GOUVERNEMENT

Liberté
Égalité
Fraternité

DÉSINFORMATION RUSSE : MIEUX CONNAÎTRE LE PHÉNOMÈNE POUR Y FAIRE FACE

Dossier de presse

Introduction

Aujourd'hui, dans les conflits internationaux, la désinformation s'est imposée comme une arme de guerre. Ce sont des mensonges dissimulés dans notre flot quotidien d'informations, qui visent à manipuler les faits.

La désinformation est utilisée pour semer le doute et créer des tensions au sein de nos sociétés. C'est notamment ce que la Russie, dissimulée derrière le dispositif RRN, a fait en novembre dernier en organisant la diffusion et l'amplification artificielle d'images d'étoiles de David taguées sur des murs de la région parisienne. Les commanditaires de ces campagnes attisent les haines, cherchent à nous monter les uns contre les autres, ici, chez nous.

La Russie n'est pas le seul acteur de la désinformation, mais elle utilise des moyens financiers et des méthodes qui la distinguent. Depuis le 24 février 2022, les attaques informationnelles russes se sont non seulement intensifiées, mais elles ont aussi changé de nature. La guerre d'agression menée contre l'Ukraine se prolonge dans une guerre informationnelle en Ukraine et dans tous les États qui soutiennent les Ukrainiens.

À l'aune des menaces que font peser les acteurs russes de la désinformation sur les élections européennes de juin prochain, il est de la responsabilité des gouvernements européens d'anticiper, de veiller, de caractériser, de dénoncer les manœuvres et les manipulations de l'information.

Face à ces manipulations de l'information, nous avons organisé notre réponse, tant au niveau national que dans une dynamique partenariale à l'international.

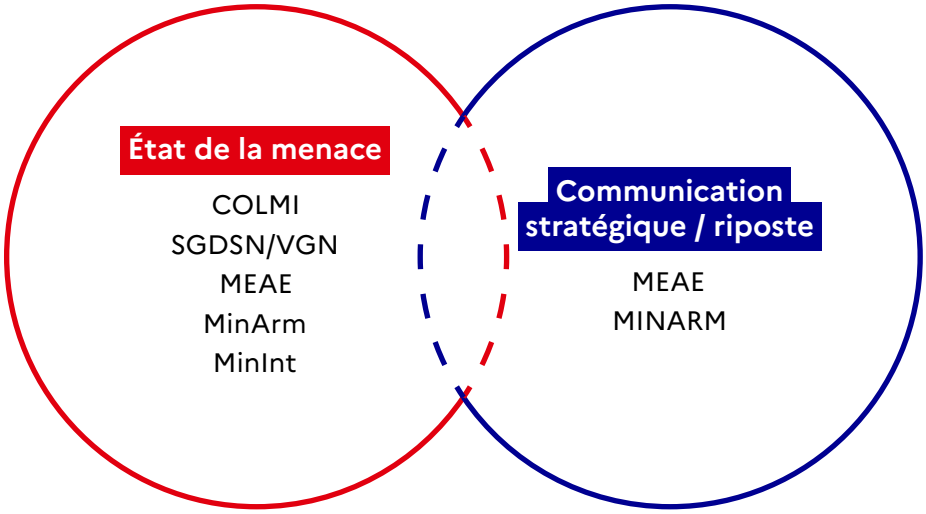
La France s'est armée pour faire face

La réponse française aux ingérences numériques étrangères, et notamment russes, implique un ensemble d'acteurs étatiques qui coordonnent étroitement leurs efforts.

La particularité de la France est de s'être dotée à la fois d'une agence spécialisée dans l'investigation en ligne (VIGINUM) et d'une équipe dédiée à la réponse en matière de crise informationnelle (MEAE/EMA), ce qui lui permet de couvrir un champ très large.

La force de notre réponse réside également dans la fidélité à nos valeurs et à nos principes démocratiques.

Coopération internationale



La France a construit une dynamique forte avec ses partenaires européens

Nous renforçons notre lutte contre les ingérences numériques étrangères et les manipulations de l'information, en particulier au sein de l'Union européenne.

Au sein de l'Union européenne, la question de la lutte contre les ingérences étrangères et contre les manipulations de l'information (Foreign Information Manipulation and Interference ou FIMI) est traitée au niveau politique par le Conseil des Affaires étrangères. Les décisions prises dans ce cadre se traduisent en actions concrètes menées par la « stratcom » du SEAE qui a développé depuis deux ans une boîte à outils pour lutter contre les menaces hybrides.

Le SEAE, pionnier dans la définition des FIMI, a mis en place un rapid alert system qui permet aux États membres de signaler des incidents et de partager des enquêtes sur des ingérences numériques étrangères. Le SEAE a aussi développé un site internet EUvsDisinfo qui décrypte les manœuvres russes.

Ces réponses doivent être accompagnées de progrès en matière de modération des contenus sur les plateformes de réseaux sociaux. Les acteurs du numérique ont une responsabilité dans la sélection des contenus qu'opèrent leurs algorithmes. La France et ses partenaires européens se mobilisent auprès du secteur privé afin de lutter contre la désinformation.

La mise en œuvre du Digital Service Act de l'Union européenne depuis le 25 août dernier constitue une avancée majeure pour que les entreprises concernées renforcent leurs standards en la matière. Mais nous devons aller plus loin pour conduire ces entreprises à modérer et à le faire dans un plus grand nombre de langues.

Digital Service Act : la législation sur les services numériques réglemente les intermédiaires et plateformes en ligne tels que les places de marché, les réseaux sociaux, les plateformes de partage de contenus, les boutiques d'applications et les plateformes de voyage et d'hébergement en ligne. Son principal objectif est de prévenir les activités illégales et préjudiciables en ligne et la propagation de la désinformation. Elle garantit la sécurité des utilisateurs, protège les droits fondamentaux et crée un environnement équitable et ouvert pour les plateformes en ligne.

(Source : Commission européenne : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en *)*

Comprendre la désinformation russe pour mieux y répondre

Les ingérences numériques en provenance de Russie ne sont pas une nouveauté. Les incidents se sont multipliés en Europe et aux États-Unis depuis 2014 et l'annexion illégale de la Crimée.

Cette stratégie hybride a atteint une intensité inédite après le 24 février 2022 et le lancement par la Russie de sa guerre d'agression contre l'Ukraine : en juin 2023, les autorités françaises ont ainsi mis en évidence l'existence d'une campagne numérique de manipulation de l'information contre la France impliquant des acteurs russes (voir ci-dessous). Depuis, la France a condamné plusieurs opérations d'ingérence numériques russes, et l'Union européenne a imposé des sanctions contre plusieurs personnes et entités russes liées à des campagnes de manipulation de l'information.

Les manœuvres de manipulation de l'information et de désinformation conduites par des acteurs russes servent actuellement des objectifs stratégiques bien identifiés : légitimer la guerre d'agression russe contre l'Ukraine, saper la cohésion des soutiens de l'Ukraine, déstabiliser les sociétés des démocraties libérales.

Ces actions ciblent prioritairement l'Ukraine, mais également les opinions publiques occidentales, ainsi que les classes dirigeantes et les opinions publiques de pays tiers, notamment en Afrique subsaharienne. La Russie a par ailleurs renforcé récemment ses actions de désinformation dans d'autres régions, comme l'Amérique latine.

Les modes opératoires classiques utilisés par les Russes

Création de médias, de fondations et de think tanks contrôlés par des acteurs russes. Par exemple, la Fondation pour la lutte contre l'injustice (Foundation to Battle Injustice) est directement pilotée par les structures d'influence du Projet Lakhta d'Evgueni Prigogine.

Utilisation de centaines de milliers de comptes de réseaux sociaux inauthentiques : il s'agit de comptes sur les réseaux sociaux, appartenant à de pseudo-utilisateurs, qui publient et partagent des contenus antioccidentaux et pro-russes. Ces comptes sont pour certains gérés depuis des fermes à trolls, d'autres sont animés de manière automatisée (on parle alors de *bots*).

Placement clandestin de publications : il s'agit d'une pratique utilisée par les structures russes de désinformation, étatiques et privées, qui consiste à faire publier par des médias légitimes et contre paiement, des articles « prêts à l'emploi » favorables aux intérêts russes. Ce mode opératoire qui s'apparente à de la corruption, permet à la Russie de contourner :

→ les règles adoptées par les organismes spécialisés dans la vérification des faits (*fact-checking*) ;

→ les mécanismes de détection des plateformes de réseaux sociaux qui ont pour objectif la lutte contre la manipulation de l'information ;

→ les sanctions mises en place par la France et l'Union européenne contre des organes russes de propagande reconnus tels que RT ou Sputnik.

Ainsi, le Projet Lakhta fait publier plusieurs milliers d'articles par an, en différentes langues, dans une soixantaine de médias y compris occidentaux. Outre,

l'effet d'influence recherché sur les populations locales (exemples : soutien à un politicien pro-russe, critique des actions occidentales), ces publications créent également de manière artificielle l'impression que les opinions publiques de différents pays sont favorables à la Russie.

Les mercenaires de l'influence russe s'appuient également sur des relais locaux. Ces personnes, qui sont parfois rémunérées, peuvent être idéologiquement convaincues et avoir conscience de leurs actes. Toutefois, dans d'autres cas, ces mercenaires parviennent à leurs fins en trompant leurs interlocuteurs qui sont alors inconscients d'être victimes de la machine de propagande russe.

Plus précisément, on observe différents modes opératoires russes en matière de manipulation de l'information (MI) depuis le début de la guerre d'agression russe en Ukraine.

Depuis quelques mois, si la qualité des narratifs propagés a baissé, **la coordination des différents vecteurs de diffusion des MI russes s'est renforcée**. Les manœuvres russes s'appuient sur des vecteurs très variés : clonage de sources officielles (fausses pages Facebook de grands médias internationaux publiant de véritables articles), chaînes Telegram, réseaux conspirationnistes, mais également canaux officiels et actions dans le monde physique (exemple de Dmitri Rogozine envoyant à notre ambassadeur à Moscou, Pierre Lévy un éclat d'obus tiré par un canon Caesar, qu'il aurait reçu dans la colonne vertébrale).

Les actions « multicouches » se généralisent : de premiers articles formulent des allégations fausses sur la base de preuves douteuses, une deuxième vague d'articles commente les premiers, et ainsi de suite, jusqu'à l'intégration de ces informations fabriquées dans les prises de position officielles russes, jusqu'au plus haut niveau de l'État russe. **L'objectif est d'inonder l'espace informationnel** pour créer la confusion.

Existant depuis 2014, le « faux *fact-checking* » prend aujourd'hui une nouvelle ampleur. Il s'agit de « débunker » des allégations fictives créées pour l'occasion.

Dans l'incapacité de proposer un contre-récit crédible (exemple du massacre de Boutcha), la Russie multiplie les récits alternatifs pour détourner l'attention.

Le *timing* des opérations informationnelles est essentiel pour juger de l'effet obtenu. Des récits sont propagés à des moments-clefs du débat politique dans les pays visés. Les temps électoraux sont particulièrement exposés.

Depuis février 2022, les manœuvres russes se sont multipliées dans l'espace informationnel français.

Elles ne sont pas toutes de même nature. Mais toutes ces manœuvres relèvent d'une stratégie claire : repérer des failles dans le débat public et s'y engouffrer. Trois exemples récents donnent la mesure de la diversité des modes d'action.

RRN (*RECENT RELIABLE NEWS*)

Cette campagne de manipulation de l'information a pour objectif de discréditer le soutien occidental à l'Ukraine. Dénommée RRN en raison de la place centrale occupée par le prétendu média *Reliable Recent News*, cette campagne s'articule autour de quatre composantes :

— la diffusion de contenus pro-russes liés à la guerre en Ukraine, dénigrant notamment ses dirigeants ;

— l'usurpation de l'identité de sites de médias, mais aussi gouvernementaux, européens, *via* la technique de typosquatting visant à reproduire leur nom de domaine ;

— la création de sites Web d'actualités francophones partageant des contenus polémiques, instrumentalisant l'actualité nationale française ;

— la mise en œuvre de moyens inauthentiques combinés, tels que des faux sites ou des faux comptes sur les réseaux sociaux, permettant de relayer les contenus.

Pour ce faire, la campagne RRN s'appuie sur un ensemble de narratifs inauthentiques, reprenant quatre thèmes principaux. Ils visent à créer de la division et à susciter artificiellement la défiance entre la société civile et ses gouvernants :

— l'inefficacité supposée des sanctions visant la Russie, qui pèseraient avant tout sur les États européens et/ou leurs citoyens ;

— la prétendue russophobie des États occidentaux ;

— la barbarie dont feraient preuve les forces armées ukrainiennes, ainsi que l'idéologie néonazie qui prédominerait chez les dirigeants ukrainiens ;

— les effets négatifs qu'entraînerait l'accueil de réfugiés ukrainiens pour les États européens.

Alors que 355 noms de domaine usurpant l'identité de médias ont été détectés par VIGINUM, quatre ciblent plus spécifiquement le public francophone et reprennent l'identité graphique de quotidiens français, à savoir *20 Minutes*, *Le Monde*, *Le Parisien* et *Le Figaro*. Ce sont au moins 58 articles qui ont été publiés via ces canaux.

VIGINUM, dans le cadre de son investigation en sources ouvertes, a par ailleurs pu identifier l'implication d'individus russes ou russophones ainsi que de plusieurs sociétés russes.

À partir de la fin du mois de mai 2023, la campagne RRN a connu un développement inédit, puisque c'est l'identité du site web du ministère de l'Europe et des Affaires étrangères qui a été usurpé.

LES ÉTOILES DE DAVID

La France a condamné l'implication du même réseau *Recent Reliable News* (RRN/ Doppelgänger) dans l'amplification artificielle et la primo-diffusion sur les réseaux sociaux de photos de tags représentant des étoiles de David dans le 10e arrondissement de Paris quelques jours après les massacres du 7 octobre perpétrés par le Hamas.

S'agissant des faits eux-mêmes, l'enquête judiciaire en cours devra établir la possible responsabilité d'un commanditaire étranger.

En ce qui concerne leur amplification, VIGINUM, service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères, a détecté le 6 novembre 2023 l'implication d'un réseau de 1 095 « *bots* » sur la plateforme X (anciennement Twitter) : ces « bots » ont publié 2 589 posts qui ont amplifié la polémique liée aux étoiles de David. VIGINUM considère, avec un haut degré de confiance, que ces « *bots* » sont affiliés au dispositif RRN dans la mesure où une de leurs activités principales consiste à réorienter vers des sites internet du dispositif RRN.

En ce qui concerne la primo-diffusion des photos, alors que la première publication authentique des photos des tags semble être intervenue le 30 octobre à 19 h 37 sur X, VIGINUM a daté les premières publications du réseau de « bots » RRN du 28 octobre, à partir de 19 h 24, soit près de 48 h avant.

Cette nouvelle opération d'ingérence numérique russe contre la France témoigne de la persistance d'une stratégie opportuniste et irresponsable visant à exploiter les crises internationales pour semer la confusion et à créer des tensions dans le débat public en France et en Europe.

PORTAL KOMBAT

Entre septembre et décembre 2023, VIGINUM a analysé l'activité d'un réseau de prétendus sites d'information numériques qui diffusent des contenus pro-russes à des publics internationaux.

Initialement, ce réseau, composé d'au moins 193 sites, couvrait les nouvelles de localités russes et ukrainiennes. Il s'est développé depuis l'invasion de l'Ukraine par la Russie en février 2022 et s'est concentré sur les territoires ukrainiens occupés et sur plusieurs pays occidentaux - dont la France, l'Allemagne et la Pologne - qui soutenaient l'Ukraine.

Les sites de ce réseau ne produisent aucun contenu original mais relaient massivement des publications issues de trois types de sources : des comptes de réseaux sociaux d'acteurs russes ou pro-russes, des agences de presse russes et des sites officiels d'institutions ou d'acteurs locaux.

Son objectif principal est de couvrir le conflit russo-ukrainien en présentant ce que la Russie appelle « l'opération militaire spéciale » sous un jour positif et en dénigrant l'Ukraine et ses dirigeants. Très orientés idéologiquement, ces contenus présentent des récits manifestement inexacts ou trompeurs qui, s'agissant des portails ciblant la France, pravda-fr[.]com, l'Allemagne, pravda-de[.]com, et la Pologne, pravda-pl[.]com, participent directement à la polarisation du débat public.

Pour tenter d'atteindre un public plus large, ce réseau utilise un certain nombre de techniques telles que la sélection minutieuse de sources de propagande pro-russe en fonction de la localité ciblée, l'automatisation massive de la diffusion des contenus et l'optimisation du référencement sur les moteurs de recherche.

Conclusion

Des analyses convergentes permettent aujourd'hui d'affirmer que la dénonciation publique est l'un des principaux leviers de la lutte contre les attaques informationnelles : détecter, caractériser, dénoncer, faire connaître le plus largement possible.

Par ailleurs, notre gouvernement s'est organisé pour protéger notre démocratie et nos concitoyens directement visés par ces attaques informationnelles.

Dans le cas des manœuvres RRN et Étoiles de David, la dénonciation des faits a permis de contenir l'impact de ces campagnes.

Si la Russie mobilise d'énormes moyens humains, financiers et techniques à l'encontre de la France, pour des résultats qui demeurent limités aujourd'hui, la vigilance de la France et des partenaires européens est totale et notre coordination se renforce.