriques attaquant les valeurs occidentales et exposant les prétendues raisons de la supériorité

21 Weber J. et Baig R., Fake content targets international media, DW, août 2022 (en anglais).
22 Voir Alaphilippe A. et al, Doppelganger – Media clones serving Russian propaganda, EUDisinfoLab, septembre 2022 (en anglais). Voir le rapport de VIGINUM intitulé RRN: une campagne numérique de manipulation de l'information complexe et persistante, 13 juin 2023.
23 'Fake news inception': Debunking fake Charlie Hebdo covers, France 24 English, 12 décembre 2022 (en anglais).
24 Jankowicz, Hunchak, Pavliuc et al, Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, Wilson Center, janvier 2021 (en anglais); Bilousenko, Pivtorak, Iliuk, Slyvenko, Prostitution will save Ukraine from the default": Investigating Russian gender disinformation in social networks, Detector Media, septembre 2022 (en anglais).
25 Voir Zhang, A. et Cave, D., Smart Asian women are the new targets of CCP global online repression, ASPI, juin 2022 (en anglais); Allen-Ebrahimian, B., China-linked Twitter harassment targets female Asian journalists outside China, Axios, juin 2022 (en anglais).
26 Voir le procès-verbal de la 46e réunion du Comité OTAN sur la dimension de genre : menaces hybrides, désinformation et sécurité humaine, OTAN, octobre 2022; Strand et Svensson, Disinformation campaigns about LGBTI+ people in the EU and foreign influence, Parlement de l'Union européenne, juillet 2021 (en anglais); Bradshaw, S., Identity-based Propaganda: Discrimination, Division and Democracy, Stanford University, conférence en ligne, janvier 2022 (en anglais).

de la Russie sur les démocraties occidentales. L'équipe chargée des données au sein du Service européen pour l'action extérieure (SEAE) a détecté cette nouvelle tendance à l'aide des éléments suivants : une vidéo soulignant la « russophrénie » occidentale et les prétendues tentatives d'annulation de la culture russe; une publicité invitant les citoyens de l'UE à s'installer en Russie; six vidéos commerciales se moquant des citoyens de l'UE en ce qui concerne la crise énergétique; et une publicité dénigrant la position de l'UE en matière d'identité de genre[27]. Ces vidéos mettent en scène des acteurs professionnels qui ont déjà joué des rôles dans des émissions de télévision, des séries et des films russes, ce qui témoigne d'une « professionnalisation » croissante de cette industrie de la propagande.

5. Repositionnement des marques des médias soutenus par le Kremlin pour contourner les sanctions de l'UE

Après que l'UE a annoncé des sanctions contre les médias publics *Russia Today* (RT) et *Sputnik*, et que *Telegram* les a bannis de sa plateforme, les chaînes *Telegram* alignées sur le Kremlin ont réagi en changeant de marque et en apportant des modifications qui leur ont permis d'avoir « plusieurs longueurs d'avance » sur les organismes de réglementation[28]. Les propagandistes ont utilisé des tactiques telles que la création de comptes copiés et de comptes miroirs et les changements de nom, de couleur et de logo des chaînes. Ils se sont aussi appuyés sur des auditeurs fidèles pour partager du contenu dans des transmissions en direct et des instructions sur la manière d'accéder aux chaînes interdites à l'aide d'un RPV[29]. Les chaînes en question ont également commencé à publier des articles sur des plateformes de publication anonymes afin de conserver leur apparence de nouvelles, sans les noms des médias soutenus par le Kremlin dans leurs adresses URL. Elles se sont tournées vers les canaux diplomatiques officiels pour continuer à diffuser la désinformation, les comptes de médias sociaux de nombreux dirigeants des médias d'État et le réseau des comptes du ministère des Affaires étrangères et de l'ambassade de Russie n'ayant pas été affectés par les interdictions.

DÉVELOPPEMENTS AU NIVEAU MONDIAL

6. Garanties de sécurité et utilisation de l'histoire pour gagner en crédibilité et en influence

En 2022, des acteurs affiliés à l'État russe, tels que la société militaire privée groupe Wagner, ont poursuivi leurs tentatives pour gagner en influence dans le monde, notamment en Afrique, au MoyenOrient et en Amérique latine. Apparemment insensibles aux droits de la personne et aux pratiques commerciales responsables, les tactiques employées par ces agents consistaient à promettre des garanties de sécurité en échange de l'extraction de ressources naturelles ou de l'accès à des sites stratégiques, notamment des ports[30]. Leur présence dans plusieurs pays africains a également entraîné des ingérences dans l'environnement de l'information, comme cela a été démontré récemment au Mali, au Burkina Faso, à Madagascar et au Soudan[31]. Une autre tactique du groupe Wagner a consisté à exploiter l'histoire coloniale de certains pays européens en Afrique, comme la France, ou les perceptions négatives du rôle historique des États-Unis en Amérique latine, afin de rendre plus crédibles les actions de la Russie dans ces pays, ainsi qu'en Ukraine.

7. Réseaux amplificateurs de la République populaire de Chine et discours anti-occidentaux

Les autorités chinoises se sont appuyées sur des réseaux amplificateurs normalement impliqués dans la promotion de programmes gouvernementaux régionaux ou municipaux pour submerger de manière non organique (« envahir ») l'espace d'information afin de défendre des politiques jugées sensibles par le gouvernement du Parti communiste chinois (par exemple, le Xinjiang, Taïwan). Alors que ces réseaux de faux comptes semblent fonctionner de manière indépendante dans différentes régions, ils présentent en fait de nombreux indicateurs de leur coordination[32]. En outre, nous avons observé un alignement

27 Les liens suivants sont fournis seulement à titre de référence pour la recherche : culture russe (lien); déménagement en Russie (lien); crise énergétique (lien, lien, lien).
28 Voir Killeen, M.,Kremlin-backed media evading EU sanctions, report finds, Euractiv, mai 2022 (en anglais).
29 Voir Gerster L. et Arcostanzo F., How Russian State-Controlled Media and its Supporters are Circumventing Social Media Restrictions, ISD, mars 2022 (en anglais).
30 Fasanotti, F. S. Russia's Wagner Group in Africa: Influence, commercial concessions, rights violations, and counterinsurgency failure, Brookings Institution, février 2022 (en anglais).
31 Ehl, D., More than mercenaries: Russia's Wagner Group in Africa, DW, avril 2023; également, Fasanotti dans Fn. 31 (en anglais).
32 À titre de référence, voir Linvill D., et Warren, P., Understanding the Pro-China Propaganda and Disinformation Tool Set in Xinjiang, Lawfare, 1er décembre 2021 (en anglais).

significatif entre la Fédération de Russie et la RPC, avec des profils chinois et des réseaux de trolls qui s'attachent à diffuser de la propagande prorusse et des messages de désinformation en Asie du Sud-Est. Après le sommet de Samarkand entre Poutine et Xi, la désinformation diffusée par ces réseaux s'est alignée plus étroitement sur la propagande russe. Les comptes censés couvrir les événements en Ukraine comprennent des comptes rendus erronés de développements sur le terrain, y compris les « référendums » sur l'annexion.

8. Tentatives de l'Iran pour discréditer l'Occident

L'Iran n'a cessé de diffuser des messages de désinformation et de propagande visant vraisemblablement à discréditer l'Occident, en particulier les États-Unis et les adversaires de l'Iran au Moyen-Orient, notamment Israël. L'Iran a amplifié les récits de duplicité, d'hégémonie et d'interventionnisme de l'Occident dans le but probable de saper les politiques et les mesures occidentales. Il a également cherché à discréditer ou à contrer les révélations sur les autorités iraniennes faites par des organes de presse occidentaux et de la diaspora[33]. L'Iran a fait l'objet d'une censure internationale plus large à la suite de la répression violente des manifestations antigouvernementales qui, selon les autorités iraniennes, ont été orchestrées par les États-Unis et Israël. Les autorités iraniennes ont également cherché à nier que l'Iran avait livré de l'équipement militaire à la Russie, notamment des drones, destinés à être utilisés en Ukraine[34].

33 Al-Faour N., How Iran is manipulating the online narrative to cover up its violent crackdown on protests, Arab News, octobre 2022 (en anglais).

34 Martinez A., Iran denies that it is supplying weaponry to Russia for use in Ukraine (NPR, October 20, 2022)

ACTIVITÉS DU MRR DU G7 EN 2022

Tout au long de l'année 2022, en partenariat avec des démocraties d'optique commune, le MRR a intensifié ses activités d'échange d'information afin de renforcer les réponses collectives à la guerre d'agression russe contre l'Ukraine. Il a continué de fournir une plateforme pour discuter de l'évolution des approches nationales et internationales.

ÉCHANGE D'INFORMATION

Les agents de coordination du MRR du G7 se sont réunis tous les mois pour mettre en commun leurs mises à jour, analyses, pratiques exemplaires et leçons apprises. Les thèmes prioritaires comprenaient entre autres la situation d'urgence en Ukraine, les leçons tirées de la sécurisation des élections en 2021, les menaces étrangères contre les droits et les libertés de nos citoyens, y compris l'ingérence infranationale. Les agents de coordination ont fait appel à des experts du milieu universitaire et de la société civile pour étayer leurs évaluations de l'évolution des menaces (y compris pendant les élections), de l'environnement de l'information ukrainien et de la désinformation liée à la pandémie de COVID 19. De plus, des réunions de travail ont eu lieu chaque mois pour favoriser la coordination entre les équipes de soutien sur des questions politiques en constante évolution, telles que la manipulation de l'information et l'ingérence étrangères, ainsi que les menaces hybrides.

RENFORCEMENT DES CAPACITÉS D'ANALYSE

Les analystes du MRR du G7 se sont réunis régulièrement pour échanger en temps réel des idées et des analyses sur plusieurs sujets, notamment la manipulation de l'information et l'ingérence étrangères, la désinformation concernant la guerre contre l'Ukraine et la manipulation russe de l'information relative à l'approvisionnement en denrées alimentaires et en énergie. Les analystes ont également systématiquement participé à des analyses conjointes de l'environnement en ligne et à des échanges d'information facilités par un groupe de travail analytique américain créé en 2021. Le groupe de travail a poursuivi l'élaboration d'une typologie pour évaluer le niveau d'affiliation entre les acteurs étatiques et les médias. En outre, un certain nombre d'échanges entre les équipes d'analyse du MRR du G7 et des activités de renforcement des capacités ont eu lieu tout au long de l'année 2022 afin de faciliter le transfert de connaissances et de compétences et de favoriser l'élaboration d'un cadre commun pour l'analyse des menaces favorisant une réponse collective.

RENFORCEMENT DES CONNAISSANCES

Le MRR du G7 a permis et soutenu un groupe de travail dirigé par les États-Unis afin de créer un « programme international de recherche sur la contre-désinformation » pour les universités et les groupes de réflexion. Le groupe de travail était composé de représentants de dix nations et organisations gouvernementales partenaires, ainsi que de neuf agences gouvernementales américaines. Le programme a été élaboré à partir d'enquêtes et de consultations, et le rapport final a été transmis à de nombreux chercheurs universitaires et groupes de réflexion afin de permettre des recherches sur les principales lacunes en matière de connaissances et sur les sujets prioritaires pour soutenir l'élaboration de politiques fondées sur des données probantes.

RENFORCEMENT DE LA CAPACITÉ DE RÉPONSE COLLECTIVE

Avec le début de la guerre d'agression russe contre l'Ukraine en février 2022, le MRR du G7 a intensifié ses travaux. En plus de soutenir l'analyse de l'environnement de l'information ukrainien, la surveillance des espaces en ligne pour la désinformation russe, l'échange d'information et l'élaboration de réponses stratégiques en matière de communication, le MRR du G7 s'est associé à la Fondation Carnegie pour la paix internationale afin de lancer un projet pilote visant à coordonner une réponse multipartite en Ukraine et dans ses environs. Parrainé par le Canada, un partenariat composé de représentants des gouvernements du MMR du G7, des organismes du secteur économique et de la société civile a été créé en juillet pour faciliter la coordination avec les autorités ukrainiennes dans le but de préserver l'intégrité

de l'environnement de l'information en Ukraine. Les enseignements tirés de cet exercice (qui devrait se poursuivre en 2023) peuvent être utilisés pour orienter la façon dont les pays et les organismes répondent aux futures crises de l'environnement de l'information afin de protéger les citoyens et l'intégrité de l'information, et afin de contrer la manipulation de l'information et l'ingérence étrangères. Lors de leur réunion à Berlin, en octobre 2022, les agents de coordination du MRR du G7 ont confirmé la nécessité de renforcer les capacités de réponse collective en élaborant un cadre de réponse clair et des principes opérationnels. Ces travaux débuteront en 2023.

PLEINS FEUX SUR LES PAYS ET LES ORGANISMES

Canada

Lutter contre la désinformation russe sur l'Ukraine et soutenir la recherche canadienne

La lutte contre la désinformation russe au sujet de l'Ukraine a été une préoccupation majeure du gouvernement du Canada en 2022. Afin de contrer la fausse information et les théories du complot russes en ce qui concerne l'invasion illégale, le gouvernement du Canada a adopté une position publique ferme, publiant, depuis Affaires mondiales Canada, le ministère de la Défense nationale et le Centre de la sécurité des télécommunications, des dizaines de réfutations des publications mensongères de la Russie[35]. Ces réfutations, publiés sur des plateformes de médias sociaux populaires en plusieurs langues, démontaient directement les déclarations mensongères. Le Canada a également sanctionné plus de 100 entités et citoyens russes complices de la désinformation et de la propagande russes[36], et a diffusé des conseils sur la manière d'identifier la désinformation, la mésinformation et la malinformation en ligne[37]. En août 2022, le premier ministre a également annoncé l'établissement d'une unité dédiée au sein du MRR Canada au ministère des Affaires mondiales afin de surveiller, de détecter et de contrer la désinformation russe et toute autre désinformation parrainée par des États[38].

Au niveau national, le gouvernement du Canada a engagé plus de 5 500 000 dollars pour collaborer avec la société civile et le milieu universitaire afin de renforcer la capacité des partenaires non gouvernementaux à lutter contre la désinformation. Le *Réseau canadien de recherche sur les médias numériques*, qui relève de l'*Observatoire de l'écosystème médiatique* de l'Université McGill et de l'Université de Toronto, est la plus importante de ces initiatives. Il produira et soutiendra la production de recherches sur la dynamique de l'écosystème de l'information au Canada et sur la manière dont cette information affecte les attitudes et les comportements des Canadiens. Il éduquera également les Canadiens sur la qualité de l'information dans l'écosystème de l'information, y compris la désinformation, et élaborera et soutiendra des stratégies plus larges pour armer les Canadiens contre la désinformation et accroître leur littératie numérique.

France

Renforcer les capacités du gouvernement à détecter la manipulation de l'information et l'ingérence étrangères et à coordonner les contre-mesures

En 2021, la France a mis en place VIGINUM afin de renforcer son dispositif national de lutte contre la manipulation de l'information. VIGINUM surveille et détecte les ingérences numériques étrangères et vise à contrer les campagnes étrangères de manipulation de l'information qui cherchent à nuire à la France et à ses intérêts fondamentaux. VIGINUM opère dans un cadre juridique et éthique rigoureux et son activité est examinée par un comité éthique et scientifique composé d'experts juridiques, diplomatiques, scientifiques et médiatiques. En 2022, au cours de sa première année complète de fonctionnement, VIGINUM a concentré l'essentiel de son activité sur la protection des élections présidentielles (avril) et législatives (juin). VIGINUM a également mené des opérations visant à protéger le débat public en ligne sur divers événements nationaux ou internationaux susceptibles d'être exploités par des acteurs étrangers malveillants.

Sur la base de ces efforts, un nouveau service d'analyse et de stratégie (Veille et Stratégie) a été créé au sein du ministère des Affaires étrangères, en juillet 2022, pour coordonner la lutte contre les campagnes de manipulation de l'information et d'ingérence étrangères, y compris les communications stratégiques, la surveillance de l'espace médiatique international (journaux, radio, télévision, médias sociaux) et les collaborations avec des partenaires internationaux d'optique commune. Afin de favoriser l'intégrité de l'information au niveau mondial, ce ministère travaille en étroite coordination avec ses missions diplomatiques, ainsi qu'avec d'autres unités au sein du ministère, pour soutenir la liberté de la presse, la protection du journalisme à l'étranger et la régulation des plateformes (par exemple, la modération du contenu et la transparence algorithmique).

35 Affaires mondiales Canada, Contrer la désinformation par des faits – L'invasion russe de l'Ukraine.
36 Affaires mondiales Canada, Sanctions – Invasion russe de l'Ukraine.
37 Centre canadien pour la cybersécurité, Repérer les cas de mésinformation, désinformation et malinformation.
38 Premier ministre du Canada, Le premier ministre annonce du soutien supplémentaire à l'Ukraine.

Allemagne

Améliorer la coordination intergouvernementale et les communications publiques pour contrer les menaces hybrides

La pandémie actuelle et la guerre d'agression russe contre l'Ukraine ont montré que les menaces hybrides, dont la désinformation, constituent l'un des principaux défis sécuritaires et sociopolitiques auxquels l'Allemagne est confrontée. À la suite de l'invasion de l'Ukraine par la Russie, l'Allemagne a mis en place un groupe de travail interministériel dirigé par le ministère fédéral de l'Intérieur et de la Communauté afin de favoriser des réponses coordonnées à apporter aux menaces hybrides, en particulier à la désinformation. Ce groupe de travail coordonne toutes les activités visant à lutter contre la diffusion délibérée de renseignements faux et trompeurs dans le contexte de la guerre contre l'Ukraine, notamment en renforçant la communication proactive et transparente et en équipant la société face aux menaces dans l'espace de l'information.

En outre, un groupe de travail interministériel sur les menaces hybrides a été mis en place sous l'égide du ministère fédéral de l'Intérieur et de la Communauté dans le but de renforcer la coopération entre tous les niveaux de gouvernement. Ce groupe de travail, qui réunit des représentants des ministères nationaux, des États fédéraux, des autorités de sécurité, des organismes municipaux et des services de renseignement, se concentre sur des aspects spécifiques des menaces hybrides au niveau infranational.

En outre, le ministère fédéral des Affaires étrangères allemand a renforcé la communication proactive de l'Allemagne dans le monde, au moyen de son réseau de plus de 220 missions et centres de contenu régionaux à l'étranger. Par le partage de son analyse des médias sociaux, le ministère assure un échange étroit sur la désinformation avec ses partenaires internationaux et dans le cadre des tribunes multilatérales. En outre, le ministère continue à promouvoir la résilience de la société face à la désinformation dans les pays partenaires, en mettant l'accent sur les pays baltes et les Balkans occidentaux.

Italie

Renforcer la résilience nationale et contrer la désinformation russe

Depuis l'invasion de l'Ukraine par la Russie, l'Italie a vu une augmentation des messages de désinformation russes, principalement diffusés par des profils officiels affiliés à l'État, des affiliés proKremlin et des influenceurs dans l'écosystème italien de l'information. À la suite de l'imposition de sanctions, l'Italie a fermé deux médias parrainés par l'État russe (*Sputnik* et *RT*), qui amplifiaient la désinformation du Kremlin. L'Italie a également été témoin d'un alignement significatif entre la Russie et la République populaire de Chine dans l'environnement de l'information, avec des profils et des trolls chinois diffusant de la propagande prorusse et des messages de désinformation en Asie du Sud-Est.

Pour lutter contre la désinformation, l'Italie a adopté une série de mesures, notamment : la sensibilisation et la résilience du public au moyen de campagnes médiatiques (*RAI news*); la mise en œuvre d'une *Stratégie nationale de cybersécurité 2022-2024*; la contribution à l'élaboration et à la mise en œuvre de la Loi de l'UE sur les services numériques; la réalisation d'une analyse d'évaluation des risques pour protéger les campagnes électorales; la création d'une unité de surveillance au sein du ministère des Affaires étrangères pour lutter contre la propagation de la désinformation; la création d'un groupe de travail interministériel sur la lutte contre les menaces hybrides; et l'utilisation de communications stratégiques pour repousser la désinformation de la Russie sur des questions spécifiques.

Japon

Adopter une nouvelle Stratégie de sécurité nationale pour faire face aux menaces étrangères, y compris la désinformation

En décembre 2022, le Japon a publié une nouvelle Stratégie de sécurité nationale, qui décrit les approches visant à renforcer les réponses du Japon en ce qui concerne la guerre de l'information. La stratégie prévoit la création d'une nouvelle structure gouvernementale chargée de rassembler et d'analyser les données relatives aux menaces provenant de l'étranger, y compris la désinformation. La nouvelle structure vise à renforcer la communication externe, à améliorer la coopération avec les organismes non gouvernementaux et à utiliser activement une communication stratégique gouvernementale coordonnée pour contrer ces menaces.

Royaume-Uni

Créer un Groupe de travail chargé de défendre la démocratie

En novembre 2022, le Royaume-Uni a annoncé la création d'un nouveau Groupe de travail pangouvernemental chargé de défendre la démocratie. Sa mission est de réduire les risques pour les processus démocratiques, les institutions et la société britannique et de veiller à ce qu'ils soient sûrs et résilients face aux menaces d'ingérence étrangère. Le groupe de travail réunit les services gouvernementaux concernés, les forces de l'ordre et les agences de renseignement, et travaille en étroite collaboration avec le Parlement. Il collaborera également avec des partenaires extérieurs au gouvernement central et au Parlement, notamment des partenaires internationaux, des administrations décentralisées du Royaume-Uni, des collectivités locales et des organismes privés et non gouvernementaux.

États-Unis

Lutter contre la propagande étrangère et la désinformation

Le *Global Engagement Center* (GEC) collabore avec divers partenaires pour renforcer de manière globale la résilience mondiale face à la propagande étrangère et la désinformation. En utilisant une approche pansociale, le GEC renforce la capacité des partenaires à déceler et contrer l'influence malveillante, soutient la recherche sur les activités et les méthodes de propagande et de désinformation des acteurs étrangers et leur dénonciation et veille à ce que les publics vulnérables aient accès à des données de qualité, indépendantes et factuelles. Depuis 2019, le GEC a renforcé la capacité des personnes, de la société civile, des universités, des médias et des organismes partenaires dans plus de 70 pays afin d'accroître la résistance mondiale face à la propagande et à la désinformation. Le GEC s'appuie sur les pouvoirs d'octroi de subventions de son unité et sur divers mécanismes de financement pour faciliter la mise en place de programmes locaux destinés à soutenir ces initiatives. On peut consulter ses rapports destinés au public sur le site state.gov/disarming-disinformation.

Union européenne

Concevoir des boîtes à outils pour la lutte contre les menaces hybrides et la manipulation de l'information et l'ingérence étrangères, et pour la protection de l'intégrité de l'enseignement et de la recherche

En décembre 2022, l'UE a adopté un cadre pour une réponse coordonnée aux campagnes hybrides (la Boîte à outils hybride de l'UE), permettant ainsi une action plus éclairée et plus ciblée contre l'influence hybride, basée sur une connaissance globale de la situation et s'appuyant sur un large éventail de mesures internes et externes. En réponse aux menaces d'ingérence étrangère visant les établissements d'enseignement supérieur et les organismes de recherche, la Commission européenne a publié en janvier 2022 une boîte à outils (en anglais) sur la manière d'atténuer l'ingérence étrangère dans la recherche et l'innovation, tout en sauvegardant des valeurs fondamentales comme la liberté académique, l'intégrité et l'autonomie institutionnelle.

Le Service européen pour l'action extérieure (SEAE) a continué à faire avancer ses travaux sur la manipulation de l'information et l'ingérence étrangères, en renforçant le cadre de l'UE pour répondre à de telles situations grâce à une définition, une méthodologie analytique et une boîte à outils communes. Les citoyens européens s'intéressent de près à la manipulation de l'information et à l'ingérence étrangères, comme en témoigne le nombre de personnes qui ont consulté le site Web d'*EUvsDisinfo* (plus de 2,5 millions) et le nombre de celles qui ont été jointes par les canaux de médias sociaux d'*EUvsDisinfo* (quelque 20 millions de personnes). Alors que la Russie continue de recourir à la manipulation de l'information et à l'ingérence étrangères dans sa guerre contre l'Ukraine, ainsi qu'à des tribunes multilatérales (dont les Nations Unies et le Conseil de sécurité des Nations Unies), le SEAE a jeté les bases, en 2022, d'une coopération accrue avec les Nations Unies. La Commission européenne travaille de concert avec le SEAE sur les communications stratégiques, le suivi et la connaissance de l'environnement médiatique afin de relever les défis nationaux et étrangers.

OBSERVATEURS

Australie

Créer de nouveaux groupes de travail pour renforcer la résilience nationale et la démocratie

Le 8 décembre 2022, le gouvernement australien a annoncé la création de deux groupes de travail au sein du ministère de l'Intérieur afin de renforcer la résilience de l'Australie face aux défis durables et émergents en matière de sécurité nationale, soit : le *National Resilience Taskforce* (NRT) et le *Strengthening Democracy Taskforce* (SDT). Le NRT s'efforce de renforcer la résilience nationale de l'Australie en examinant l'exposition et la vulnérabilité croissante du pays face aux crises d'importance nationale et en veillant à ce que le gouvernement australien dispose des politiques, de la législation et des capacités nécessaires pour gérer des crises nationales de plus en plus complexes et simultanées, y compris celles exacerbées par les changements climatiques.

Le SDT recherche des initiatives pratiques pour protéger et soutenir la résilience de la démocratie australienne, à court et à long terme. Le groupe de travail s'appuie sur de nombreuses données, preuves, recherches et pratiques émergentes pour identifier les flux de renforcement (démocratisation) et d'affaiblissement (antidémocratisation) les plus significatifs qui peuvent être respectivement renforcés et perturbés afin d'avoir le plus grand potentiel d'impact. Le groupe de travail s'appuiera sur le large éventail de mesures déjà en place ou en cours d'élaboration pour soutenir une démocratie forte et résiliente.

Ces groupes de travail constituent des outils complémentaires qui renforcent positivement la prospérité, la sécurité et la souveraineté de l'Australie.

Nouvelle-Zélande

Soutenir l'enseignement supérieur – « Recherche digne de confiance – Exigences en matière de protection de la sécurité »

En septembre 2022, l'organisme national représentant le secteur universitaire *Aotearoa Nouvelle-Zélande* a publié un guide sur la manière dont les hauts responsables doivent envisager la réponse de leurs universités à un environnement géopolitique en constante évolution et de plus en plus complexe. Cela signifie que les universités doivent examiner la manière dont elles gèrent les risques liés aux activités de recherche, en particulier celles qui impliquent des partenariats internationaux, dans les domaines de la recherche appliquée, de la recherche sur les technologies émergentes à double usage ou culturellement sensibles ou une application qui pourrait être préjudiciable ou nuire à leur réputation. L'approche recommandée en matière de politiques, de planification et d'évaluation des risques est axée sur la gestion des risques et la protection des personnes, des biens et de la réputation, tout en maintenant un engagement fort en faveur du respect de la liberté académique et de la promotion des avantages généraux de la collaboration internationale.

Organisation du traité de l'Atlantique Nord (OTAN)

Lutter contre les activités d'information hostiles, y compris la désinformation

L'Organisation du traité de l'Atlantique Nord (OTAN) a déployé des efforts sans précédent pour réfuter de façon proactive les messages de la Russie sur l'invasion de l'Ukraine, afin de rendre son public plus résistant à la désinformation, de renforcer l'unité de l'alliance et de maintenir le soutien à l'Ukraine.

Depuis l'automne 2021, l'OTAN a délibérément déclassifié des quantités importantes de renseignements sur le renforcement militaire de la Russie et sur ses projets d'invasion totale de l'Ukraine, y compris d'éventuelles opérations sous fausse bannière. Cette mesure a été menée en coordination avec les Alliés, afin de dénoncer et de dissuader les actions de la Russie, et d'accroître la compréhension, la résilience et le soutien de nos publics. Cela s'est fait systématiquement au moyen des communications publiques du secrétaire général de l'OTAN et de ses hauts fonctionnaires, ainsi que par une série de réunions d'information. En 2022, l'OTAN a maintenu cette approche qui a favorisé l'unité des opinions publiques alliées sur les activités russes, facilité le maintien du soutien à l'Ukraine et démenti de façon proactive la désinformation russe plutôt que de la démentir une fois qu'elle a pris de l'ampleur. En outre, l'OTAN a constamment traqué les messages hostiles, en réfutant, de façon proactive ou réactive, les principaux mensonges russes sur l'OTAN au moyen de communications proactives et de sa plateforme *Mise au point*, créée en 2014, après l'annexion illégale de la Crimée par la Russie.

Suède

Créer l'Agence de défense psychologique : première année d'activité

Créée en janvier 2022, l'Agence suédoise de défense psychologique est chargée de déceler, d'analyser, de prévenir et de combattre les informations malveillantes et les ingérences étrangères visant la Suède ou les intérêts suédois. L'agence possède à la fois un rôle opérationnel et le mandat de renforcer la résilience de la société face aux ingérences étrangères.

En raison de l'augmentation des campagnes de désinformation russes suite à l'invasion de l'Ukraine et à la décision de la Suède de demander l'adhésion à l'OTAN, l'agence a lancé une campagne d'information nationale à l'approche de l'élection générale, pour sensibiliser les citoyens à la désinformation et leur conseiller de rester vigilants. Tout au long de l'année 2022, la Suède a été victime d'une vaste campagne d'information coordonnée prétendant que les enfants et les familles musulmanes étaient systématiquement victimes d'abus de la part des autorités suédoises. La campagne est toujours en cours et se propage dans le monde entier, bien qu'à présent à un niveau réduit. Le gouvernement a mis en place plusieurs contre-mesures, notamment des activités de communication stratégique multipartites.

Pays-Bas

Promouvoir une approche « pangouvernementale » pour la lutte contre les menaces hybrides

Les Pays-Bas ont continué à travailler sur une structure interministérielle pour faciliter une approche pangouvernementale afin de lutter contre les menaces hybrides, notamment en élaborant un module de formation pour les fonctionnaires afin d'améliorer leurs connaissances et leur compréhension de ce type de menace. De plus, les services de renseignement néerlandais et le coordonnateur national de la lutte contre le terrorisme et de la sécurité (en anglais) ont publié la deuxième évaluation globale de la menace nationale en novembre 2022. L'évaluation a accordé une attention particulière à la façon dont la stabilité sociale et politique des Pays-Bas était affectée par l'ingérence étrangère, ainsi qu'aux menaces accrues pesant sur la sécurité économique. Le Parlement a été informé de ces deux processus dans une lettre sur les « menaces envers l'État », signée par neuf ministres, qui met en évidence les grands principes, les approches et les domaines d'intervention pour lutter contre les menaces hybrides, y compris la coopération avec les partenaires internationaux. Dans une lettre distincte adressée au Parlement sur la lutte contre la désinformation, une attention particulière a été accordée à la lutte contre la manipulation de l'information et l'ingérence étrangères.