Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

19 juin 2024

Activités d'influence et désinformation

Rapport du Conseil fédéral en réponse au postulat 22.3006 CPS-N

Table des matières

1. Introduction

1.1 Postulat 22.3006

En janvier 2022, la Commission de la politique de sécurité du Conseil national (CPS-N) a déposé un postulat demandant un état des lieux relatif à la menace que constituent pour la Suisse les campagnes de désinformation.

Concrètement, le Conseil fédéral était prié d'élaborer un rapport indiquant dans quelle mesure notre pays était touché par des campagnes de désinformation ou des activités visant à influencer l'opinion publique. En outre, il était chargé de proposer des mesures permettant de prévenir cette menace. Le postulat se référait au rapport sur la politique de sécurité 2021 du Conseil fédéral, qui contenait un examen détaillé de cette question et indiquait que les activités d'influence pouvaient saboter des processus politiques et nuire à la confiance accordée par la population aux institutions démocratiques. Les luttes de pouvoir menées au niveau international accroissent le risque pour la Suisse de devenir, elle aussi, la cible de telles activités.

Le 23 février 2022, le Conseil fédéral a proposé d'accepter le postulat, lequel a été adopté par le Conseil national le 9 mars 2022.

1.2 Actualité et contextualisation

En Europe et dans le voisinage de la Suisse, la situation est devenue plus instable, plus confuse et plus imprévisible sur le plan de la sécurité. Les tensions et les rivalités entre les grandes puissances se sont accrues. À la suite de l'agression militaire de la Russie contre l'Ukraine, la guerre a fait son retour en Europe, ébranlant durablement l'ordre sécuritaire du continent. Dans le pourtour de ce dernier, d'anciens conflits armés se sont ravivés, et d'autres ont éclaté. Une escalade est à craindre au Proche-Orient, avec des conséquences mondiales. La polarisation s'accroît dans nombre de sociétés occidentales. Les valeurs démocratiques et les normes du droit international sont remises en question dans le monde entier. Façonnée par les changements liés à la politique de puissance et les évolutions technologiques, la conduite des conflits est en train de se transformer. Comme le montrent la guerre en Ukraine ou celle entre Israël et le Hamas, l'espace de l'information joue désormais un rôle important dans les hostilités et est utilisé par différents États pour des activités d'influence.

Le recours à des moyens relevant des conflits hybrides (p. ex. cyberattaques ou activités d'influence) s'est renforcé depuis le rapport sur la politique de sécurité 2021. Les États qui défendent ou veulent changer les rapports de force existants en usant de violence agissent plus qu'autrefois dans la zone grise entre le conflit armé et la paix. Les moyens engagés dans des conflits hybrides sont généralement complexes et imprévisibles. Souvent, les acteurs qui les utilisent sont à même de nier leur implication de manière plausible. Les sociétés ouvertes et démocratiques représentent des cibles de choix pour des activités d'influence visant les débats libres et les processus politiques, ce qui peut constituer une menace pour la sûreté intérieure comme extérieure. En conséquence, il convient de mieux identifier et de combattre les tentatives d'influence de la part d'acteurs étatiques ou mandatés par des États.

Les activités d'influence dans l'espace de l'information – qui comprennent la désinformation (cf. définitions au point 2.1) – font l'objet de discussions intenses au sein du monde politique et des médias de nombreux pays occidentaux. On leur attribue souvent un très grand potentiel destructeur. Si le défi qu'elles constituent n'est pas nouveau, elles sont désormais exacerbées non seulement par les changements liés à la politique de puissance, mais aussi par les évolutions technologiques, la vitesse de diffusion des informations et le rôle toujours plus grand des entreprises – des plateformes de médias sociaux aux « fermes à trolls » – dans la production et la dissémination de désinformation. L'utilisation généralisée des médias sociaux et les possibilités croissantes de générer et de partager des images, des fichiers audios et des vidéos grâce à l'intelligence artificielle (IA) rendent la situation encore plus complexe. En outre, des cyberattaques peuvent aussi accompagner et favoriser des activités d'influence. La polarisation croissante des sociétés est à la fois la source et l'objectif des activités d'influence.

Ce sont en premier lieu des acteurs étatiques ou mandatés par des États qui tentent d'exercer une influence et qui recourent à la désinformation, souvent de manière globale et coordonnée et avec des ressources considérables. Pour la Suisse, les acteurs qui menacent le plus la politique gouvernementale et la politique de sécurité sont ceux qui promeuvent de manière agressive des valeurs, des normes et

des systèmes politiques différents tout en cherchant à saper les institutions démocratiques. Les activités de la Russie, mais aussi de la Chine, devraient rester les plus notables pour la sécurité de notre pays à moyen et long termes.

Les alliances, communautés et États occidentaux sont également actifs dans l'espace de l'information et tentent de faire valoir leur point de vue dans les débats politiques d'autres pays. Cependant, ils ne sauraient être vus comme des menaces pour la politique de sécurité de la Suisse dès lors qu'ils ne remettent pas en question et ne sapent pas l'ordre étatique de notre pays et son système démocratique.

La guerre en Ukraine fournit des exemples actuels d'activités d'influence dans l'espace de l'information. S'adressant à un public mondial, des chaînes russes sur les réseaux sociaux et dans les médias en ligne proposent une interprétation alternative de la situation, propagent de la désinformation et offrent une vision distordue de la réalité en Ukraine. De son côté, le Kremlin utilise des mesures répressives pour contrôler avec succès le flux d'informations en Russie et dans les régions ukrainiennes occupées. La Chine accroît également ses activités d'influence dans le monde entier et en particulier dans les pays occidentaux. Son action a une portée systémique et stratégique, car elle est souvent initiée et dirigée par le Parti communiste lui-même. Elle sert des intérêts politiques et idéologiques qui s'opposent en grande partie aux principes démocratiques communément acceptés. En parallèle, la Chine durcit ses propres lois afin de se protéger contre les ingérences étrangères sur son territoire. De même, de nombreux autres États renforcent leurs dispositions afin de mieux contrôler l'espace national de l'information.

La Suisse, sa société civile et ses autorités sont elles aussi davantage visées par des activités d'influence. Notre engagement en faveur du droit international et de la démocratie, de même que la pression croissante pour se positionner sur l'échiquier géopolitique mondial, sont des facteurs qui contribuent à cette hausse. Située au cœur du continent européen, la Suisse partage les valeurs occidentales, fait partie de l'espace de l'information des pays de l'Ouest et dispose de connexions internationales fortes sur les plans économique et politique. Par conséquent, elle constitue depuis des années une cible indirecte d'activités dirigées contre les États occidentaux en général. Cependant, elle est aussi de plus en plus visée directement. En outre, le risque existe que son territoire serve de plaque tournante pour y mener ou y financer des activités d'influence contre des pays tiers ou des organisations internationales.

La Suisse est tenue de détecter les efforts systématiques de manipulation de l'espace de l'information par des acteurs étatiques ou mandatés par des États, d'identifier leurs auteurs et leurs intentions, et d'y réagir. À cette fin, il est crucial de savoir évaluer le potentiel et le fonctionnement des activités d'influence.

1.3 Objet et structure

Le présent rapport examine dans quelle mesure la Suisse est touchée par des activités d'influence ayant un impact sur l'espace de l'information et menées principalement par des acteurs étatiques ou mandatés par des États étrangers. Ces acteurs ont une incidence particulièrement grande sur la politique de sécurité. Mettant en lumière les conséquences de telles actions sur la politique gouvernementale et la politique de sécurité, il explique leurs répercussions tant directes qu'indirectes sur le fonctionnement, la résilience et la cohésion de l'État et de la société.

Le rapport présente tout d'abord les concepts et décrit les objectifs, les mécanismes, les acteurs et les effets des activités d'influence – y compris la désinformation – dans l'espace de l'information (chap. 2). Puis il explique comment d'autres États, alliances, communautés et organisations gèrent ces questions (chap. 3). Il expose ensuite l'état de la menace, l'ampleur du phénomène et les caractéristiques spécifiques de la Suisse, notamment à l'aide d'exemples concrets (chap. 4), ainsi que le cadre juridique actuel (chap. 5). Pour terminer, il présente les travaux entrepris et les compétences dans notre pays (chap. 6) ainsi que les options envisageables (chap. 7). À la fin du rapport, un glossaire répertorie les termes couramment employés en lien avec ce sujet.

2. Comprendre les activités d'influence et la désinformation

2.1 Définitions

Sur le plan de la politique de sécurité, les activités d'influence revêtent une importance particulièrement élevée si elles émanent d'un État, qu'elles sont dirigées contre le fonctionnement d'un État ou d'une société, ou qu'elles ont pour objectif de saper l'ordre démocratique d'un pays. En cela, elles se distinguent des démarches usuelles de représentation d'intérêts, lesquelles visent à contribuer de façon légitime à la formation de l'opinion, par exemple en politique ou dans les relations diplomatiques. Le présent rapport se concentre sur les activités d'influence dans l'espace de l'information, en opposition par exemple aux cyberattaques ou aux activités d'influence usant de moyens militaires (sabotage, déploiement de troupes sans insignes à l'étranger, etc.). Il se focalise sur les acteurs étatiques ou mandatés par des États étrangers qui sont particulièrement importants pour la politique de sécurité (et non sur des groupes terroristes ou des acteurs motivés uniquement par l'appât du gain).

Il n'existe pas de définitions précises et admises universellement pour les notions d'*influence* et de *désinformation*. Cependant, la plupart des travaux reposent sur une compréhension commune de leur signification. Les **activités d'influence dans l'espace de l'information** se réfèrent à différents comportements et stratégies visant à manipuler les perceptions, les réflexions et les actions d'individus, de groupes ou de sociétés entières. Elles peuvent être le fait d'acteurs tant étatiques que non étatiques. Leur arsenal comprend, outre la désinformation, des moyens comme l'omission délibérée de faits, la réinterprétation d'événements, la manipulation de contenus visuels, le recours à de faux profils sur les réseaux sociaux ou la censure.

La **désinformation** désigne des informations trompeuses ou entièrement inventées qui sont utilisées délibérément pour influencer la formation de l'opinion publique, manipuler les processus politiques, miner la crédibilité des institutions et des médias ou mettre en doute la fiabilité des informations[1]. L'Union européenne (UE) et l'Organisation du Traité de l'Atlantique Nord (OTAN), qui la définissent de façon similaire, la comprennent dans un sens large comme des informations manifestement fausses ou trompeuses qui sont créées, présentées et diffusées dans un but lucratif ou pour tromper intentionnellement le public[2]. La désinformation peut être produite et disséminée par divers acteurs dans différents buts. Elle ne constitue pas toujours une activité d'influence et n'a pas nécessairement de conséquences importantes sur la politique gouvernementale ou la politique de sécurité.

Tant les activités d'influence que la désinformation se caractérisent principalement par la diffusion délibérée de fausses informations dans l'intention de tromper. Elles se distinguent ainsi de la mésinformation (de l'anglais *misinformation* ; cf. glossaire), qui consiste à transmettre des informations que l'on croit véridiques mais qui sont en réalité erronées. En d'autres termes, elles n'incluent pas les erreurs ni les fausses informations propagées de bonne foi, non plus que la satire, la parodie ou les informations ou commentaires partisans qui peuvent être clairement identifiés comme tels.

2.2 Objectifs et méthodes

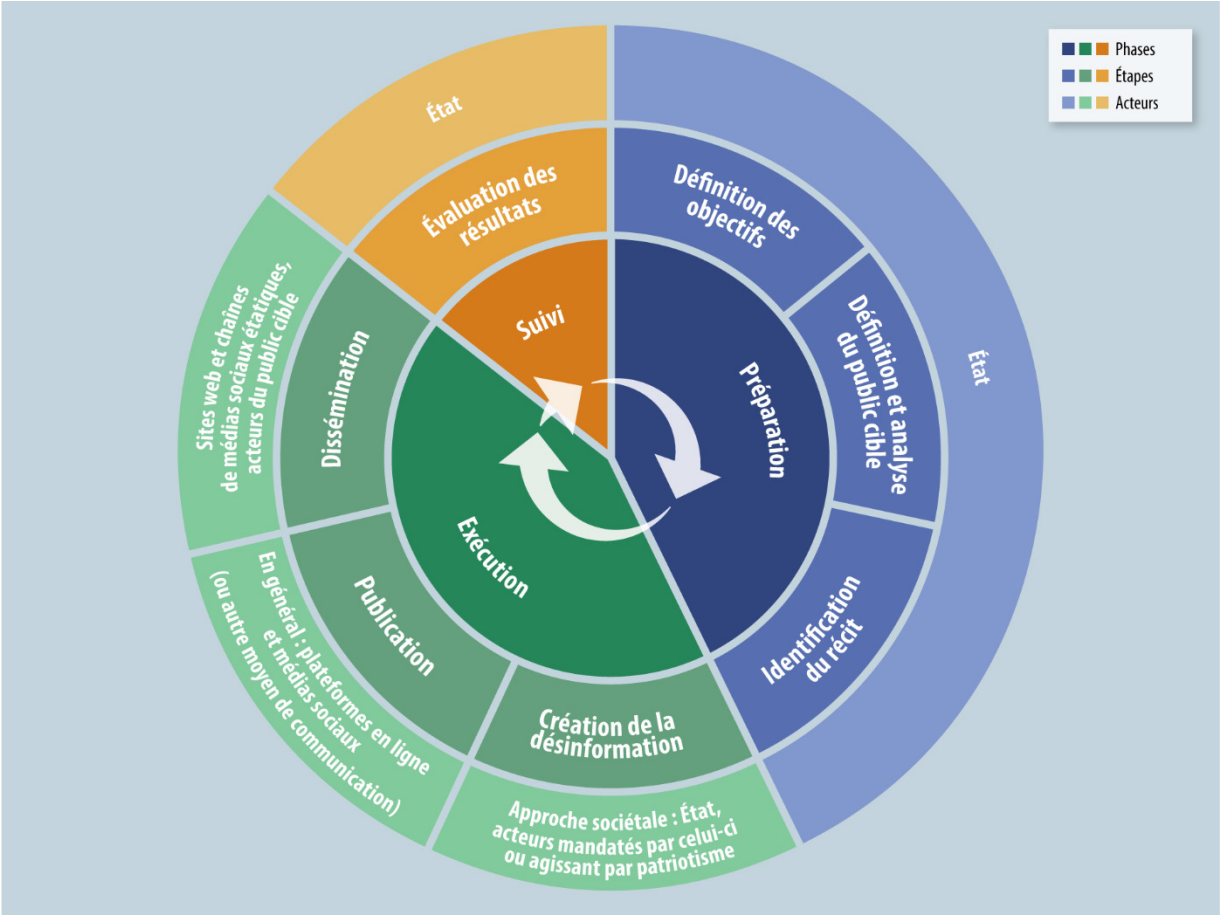
Les activités d'influence menées par des États visent souvent des sociétés ouvertes et démocratiques qui connaissent des débats d'idées honnêtes fondés sur des faits établis et où la libre circulation des informations – même fausses – constitue un droit fondamental. Leur objectif consiste généralement à manipuler l'opinion publique et la prise de décisions (notamment au niveau politique) afin de convaincre un groupe cible d'un certain point de vue ou de fragiliser la crédibilité de la partie adverse. Il s'agit de semer le trouble, la peur, l'indignation ou la division au sein de la population ciblée, ainsi que de miner la confiance dans les institutions étatiques.

Une ou plusieurs sources se chargent de relayer les contenus à travers différents canaux d'information. En général, les acteurs définissent le public cible à l'avance et choisissent un contexte et un moment permettant de maximiser l'effet de leurs agissements. Ils peuvent coordonner plusieurs activités dans le cadre d'une opération. Le graphique 1 illustre la préparation d'une telle action coordonnée et ses suites. Toutes les activités ne sont pas nécessairement planifiées de longue date ni dans les moindres détails.

[1] Office fédéral de la communication, rapport *Désinformation en Suisse 2021* (en allemand).
[2] Cf. https://commission.europa.eu et https://www.nato.int.

De même, il n'y a aucune garantie que l'objectif visé puisse être atteint, même en cas de planification minutieuse et d'investissements élevés.

Les acteurs qui veulent exercer une influence ont particulièrement besoin de comprendre leurs groupes cibles. Pour les individus, ils peuvent jouer sur certains traits de personnalité comme la vanité ou l'altruisme. Pour les groupes, ils peuvent exploiter des caractéristiques sociodémographiques ou collectives telles que des traumatismes nationaux ou des fractures sociales. Il est probable qu'ils ne parviennent pas toujours à atteindre exactement leur public cible ou à calibrer leurs contenus avec précision. Cependant, la désinformation a un impact dès le moment où elle sème le doute concernant des faits établis ou des informations officielles, sans que son message spécifique soit pour autant considéré comme vrai. Des indices montrent également que les activités d'influence recourent à une multitude de récits, parfois même contradictoires, afin d'accroître leurs chances de succès auprès de différents groupes cibles. Ces activités comportent toutefois aussi des risques et peuvent se révéler contreproductives si leur origine est découverte, raison pour laquelle des efforts considérables sont généralement déployés pour la dissimuler.



Graphique 1 Déroulement et acteurs d'une opération de désinformation étatique

Même lorsque la désinformation est identifiée comme telle et réfutée, elle continue souvent d'être propagée. En psychologie, il est en effet démontré que les gens croient plus facilement les affirmations répétées régulièrement, indépendamment de leur véracité (effet de vérité illusoire[3]).

Les activités d'influence menées dans l'espace de l'information englobent un large éventail de méthodes telles que la falsification de contenus audiovisuels, la présentation d'informations hors de leur contexte, la création de récits alternatifs et l'utilisation de faux comptes en ligne pour propager des idées. Les

[3] Catherine Hackett Renner, *Validity effect,* in Rüdiger F. Pohl (éd.), *Cognitive illusions,* Psychology Press (Hove, Royaume-Uni : 2004), p. 201–213.

méthodes employées ont généralement pour but de rendre la désinformation difficile à distinguer, par le public visé, d'articles au point de vue équilibré et bien documentés. C'est pourquoi les contenus diffusés sont aussi repris dans des médias d'apparence sérieuse et objective ou sur des médias en ligne alternatifs. La crédibilité de la désinformation est en outre renforcée lorsqu'elle s'appuie sur les déclarations de prétendus experts.

Une autre méthode consiste à cloner le visuel de sites d'information connus et à y insérer de la désinformation afin de profiter de la popularité et de la crédibilité de ces portails. Fin 2022, des recherches menées par la presse allemande et les ONG DisinfoLab et Qurium ont ainsi permis de mettre au jour l'opération *Doppelgänger*. Une soixantaine de faux sites d'actualités imitant de grands médias internationaux (Le Monde, The Guardian, Spiegel, etc.) ont été mis en ligne, tandis que plus de 1600 comptes et plusieurs centaines de fausses pages ont été créés sur les réseaux sociaux. Selon un rapport de sécurité de Meta du 29 août 2023, l'opération visait à disséminer de la désinformation favorable à la Russie concernant la guerre en Ukraine[4].

Par ailleurs, des cyberattaques peuvent favoriser des activités d'influence, par exemple en dérobant des informations sensibles ou classifiées qui seront ensuite diffusées auprès d'un public cible dans leur version originale ou sous une forme manipulée (méthode *hack and leak*).

2.3 Acteurs

Comme le montre le graphique 1, les activités d'influence peuvent inclure une multitude d'acteurs, dont des organes étatiques, des entreprises (p. ex. plateformes ou médias) et des individus (p. ex. internautes), qui y participent intentionnellement (voire sur ordre) ou involontairement. Par conséquent, les acteurs de l'influence ont des difficultés à contrôler et à coordonner ce processus. C'est également pour cette raison que ces activités ne réussissent pas forcément, même avec des ressources considérables.

Des personnalités politiques et des membres de la société civile, réels ou semblant l'être, peuvent servir de vecteurs à des activités d'influence. Par exemple, pour promouvoir son point de vue, la Russie utilise souvent comme couvertures des institutions ou des associations qui se prétendent apolitiques, ainsi que des partis et des politiciens pro-russes présents dans les pays occidentaux. Leurs liens avec l'État russe et leur financement par celui-ci doivent rester cachés. Par le biais de dons à des partis politiques, de conférences et d'invitations à visiter la Russie, le Kremlin a forgé un réseau de politiciens européens de toutes tendances qui sont bienveillants à son égard. De son côté, la Chine instrumentalise en sous-main sa diaspora pour défendre et promouvoir ses intérêts. Elle accroît également son influence en utilisant à ses propres fins des acteurs clés qui ne sont pas chinois, parfois à l'insu de ceux-ci. Les personnes ciblées peuvent par exemple faire partie des médias, du monde politique, d'administrations, d'entreprises, d'universités ou d'associations.

L'essor de la digitalisation et la diversité des moyens technologiques qui en découle permettent de diffuser des informations à moindre coût à un large public situé au-delà de ses propres frontières. Dans ce contexte, les utilisateurs peuvent être plus que de simples récepteurs d'informations : ils peuvent partager des contenus numériques, les commenter et les *liker*, contribuant ainsi – consciemment ou non – à la propagation de désinformation à une plus large échelle, dans le but par exemple de générer des clics ou de l'attention. Dans les médias sociaux, il est particulièrement difficile, voire impossible, de détecter la désinformation ou ses auteurs en temps réel. Selon les analyses de l'UE, les activités d'influence recourent en premier lieu à des photos et à des vidéos[5]. Par exemple, la Russie fait un usage intensif de moyens numériques de communication et d'information pour répandre de la désinformation.

---

[4] Meta, Meta's Adversarial Threat Report, Fourth Quarter 2022, 23 février 2023, <https://about.fb.com/news/2023/02/metas-adversarial-threat-report-q4-2022> (consulté le 21 février 2024).
[5] SEAE, Report on FIMI Threats, février 2023, p. 5, <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf> (consulté le 21 février 2024).

Outre les médias sociaux, elle utilise également ses émetteurs étatiques internationaux Russia Today (RT) et Sputnik, qui sont diffusés dans le monde entier dans une trentaine de langues, y compris en français et en allemand.

Des acteurs privés de l'industrie de la désinformation, véritables mercenaires de l'influence numérique (*influence-for-hire*), peuvent aussi encourager l'utilisation de méthodes et de technologies de manipulation en commercialisant en ligne divers services et logiciels dans ce domaine. Par exemple, l'entreprise israélienne Team Jorge, démasquée en 2022, proposait de manipuler des élections, notamment par le biais de la désinformation.

Sur les médias sociaux et dans les forums en ligne, les faux comptes de trolls et de bots peuvent lancer des débats, remettre en question des affirmations et propager des rumeurs. Des bots sociaux ou des personnes mandatées par des États qui se font passer pour des utilisateurs ordinaires au moyen d'une fausse identité peuvent générer de nombreux contenus et, ainsi, donner l'impression erronée qu'une multitude de gens défendent le même point de vue. Par exemple, des logiciels sont capables de publier automatiquement des réponses standardisées sur des forums concernant des thèmes particuliers.

Fin août 2023, l'entreprise Meta a identifié un réseau de 7704 faux comptes, 954 pages et groupes sur Facebook et de 15 comptes sur Instagram apparemment utilisés afin de disséminer de la désinformation pour le compte de la Chine. L'objectif principal était de diffuser des commentaires positifs sur la Chine et la province du Xinjiang, où l'État chinois mène une répression massive contre la minorité ouïghoure, de même que des messages ciblant les États-Unis, des gouvernements occidentaux ainsi que des journalistes et des chercheurs résidant en Chine qui se montraient critiques envers le gouvernement chinois[6].

Par conséquent, les plateformes numériques jouent un rôle central dans la propagation de la désinformation. Leurs algorithmes souvent opaques, de même que ceux des moteurs de recherche, peuvent recommander des pages aux utilisateurs en fonction de leurs préférences et de leurs intérêts, et mettre en avant les contenus les plus partagés. Il est fréquent qu'une personne qui a déjà été en contact avec de la désinformation ou qui a un profil susceptible d'y être réceptive se voie proposer des contenus similaires à ceux qu'elle a déjà consultés. Ainsi, le caractère ouvert d'internet, combiné à des barrières techniques à l'entrée peu élevées et à l'absence d'informations sélectionnées par des journalistes, peut renforcer la propagation de la désinformation[7]. Cette dernière est également colportée sur les plateformes numériques et les portails médiatiques, car les entreprises concernées font la chasse aux clics pour s'assurer des revenus. C'est pourquoi des médias, réels ou fictifs, propagent des contenus insuffisamment vérifiés qui présentent souvent des titres accrocheurs ou des miniatures trompeuses (« piège à clics »).

Les conditions d'utilisation et les services de modération varient considérablement d'une plateforme à l'autre. En réaction à certaines restrictions comme l'interdiction de RT et de Sputnik par l'UE ou le blocage de nombre de ses comptes fictifs sur les réseaux sociaux, la Russie recourt de plus en plus à d'autres canaux sur internet, notamment à des adresses web légèrement modifiées ou à de nouvelles plateformes. Depuis le début de la guerre en Ukraine, on constate une recrudescence de la propagande russe dans des langues européennes sur des plateformes non occidentales peu réglementées telles que TikTok ou Telegram.

Le développement fulgurant de l'IA et sa prolifération risquent d'accroître de façon dramatique le potentiel des activités d'influence, et ce, sur le plan tant quantitatif que qualitatif. En effet, l'IA permet d'automatiser nombre de processus nécessaires à la création et à la diffusion de désinformation. On peut citer l'exemple des *deep fakes*, c'est-à-dire des vidéos, des photos ou des fichiers audios manipulés à l'aide de l'IA, souvent avec un investissement moindre en ressources et en temps, pour falsifier des

[6] The Guardian, Meta closes nearly 9,000 Facebook and Instagram accounts linked to Chinese 'Spamouflage' foreign influence campaign, 29 août 2023, <https://www.theguardian.com/australia-news/2023/aug/30/meta-facebook-instagram-shuts-down-spamouflage-network-china-foreign-influence> (consulté le 23 février 2024).
[7] Cf. *Saurwein/Spencer-Smith,* Inhaltsregulierung auf Internet-Plattformen. Optionen für verantwortungsorientierte Governance auf nationaler Ebene, p. 42.

événements ou des personnes de manière très réaliste. Ces contenus peuvent ensuite être diffusés sur tous les canaux usuels, en particulier sur les médias sociaux dépourvus de modération. Des outils tels que les grands modèles de langage facilitent le recours à de faux comptes d'utilisateurs et la simulation de mouvements sociaux (*astroturfing*). Comme ces instruments sont toujours plus performants, les individus et les autorités de surveillance et de régulation ont de plus en plus de mal à discerner que les résultats correspondants ont été générés artificiellement.

2.4 Effets possibles

Toutes les activités d'influence partent du postulat que les actions menées dans l'espace de l'information peuvent affecter les pensées, les discours et les comportements des individus. Elles peuvent saper la confiance dans les institutions, empêcher la libre formation des opinions et entraver les processus décisionnels, mettant ainsi en péril la marge de manœuvre des États, les processus démocratiques et la sécurité nationale, et ce, même si elles ne touchent qu'une infime partie de la population. Il convient de distinguer les effets en fonction de leur horizon temporel. À court terme, il peut par exemple s'agir d'influer sur la formation des opinions pour une votation. À moyen terme, c'est le ton, les caractéristiques et le degré de polarisation du discours politique d'un pays qui peuvent être visés. Enfin, la confiance dans les institutions peut constituer une cible à long terme.

Il est difficile de mesurer précisément l'impact des activités d'influence, par exemple lorsqu'elles sont menées par des États sur les réseaux sociaux[8]. Les milieux scientifiques et les médias en tirent des conclusions variées quant à leurs effets possibles et aux facteurs qui les favorisent (combinaisons de contenus de désinformation, moment choisi pour le déclenchement de l'opération, potentiel de diffusion, contexte). Dans ce contexte, il est pertinent d'étudier les effets des activités d'influence et de désinformation durables et potentiellement coordonnées plutôt que des activités ponctuelles.

Les activités d'influence et la désinformation peuvent contribuer à saper durablement la confiance placée dans les personnalités politiques et publiques en général, les médias, les institutions et les informations elles-mêmes. Elles peuvent entraver le processus de libre formation de l'opinion et de la volonté publiques dans les démocraties. Les personnes touchées peuvent se désintéresser de la politique, car leur confiance dans les informations et les processus s'est érodée. La défiance envers les institutions et les processus démocratiques peut compliquer la communication et la recherche de compromis au-delà des clivages politiques, car les certitudes communes relatives aux faits sont remises en question en tant que fondement des débats politiques. Les activités d'influence peuvent par exemple saper la confiance dans la police ou les autorités de poursuite pénale en donnant l'impression que les autorités mènent des enquêtes partiales, agissent de manière arbitraire ou sont « infiltrées ». Dans le pire des cas, cela peut conduire à une radicalisation des personnes concernées.

L'impact structurel et durable des activités d'influence peut ensuite à nouveau préparer le terrain pour d'éventuels effets à court terme comme la mobilisation politique ou le recours à la violence. En outre, la désinformation et les activités d'influence limitent parfois la marge de manœuvre des autorités en les contraignant à mobiliser des ressources, notamment en période de crise et d'insécurité.

Différents exemples illustrent les activités d'influence menées par des États étrangers et leurs répercussions sur la résilience des institutions démocratiques. Des comptes russes sur Facebook et X/Twitter ont propagé de la désinformation concernant le référendum sur le Brexit au Royaume-Uni et les élections présidentielles américaines de 2016[9]. Lors de la campagne présidentielle de 2017, la France a été victime d'une ingérence russe sous la forme de fuites de données sensibles visant à discréditer le principal candidat, Emmanuel Macron.

Les contenus diffusés par les pirates russes concernaient notamment la migration, l'abandon des structures familiales traditionnelles, la critique des livraisons d'armes à l'Ukraine et les violences policières discriminatoires. Tous ces sujets reflètent aussi des opinions, des craintes et des revendications qui sont réellement celles d'une partie de la société. Il est donc difficile d'opérer une distinction nette entre ce qui relève de la libre formation de l'opinion et ce qui découle de la manipulation

[8] Jon Bateman, Elonnai Hickok et al., Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research, 28 juin 2021, <https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824> (consulté le 5 avril 2024).
[9] *Bayer et al.,* Disinformation and propaganda.

et de la tromperie par le biais d'exagérations. Dans certains domaines politiques, les activités d'influence menées dans l'espace de l'information s'accompagnent d'autres moyens utilisés dans des conflits hybrides. Par exemple, à l'automne 2021, le régime bélarussien a dirigé des migrants en provenance du Proche et du Moyen-Orient vers sa frontière avec la Pologne et la Lituanie. Cet événement s'est accompagné de désinformation dans les médias russes qui dénonçant le caractère totalement dysfonctionnel des systèmes européens d'asile et de migration. Cependant, la Russie peine actuellement à influencer de manière significative l'opinion publique majoritaire et les décisions politiques dans les pays occidentaux, notamment en ce qui concerne la guerre en Ukraine.

Pendant la pandémie de COVID-19, la désinformation a alimenté le scepticisme à l'égard des services étatiques en faisant appel aux émotions et aux peurs. Ainsi, elle peut conduire les gens à ignorer les consignes sanitaires des autorités et à mettre leur santé en danger. En ce sens, elle relève de la politique de sécurité et peut avoir des répercussions sur la situation économique et financière d'un pays, même à court terme. Par exemple, une photo générée par l'IA d'un bâtiment gouvernemental américain apparemment en feu a fait le tour de Facebook et de X/Twitter en quelques minutes, y compris sur les comptes de RT. Cet événement explique en partie le creux atteint à court terme par les marchés boursiers américains ce jour-là[10].

Les activités d'influence et la désinformation peuvent aussi avoir un impact sur la promotion de la paix et les efforts humanitaires. Ainsi, elles affectent ou ont affecté les missions de promotion de la paix de l'Organisation des Nations Unies (ONU) au Mali, en République démocratique du Congo et en République centrafricaine. Dans cette dernière, une campagne de désinformation en ligne a notamment accusé, au moyen de vidéos falsifiées, quatre collaborateurs de l'ONU de fournir des armes aux rebelles et incité à la violence contre la mission[11]. De telles affirmations mensongères alimentent le ressentiment au sein de la population locale, ce qui peut provoquer des actes de violence, mettre en danger la sécurité du personnel des missions internationales et compromettre la promotion de la paix et de la sécurité dans le pays[12]. Même des organisations humanitaires comme le Comité international de la Croix-Rouge peuvent être la cible de ce genre d'activités.

3. Évaluation et gestion en comparaison internationale

Ces dernières années, un nombre croissant d'États et d'organisations internationales (p. ex. OTAN, UE) ont reconnu que les activités d'influence dans l'espace de l'information représentaient un défi pour leur sécurité. Les pays qui se sentent particulièrement concernés – comme les États-Unis, le Royaume-Uni, la France ou l'Allemagne en raison de leur présence internationale, ou l'Australie, les pays nordiques ou les États baltes vu leur proximité géographique avec la Chine ou la Russie – ont déjà pris des mesures plus poussées. Compte tenu des répercussions transversales, des efforts sont aussi déployés au niveau international pour renforcer la collaboration et la coordination.

Il convient de noter que de nombreuses contre-mesures n'ont été testées que de manière limitée et que leur conception et leur efficacité dépendent fortement du contexte national. Les approches que nous présentons ci-après ne sont donc pas exhaustives.

3.1 Approche stratégique

L'Australie, l'Allemagne, la France, les Pays-Bas, le Canada, l'Autriche, le Royaume-Uni et les États-Unis considèrent les activités d'influence et la désinformation comme des menaces stratégiques. Les

[10] The New York Times, An A.I.-Generated Spoof Rattles the Markets, 23 mai 2023, <https://www.nytimes.com/2023/05/23/business/ai-picture-stock-market.html#:~:text=Fake%20news%2C%20real%20market%20drop,investor%20fears%2C%20sending%20stocks%20tumbling> (consulté le 21 février 2024).
[11] Albert Trithart, Disinformation against UN Peacekeeping Operations, International Peace Institute, novembre 2022, p. 3, <https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf> (consulté le 21 février 2024).
[12] Lors d'un sondage réalisé auprès du personnel de promotion de la paix de l'ONU, 75 % des personnes interrogées ont ainsi indiqué que la désinformation avait un impact sur leur sécurité. Cf. ibid., p. 13.

Pays-Bas les qualifient explicitement de menaces contre la sécurité nationale[13]. L'Allemagne[14] et la France[15] soulignent qu'elles menacent les processus de formation de la volonté démocratique. Les États-Unis[16] et le Royaume-Uni[17] relèvent en outre le risque d'une ingérence sur la libre formation de l'opinion politique par le biais de la désinformation, la combinaison de celle-ci avec les nouvelles technologies et le *big data* étant considérée comme particulièrement préoccupante. Ces États estiment qu'il faut notamment renforcer la détection précoce de telles menaces ainsi que la résilience des institutions et de la société. L'Allemagne prévoit d'élaborer deux stratégies, l'une pour accroître la capacité d'action face aux menaces hybrides, l'autre pour combattre la désinformation. De son côté, l'Autriche privilégie la mise en place et le développement de formats de coopération civilo-militaires et l'intensification de la collaboration avec d'autres États membres de l'UE.

Sur la base de sa boussole stratégique en matière de sécurité et de défense de 2022, l'UE a développé une boîte à outils pour lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger (*Foreign Information Manipulation and Interference Toolbox*, FIMI). Il s'agit d'améliorer l'appréciation de la situation et l'alerte précoce, de renforcer la résilience de la société et d'appliquer des mesures réglementaires et restrictives dans le cadre de régimes de sanctions géographiques. À partir de 2024, toutes les missions et opérations menées au titre de la politique de sécurité et de défense commune de l'UE doivent pouvoir faire face à la manipulation de l'information et à l'ingérence étrangère. Selon son concept stratégique 2022, l'OTAN investira dans ses capacités afin de se préparer aux menaces hybrides comme la désinformation ou les activités d'influence. Alarmée par les risques croissants encourus par les missions internationales de promotion de la paix, l'ONU a également pris conscience de la situation ces dernières années. En juillet 2022, le Conseil de sécurité a exprimé sa préoccupation face aux conséquences toujours plus fortes de la désinformation sur ces missions. La rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression a abordé la question de la désinformation dans ses deux derniers rapports[18].

3.2 Surveillance de la situation et détection précoce

Plusieurs États ont créé des institutions spécifiquement dédiées à la détection précoce. Le Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a été créé par la France en juillet 2021. À partir de sources publiques, il analyse les contenus utilisés dans les activités d'influence étrangères, en particulier avant les élections. En 2022, la Suède a mis en place une agence de défense psychologique[19] dans le but d'identifier, d'analyser et de combattre les activités d'influence étrangères dans l'espace de l'information tout en renforçant la résilience de sa population. Au Royaume-Uni également, une direction du ministère des Affaires étrangères analyse et étudie les informations accessibles au public et, sur cette base, élabore des stratégies et des contre-mesures. Une task force chargée de la défense de la démocratie (*Defending Democracy Taskforce*) se concentre spécifiquement sur l'identification précoce des menaces planant sur les élections en raison d'activités d'influence dans l'espace de l'information. Aux États-Unis, le Centre d'engagement mondial (*Global Engagement Center*) surveille la situation et oppose des faits aux récits propagés par la Russie[20].

Sous la présidence du Canada, le Groupe des sept (G7) a mis en place le Mécanisme de réponse rapide en 2018 afin d'analyser l'espace de l'information et d'identifier les menaces potentielles. Il s'agit également d'appliquer des mesures communes et de renforcer la coordination. L'Australie, la Nouvelle-Zélande, les Pays-Bas, la Suède et l'OTAN sont représentés au sein de cet organe en qualité d'observateurs. En ce qui concerne l'UE, le système d'alerte rapide du Service européen pour

---

[13] The Security Strategy for the Kingdom of the Netherlands, 3 avril 2023, <https://www.government.nl/binaries/government/documenten/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands/Security+Strategy+for+the+Kingdom+of+the+Netherlands.pdf> (consulté le 21 février 2024).

[14] Document *Nationale Sicherheitsstrategie* de juin 2023.

[15] Document Actualisation stratégique 2021.

[16] Document *US 2023 Annual Threat Assessment*.

[17] Document *UK Integrated Review of Security, Defence, Development and Foreign Policy 2021*.

[18] HCDH, Désinformation et liberté d'opinion et d'expression pendant les conflits armés, 12 août 2022, <https://www.ohchr.org/fr/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed> ; HCDH, Liberté d'expression et la dimension de genre de la désinformation, 7 août 2023, <https://www.ohchr.org/fr/calls-for-input/2023/report-freedom-expression-and-gender-dimensions-disinformation>.

[19] *Myndigheten för psykologiskt försvar* (*Psychological Defence Agency*)

[20] <https://www.state.gov/disarming-disinformation/#reports>

l'action extérieure (SEAE) promeut l'échange d'informations entre les États membres. La plateforme d'information EUvsDisinfo[21] analyse et publie des récits trompeurs afin d'y sensibiliser la population. Dans son deuxième rapport sur les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, publié en janvier 2024, le SEAE fait état de 750 incidents d'activités d'influence pour la période allant de décembre 2022 à novembre 2023[22].

3.3 Résilience fondée sur la sensibilisation, l'éducation et les compétences médiatiques

Pour les gouvernements démocratiques comme pour le secteur de la recherche, le renforcement de la résilience et une approche sociétale globale constituent les mesures les plus importantes – et un défi de taille – pour combattre les activités d'influence dans l'espace de l'information. Les nombreuses initiatives lancées dans ce domaine mettent notamment l'accent sur la sensibilisation de la société, les compétences médiatiques de la population et la qualité des médias.

L'Allemagne met en place un centre dédié à la stratégie, à l'analyse et à la résilience où sont représentés les ministères de l'Intérieur, des Affaires étrangères et de la Défense. La Suède collabore avec des organisations de la société civile, des institutions de recherche, des médias et des communes afin de contrer les activités d'influence et de sensibiliser la population. De plus, elle investit annuellement 1,2 million d'euros[23] dans la recherche. Ces dernières années, le Royaume-Uni a cherché à renforcer les compétences médiatiques de la population au moyen de campagnes et d'initiatives de réglementation. L'Australie déploie des efforts dans le même sens.

L'Observatoire européen des médias numériques (EDMO) est un réseau financé par l'UE qui réunit des acteurs issus des médias, des plateformes numériques, de la société civile et du secteur de la recherche afin d'analyser des campagnes de désinformation, de surveiller les mesures prises par le secteur des nouvelles technologies et de renforcer les compétences médiatiques de la population. Il prend part à la révision et à l'évaluation du Code de bonnes pratiques renforcé contre la désinformation (cf. pt 3.4).

D'autres initiatives étatiques communes auxquelles la Suisse participe visent à mieux protéger les journalistes et les professionnels des médias, la sphère privée et l'accès à des informations fiables. Parmi elles, on peut citer la Coalition pour la liberté des médias, la Coalition pour la liberté en ligne et le Partenariat pour l'information et la démocratie.

3.4 Réglementation et sanctions

De nombreux pays ont pris des initiatives afin de réguler les plateformes numériques. Les démarches sont très variées, allant de la réglementation étatique à l'autorégulation en passant par la coréglementation. Les approches législatives se concentrent sur la suppression ou l'étiquetage de contenus considérés comme nuisibles, la transparence de la publicité, le renforcement des droits des utilisateurs et le soutien à la recherche. Sur la base d'un acte législatif fixant le budget et les politiques en matière de défense (*2020 National Defense Authorization Act*), les États-Unis ont créé un centre d'analyse des menaces et des données des médias sociaux (*Social Media Data and Threat Analysis Center*) afin d'assurer la coordination avec les plateformes de médias sociaux.

Au niveau de l'UE, le règlement sur les services numériques (*Digital Services Act*, DSA) est entré en vigueur en août 2023. Mis en œuvre par les plateformes de manière partiellement autonome, il vise à empêcher la diffusion de contenus illégaux dans l'espace numérique et à protéger les droits fondamentaux des utilisateurs. Il couvre en partie la désinformation en ce qui concerne les discours de haine (et autres délits d'expression) et les menaces à la sûreté publique. En octobre 2023, dans le contexte de la guerre entre Israël et le Hamas, la Commission européenne a formellement demandé des informations à Meta et à TikTok sur les mesures que ces plateformes prennent contre la propagation de désinformation. Elle a en outre accéléré la surveillance et la concrétisation du DSA, notamment par un

[21] <https://euvsdisinfo.eu/fr/>
[22] SEAE, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, janvier 2024, <https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en> (consulté le 5 mars 2024)
[23] Jean-Bapiste Jeangène Vilmer : Effective State Practices against disinformation : Four country case studies. Hybrid CoE Research Report 2 (juillet 2021), p. 12.

mécanisme de coordination entre les États membres pour lutter contre la diffusion de contenus illégaux.

La Commission européenne entend combattre la désinformation sur les médias sociaux au moyen d'un code de conduite volontaire destiné aux entreprises actives dans les domaines de la technologie et de la publicité. Jusqu'à présent, ce Code de bonnes pratiques contre la désinformation a été adopté par 40 entreprises. Comme il manquait d'efficacité, il a été révisé pour devenir le Code de bonnes pratiques renforcé contre la désinformation, lequel inclut une task force permanente[24]. L'ONU recourt également à un code de conduite pour contrer la propagation de désinformation en ligne. Il s'agit d'inciter les acteurs étatiques et non étatiques à lutter contre la désinformation et à respecter les droits de l'homme. Certains pays optent en outre pour des approches réglementaires directes. Par exemple, le gouvernement norvégien a proposé un projet de loi visant à réprimer la participation à des activités d'influence menées pour le compte de services de renseignement étrangers. Plusieurs pays – comme le Brésil, la France, le Cambodge, le Kenya et la Croatie – ont édicté des lois contre la désinformation en ligne touchant les élections. Un grand nombre de ces actes législatifs ont suscité des craintes et des protestations concernant la liberté d'opinion et la liberté des médias, au point que certains États les ont déjà abrogés.

La boîte à outils FIMI développée par l'UE (cf. point 3.1) inclut, dans le cadre de régimes de sanctions géographiques, des mesures restrictives contre des personnes et des entreprises qui sont responsables d'activités d'influence dans l'espace de l'information. Dans le contexte de la guerre en Ukraine, l'UE et ses États membres ont ainsi imposé des sanctions (interdictions d'entrée, gels des avoirs, interdiction de la mise à disposition d'avoirs ou de ressources économiques, retraits de licences) à des individus et des entités russes, dont cinq chaînes de RT et Sputnik. Le 28 juillet 2023, l'UE a encore sanctionné sept personnes et cinq entités pour des cas de manipulation de l'information[25]. Le 30 mai 2023 et le 22 février 2024, l'UE a prononcé des sanctions à l'encontre d'entreprises et d'individus moldaves pour des actes de déstabilisation dans ce pays, notamment par le biais de la désinformation[26].

Plusieurs pays, dont le Royaume-Uni, les États-Unis et l'Australie, ont adopté des sanctions à l'encontre d'agents d'influence et de leurs plateformes. Les principales entreprises occidentales de médias sociaux comme Facebook, YouTube ou X/Twitter ont restreint, à divers degrés, l'accès à des contenus provenant de sources russes proches de l'État ainsi que leur diffusion.

3.5 Compétences, coordination et communication

Puisque les activités d'influence dans l'espace de l'information touchent un grand nombre de domaines et de compétences, les responsabilités sont réglées de diverses manières au sein des gouvernements et réparties entre de nombreux ministères. Une coordination est donc indispensable.

En France, la responsabilité principale est assumée par le bureau du Premier ministre, auquel Viginum est également rattaché. Un comité d'éthique scientifique surveille les activités de l'organisation. En Allemagne, c'est le ministère de l'Intérieur qui s'occupe des questions liées à l'influence et à la désinformation. Il est chargé de la coordination d'un groupe de travail interdépartemental. En Suède, l'agence de défense psychologique est rattachée au ministère de la Défense. Les pays baltes ont l'intention explicite de combattre les activités d'influence et la désinformation à l'échelle nationale, par exemple en promouvant les compétences médiatiques de la population et en intégrant les minorités, notamment russes. Une quarantaine de collaborateurs du SEAE conseillent l'UE et ses États

[24] Les membres de la task force comprennent les organisations signataires, le Groupe des régulateurs européens pour les services de médias audiovisuels, l'Observatoire européen des médias numériques et le SEAE. La présidence est assurée par la Commission européenne.
[25] Conseil de l'UE, communiqué de presse, Manipulation de l'information dans la guerre d'agression de la Russie contre l'Ukraine : l'UE inscrit sept personnes et cinq entités, 28 juillet 2023, <https://www.consilium.europa.eu/fr/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/> (version anglaise consultée le 21 février 2024).
[26] Conseil de l'UE, communiqué de presse, République de Moldavie : inscription de sept personnes sur la liste de sanctions en raison de leurs actions de déstabilisation et de leurs actions compromettant l'intégrité territoriale de l'Ukraine, 30 mai 2023, <https://www.consilium.europa.eu/fr/press/press-releases/2023/05/30/republic-of-moldova-7-individuals-listed-for-their-destabilising-actions-and-for-undermining-the-territorial-integrity-of-ukraine/> ; Conseil de l'UE, communiqué de presse, République de Moldavie : mesures restrictives à l'encontre de six personnes et d'une entité pour atteinte à l'État de droit, à la stabilité et à la sécurité dans le pays, 22 février 2024, <https://www.consilium.europa.eu/fr/press/press-releases/2024/02/22/republic-of-moldova-six-individuals-and-one-entity-listed-for-undermining-the-rule-of-law-stability-and-security-in-the-country/> (version anglaise consultée le 18 mars 2024).

membres sur la manière de faire face aux activités d'influence illégitimes et à la désinformation provenant d'acteurs étrangers. De plus, ils élaborent des rapports annuels à ce sujet. Au Royaume-Uni, le ministère des Affaires étrangères se charge de la coordination des activités, différents services gouvernementaux s'occupant aussi de ce thème selon leur perspective. La situation est similaire aux États-Unis, où le Centre d'engagement mondial est rattaché au département d'État et a pour mission de coordonner les efforts du gouvernement dans la lutte contre la désinformation.

La migration est un thème récurrent de désinformation, et les flux migratoires peuvent être instrumentalisés dans les conflits hybrides. En conséquence, la Commission européenne a proposé en 2021 une réglementation pour les situations où un pays tiers déclenche des mouvements migratoires irréguliers vers l'UE dans le but de déstabiliser celle-ci ou l'un de ses pays membres[27].

Plusieurs États ont renforcé leur communication stratégique afin de contrer les activités d'influence dans l'espace de l'information, notamment au sein de l'OTAN. Il s'agit d'un ensemble d'activités de communication coordonnées permettant aux États de transmettre et de légitimer leurs propres objectifs, intérêts et actions pour combattre les récits adverses. L'UE a créé, au sein du SEAE, un organe chargé de la communication stratégique. L'OTAN reçoit quant à elle le soutien d'une instance indépendante, le Centre d'excellence pour la communication stratégique.

4. En Suisse

4.1 Menaces

La Suisse se fonde sur un système de démocratie directe qui permet à la population de participer régulièrement aux décisions politiques, présente de potentielles lignes de fracture sociales et politiques, a une politique étrangère active et est le siège de nombreuses organisations internationales. Pour toutes ces raisons, des groupes d'influence peuvent considérer notre pays comme une cible de choix. État européen partageant les valeurs occidentales et fortement interconnecté à l'international sur les plans tant économique que politique, la Suisse est depuis longtemps une cible indirecte des activités d'influence dirigées contre les États occidentaux en général. De plus en plus, elle devient toutefois aussi une cible directe. Néanmoins, à ce jour, rien n'indique que des activités d'influence ont visé directement des votations ou des élections dans le pays.

On présume que la Russie et la Chine sont les deux pays qui cherchent à exercer le plus d'activités d'influence visant la Suisse[28]. Depuis que celle-ci applique les sanctions contre la Russie consécutives à la guerre en Ukraine, le Kremlin l'a inscrite sur sa liste des pays hostiles et a multiplié les activités de désinformation à son encontre, comme récemment dans le contexte de la Conférence de haut niveau sur la paix en Ukraine que la Suisse organise en juin 2024. Même si les médias russes diffusés à l'étranger ne gèrent pas de plateforme spécifique à la Suisse, les contenus qu'ils produisent en plusieurs langues peuvent atteindre la population de notre pays ; mais le Conseil fédéral estime que leur portée est réduite. Il n'est pas impossible que les activités d'influence russes s'intensifient si des débats politiques ou un processus politique en Suisse, comme une votation populaire, revêtaient un intérêt particulier pour la Russie. Ce risque peut concerner aussi les débats sur l'approvisionnement énergétique, la neutralité, les sanctions, le soutien à l'Ukraine ou l'utilisation éventuelle des avoirs gelés de la banque centrale russe.

En Suisse, les milieux politiques, les médias et la société en général perçoivent la désinformation et les activités d'influence et débattent de plus en plus de ce thème. La population suisse y est confrontée et en a conscience. L'enquête sur l'utilisation d'internet réalisée en 2021 par l'Office fédéral de la statistique (OFS) montre que près de la moitié de la population (45 %) déclare avoir vu des informations douteuses sur des sites d'information ou sur les réseaux sociaux. Cela signifie néanmoins

[27] Il s'agit d'un élément particulièrement pertinent dans le contexte où le Bélarus a encouragé la migration irrégulière vers la Pologne et la Lituanie à l'automne 2021. Commission européenne, Direction générale de la migration et des affaires intérieures, Proposition de règlement du Parlement européen et du Conseil visant à faire face aux situations d'instrumentalisation dans le domaine de la migration et de l'asile, 2021/0427/COD, <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52021PC0890> (version allemande consultée le 5 mars 2024).

[28] Rapport de 2021 sur la politique de sécurité du Conseil fédéral, FF 2021 2895, et rapport complémentaire de septembre 2022, FF 2022 2357.

que plus de la moitié des utilisateurs estime donc ne pas avoir vu de tels contenus ou qu'ils ne les ont pas identifiés comme tels. Selon le rapport « La désinformation en Suisse en 2021 »[29] mandaté par l'Office fédéral de la communication (OFCOM), près de la moitié des personnes interrogées considèrent la désinformation comme un problème sérieux ou grave. Selon le rapport, la désinformation constitue un problème majeur pour la cohésion sociale et pour la confiance dans les médias, les milieux politiques et les autorités. Il est difficile d'évaluer la mesure dans laquelle des activités d'influence ont déjà produit de tels effets. Les conséquences négatives sur la société, à travers sa polarisation, sur l'ordre international fondé sur des règles et sur la promotion internationale de la paix (cf. 2.3) touchent aussi les intérêts politiques et économiques de la Suisse.

Les opérations d'influence dirigées contre la Suisse représentent une menace en particulier pour sa place sur la scène politique internationale et comme siège de nombreuses organisations internationales. Le droit suisse des associations et des fondations accorde un rôle important à l'autocontrôle, ce qui pourrait augmenter le risque que le financement de certaines activités d'influence passe par la Suisse. Ainsi, Vladimir Yakounine, qui fait partie du cercle restreint des proches de Vladimir Poutine, a financé son forum *Dialogue entre civilisations*, qui mène des activités d'influence et de lobbying, à travers un réseau de fondations en Suisse. Des instituts prétendument scientifiques ou des portails internet critiques à l'égard des médias s'établissent en Suisse dans l'espoir d'obtenir une crédibilité en raison de leur localisation.

4.2 Exemples de désinformation

Deux exemples connus illustrent le contenu, le récit et le déroulement des activités d'influence et la manière dont elles peuvent toucher la Suisse. Le premier concerne le laboratoire de Spiez en 2018 et le second une fausse affiche sur les risques de pénurie d'énergie qui a circulé en 2022. Ces deux cas montrent comment des campagnes d'envergure, menées à l'échelle européenne, ciblent aussi la Suisse.

Première situation : en mars 2018, après que des agents russes ont empoisonné l'ancien espion russe Sergueï Skripal et sa fille au Royaume-Uni avec du Novitchok, le laboratoire de Spiez s'est retrouvé sous les feux de l'actualité mondiale pour avoir, avec d'autres laboratoires, analysé des échantillons relatifs à cet incident à la demande de l'Organisation pour l'interdiction des armes chimiques (OIAC). Des acteurs russes – étatiques, mandatés par l'État et non étatiques – ont tenté de saper la crédibilité du laboratoire et de ses analyses sur les médias sociaux et sur des médias sous contrôle de l'État, en attribuant la responsabilité de cet empoisonnement à d'autres acteurs. Le ministre russe des Affaires étrangères Sergueï Lavrov a prétendu que le laboratoire de Spiez n'avait pas identifié de Novitchok dans les échantillons. De nombreux médias occidentaux ont rapporté ces déclarations. Le Conseil fédéral et le laboratoire de Spiez ont réfuté ces allégations avec fermeté. Des usines à trolls russes comme l'*Internet Research Agency* ont participé à la diffusion de cette fausse information sur des médias sociaux comme X/Twitter et Facebook. Deux ressortissants russes arrêtés aux Pays-Bas ont été accusés de tentative d'espionnage contre le laboratoire de Spiez. Les actions russes contre ce dernier et l'OIAC visaient en premier lieu à détourner l'attention du rôle de la Russie, mais cherchaient aussi à nuire à la réputation du laboratoire de Spiez et donc de la Suisse.

Deuxième exemple : une fausse affiche publicitaire de la Confédération, diffusée sur les réseaux sociaux X/Twitter et Telegram en automne 2022, signalait une récompense de 200 francs pour toute dénonciation de voisins abusant du chauffage. Au moment de la parution de ce photomontage, la Suisse était en plein débat sur la menace d'une pénurie d'énergie entraînée par la guerre en Ukraine. Le 6 septembre 2022, quatre jours avant la première publication de la fausse affiche, un quotidien suisse a publié un article sur des propositions d'ordonnances prévoyant des amendes ou des peines de privation de liberté pour les personnes chauffant à plus de 19 degrés. Des médias internationaux, dont la chaîne russe RT en allemand, ont repris cette information le jour même. Dans les heures qui ont suivi sa publication sur internet, le photomontage s'est propagé rapidement sur différents médias sociaux et plateformes en ligne, y compris à travers de faux comptes sous influence russe.

[29] Vogler, D., Schwaiger, L., Schneider, J., Udris, L., Siegen, D., Marschlich, S., Rauchfleisch, A., Eisenegger, M. (2021). Fausses informations, médias alternatifs et théories du complot - Comment la population suisse gère la désinformation. Rapport pour l'Office fédéral de la communication.

Le récit ainsi véhiculé sous-entendait une dérive autocratique et un dysfonctionnement du système démocratique et de l'État de droit en Suisse. Il s'agissait de créer un sentiment d'insécurité et de diviser la population. Sans compter que cette affaire a mobilisé les ressources de différentes autorités. Plus de 80 personnes ont appelé le secrétariat général du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), dont le numéro de téléphone figurait sur la fausse affiche, pour donner suite au présumé appel à la dénonciation. Toutefois, cette perturbation ponctuelle de l'administration fédérale n'a pas eu de conséquences graves et cette action n'a pas atteint une masse critique au sein de la société.

4.3 Caractéristiques et résilience de la Suisse

La Suisse présente certaines spécificités qui tendent à limiter son exposition aux activités d'influence et de désinformation. Il faut néanmoins nuancer le tableau.

La taille réduite du pays et de son paysage médiatique, le niveau de vie élevé, le bon niveau d'instruction, la confiance élevée – et même supérieure à la moyenne – dans les institutions étatiques et les compétences politiques, en lien notamment avec la fréquence des votations populaires, contribuent à renforcer la capacité de résilience du pays et de ses institutions. Selon le rapport « La désinformation en Suisse en 2021 », qui mentionne diverses études comparatives, la Suisse est un pays dont les structures sont plus robustes que beaucoup d'autres. Cette résilience s'explique et se traduit notamment par une société peu polarisée et un paysage médiatique comprenant de nombreux médias de qualité. L'interaction entre médias privés et publics, le multipartisme et la culture du consensus politique contribuent à accroître, en comparaison internationale, la capacité de la Suisse à résister aux dérives sur internet, comme la polarisation et le populisme[30]. Une autre étude montre que notre pays est moins touché en comparaison européenne par les *fake news* du fait de sa moindre importance géopolitique et de sa diversité linguistique[31].

Toutefois, la démocratie directe et le fédéralisme suisse ne sont pas que des atouts face à la désinformation : ils peuvent constituer aussi une vulnérabilité. Car le nombre de scrutins à tous les niveaux multiplie les possibilités d'exercer une influence. Heureusement, les autorités chargées de l'organisation des élections et des votations aux différents échelons de l'État ont acquis, à force, un véritable savoir-faire. Elles coopèrent étroitement en échangeant régulièrement leurs expériences sous différentes formes institutionnalisées[32], au sein d'organes spécifiques[33] et à l'échelle internationale[34]. Les études VOX réalisées par l'institut de sondage gfs.bern montrent la confiance de la population dans les informations fournies par le Conseil fédéral, notamment lors des votations, comme dans la brochure explicative du Conseil fédéral (83 %), mais aussi dans des articles de presse (81 %) et lors d'émissions télévisées (72 %).

Les dispositions relatives à la transparence, entrées en vigueur en 2022, interdisent aux acteurs politiques de recevoir des libéralités anonymes ou provenant de l'étranger (cf. art. *76h* de la loi fédérale sur les droits politiques). Cette interdiction offre également une certaine protection contre des activités d'influence dans l'espace de l'information.

En dehors de ces facteurs structurels, si l'on aborde la thématique des activités d'influence au niveau individuel, différents indices laissent penser que la résilience de la population suisse en matière de désinformation pourrait s'amenuiser à l'avenir. Certes, la population dispose d'un niveau relativement élevé en instruction civique. Une étude révèle toutefois que les personnes interrogées en Suisse ont des compétences médiatiques plutôt faibles, légèrement inférieures à celles d'une étude comparative en Allemagne. Par exemple, de nombreux répondants ont eu du mal à déterminer les intentions de

---

[30] Selon Tobias Keller, spécialiste de la communication et des médias à l'institut de recherche gfs.bern, qui a collaboré à l'étude Numérisation de la démocratie suisse, Urs Bieri et al. : Numérisation de la démocratie suisse. La révolution technologique se heurte au système traditionnel de formation de l'opinion, Zurich, 2021.
[31] Humprecht, Edda, et al.: Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. In: International Journal of Press/Politics, tome 25, 2020, p. 493-516.
[32] Conférence suisse des chanceliers d'État.
[33] Comme la rencontre annuelle organisée depuis 2012 par la Chancellerie fédérale qui réunit des responsables de votations et d'élections de la Confédération et des cantons.
[34] Cf. Élections en temps de crise : Conférence du Conseil de l'Europe à Berne, https://www.parlament.ch/fr/services/suche-news/elections-en-temps-en-crise (version allemande consultée le 27 février 2024) / Conférence parlementaire – Les élections en temps de crise (Berne, 9-10 mai 2023) <https://pace.coe.int/fr/pages/bern-elections-conference> (version allemande consultée le 27 février 2024).

communication (en tant qu'information, commentaire ou publicité) d'un contenu médiatique, une aptitude pourtant essentielle pour évaluer la désinformation. Ils ont été 73 % à déclarer être dépassés, en partie ou complètement, par la masse d'informations à disposition[35]. Les individus qui affichent un degré d'intérêt plus élevé pour les informations et la participation politique, qui utilisent des médias *tant* numériques *que* traditionnels, et qui ont confiance dans les médias suisses en général disposent de meilleures compétences médiatiques et tendent donc à faire preuve de davantage de résilience face aux activités d'influence. Les personnes d'un certain âge constituent un groupe particulièrement vulnérable à la désinformation, car leur capacité à s'informer de manière éclairée est plus faible que celle des autres tranches d'âge, indépendamment de leur niveau de formation[36].

Selon les dernières données disponibles, la population suisse s'attribue néanmoins des compétences numériques légèrement supérieures à la moyenne internationale. Selon l'enquête Omnibus 2021 sur l'utilisation d'internet[37], ses propres évaluations la placent dans le tiers supérieur en comparaison internationale : près de 78 % de la population mentionnent des compétences de base ou plus que basiques[38]. Il y a ainsi un décalage entre l'auto-évaluation et le niveau réel de compétence.

En Suisse, le nombre de personnes qui ne consomment pas d'émissions d'information traditionnelles est en hausse[39]. En 2023, seuls 22 % des 18-24 ans déclaraient s'informer directement sur le site web d'un éditeur de presse ou à travers son application, alors qu'ils étaient encore 53 % en 2015. Les autres jeunes de cette tranche d'âge voient passer des informations sur les réseaux sociaux. Parmi les 15-29 ans, 40 % s'informent principalement à travers les médias sociaux et 25 % à travers les médias en ligne[40]. La ligne éditoriale des médias en ligne fait l'objet d'une modération moindre que celle des médias traditionnels. Quant aux médias sociaux, ils ne sont presque pas modérés. Les utilisateurs peuvent plus facilement y prendre de fausses informations pour des faits vérifiés. S'y ajoute une certaine affinité pour les récits conspirationnistes et idéologiques, qui peut pousser les utilisateurs à considérer comme vrais des contenus de désinformation qui s'accordent avec leurs convictions déjà bien ancrées, puis à les diffuser[41]. Avec les développements technologiques, et notamment l'IA, la désinformation devient de plus en plus difficile à détecter (cf. 2.2). Une autre enquête constate que la vérification des fausses informations est relativement bien établie dans la société, notamment le réflexe de consulter d'autres sources et de vérifier l'expéditeur, que ce soit sur des sites des autorités et de l'État (68 %), sur des sites de médias (61 %), mais aussi sur Google (45 %) et à travers des échanges avec des proches (43 %)[42]. Il n'y a pas vraiment de site dédié à la vérification des faits dans le contexte suisse.

---

[35] Jan Fivaz, Daniel Schwarz, Die Medienkompetenz der Schweizer Bevölkerung (*Les compétences de la population suisse en matière de médias*, rapport en allemand uniquement, avec questionnaire en français). https://arbor.bfh.ch/19556/1/Bericht. Eine repräsentative Pilotstudie für die deutsch- und französischsprachige Schweiz, 2022, p. 15, 49-51, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/schlussbericht-die-edienkompetenz-derschweizer-bevoelkerung.pdf.download.pdf/Bericht%20Medienkompetenz%202022%202.pdf> (consulté le 4 mars 2024).
[36] Ibid., p. 6, 19-20.
[37] Office fédéral de la statistique, Omnibus 2021 : enquête sur l'utilisation d'Internet, fiche signalétique <https://dam-api.bfs.admin.ch/hub/api/dam/assets/22284439/master> (version allemande consultée le 4 mars 2024)
[38] Office fédéral de la statistique, Compétences numériques générales de la population, comparaison internationale <https://www.bfs.admin.ch/asset/fr/22404710> (version allemande consultée le 4 mars 2024).
[39] Forschungszentrum Öffentlichkeit und Gesellschaft der Université Zürich, Jahrbuch Qualität der Medien 2022 (*Université de Zurich, centre de recherche sur la sphère publique et la société, annales sur la qualité des médias*, site en allemand ou en anglais seulement), <https://www.foeg.uzh.ch/en.html> (consulté le 27 février 2024).
[40] Étude Reuters sur la transformation des médias, publiée en 2023 avec l'Université d'Oxford ; Stefan Thommen et al., Monitoring Médias Suisse 2022, enquête de Publicom, p. 50-52, <https://www.monitoring-medias-suisse.ch/uploads/media/default/0001/02/MMS_2022_Recapitulatif.pdf (récapitulatif en français)> (version allemande consultée le 27 février 2024).
[41] Centre de recherche sur la sphère publique et la société de l'université de Zurich, Falschinformationen, Alternativmedien und Verschwörungstheorien – Wie die Schweizer Bevölkerung mit Desinformation umgeht, 2021 (*Fausses informations, médias alternatifs et théories du complot – Comment la population suisse gère la désinformation*, en allemand seulement) <https://www.foeg.uzh.ch/dam/jcr:96eb88c7-f0a2-4fc8-8fc2-6591e39195fa/Studie_01_2021.pdf> (consulté le 27 février 2024).
[42] Vogler et al., Fausses informations, médias alternatifs et théories du complot, p. 31 (en allemand seulement, cf. note précédente).

En ce qui concerne la confiance dans les médias, les enquêtes Eurobaromètre attribuent à la Suisse des valeurs supérieures à la moyenne ; celle du printemps 2023 a constaté que 53 % de la population faisait confiance aux médias (chiffre inchangé par rapport à 2021), alors que la moyenne européenne est de 36 %[43]. Les médias classiques (72 à 82 %) bénéficient d'une confiance nettement plus grande que les sources sur internet (29 %) et surtout que les plateformes numériques (10 %)[44]. Une autre enquête indique une certaine érosion avec une confiance générale dans les médias suisses passée de 50 % en 2016 à 42 % en 2023[45].

4.4 Perspectives

À l'ère où la politique de puissance est en pleine expansion dans le monde, il apparaît fort probable que certains acteurs étatiques ou mandatés par des États déploient davantage d'activités d'influence et de désinformation ces prochaines années en utilisant des moyens technologiques d'avant-garde pour tenter de déstabiliser les sociétés occidentales. Nul doute que certaines de ces activités viseront aussi la Suisse. Du fait de sa petite taille, de sa démocratie directe, de son haut niveau d'éducation et de la confiance dont y bénéficient les institutions politiques et les médias, notre pays a des institutions relativement robustes face à la menace. Mais, comme le montrent les enquêtes sur les compétences en matière de médias et d'information, les nouvelles habitudes de consommation des médias et les développements technologiques augmentent les défis liés à la gestion des activités d'influence et de désinformation en Suisse aussi.

L'IA élargit le cercle des acteurs susceptibles de fabriquer et de diffuser habilement de la désinformation, sans grand effort de leur part. Au fur et à mesure que les algorithmes sous-jacents de l'IA se développeront et se perfectionneront, ils devraient s'adapter de mieux en mieux à leur public cible, gagner en crédibilité, et donc maximiser leur impact. Mais l'IA offre également des possibilités d'améliorer la régulation et la vérification des faits et de mettre au jour des activités d'influence et de désinformation. Ces évolutions sont fortement influencées par de grandes entreprises technologiques qui introduisent de nouvelles technologies et prennent des initiatives d'autorégulation. Les efforts de régulation de grands États comme les États-Unis ou d'espaces économiques comme l'UE devraient aussi s'intensifier et ne manqueront pas d'avoir une incidence sur la Suisse, qui pourra en outre les reprendre ou s'en servir comme modèles.

5. Bases légales suisses

On trouve les principales dispositions concernant la gestion des activités d'influence dans différents textes juridiques, notamment ceux relatifs aux droits politiques et aux médias, à la loi sur le renseignement, aux organes chargés de la politique de sécurité, au droit pénal et aux tâches de la police.

La garantie des droits politiques dans la Constitution protège la libre formation de l'opinion (cf. art. 34, al. 2, Cst.[46]). La diffusion de fausses informations relève en principe de la protection de la liberté d'opinion en vertu de l'art. 16 Cst. et de l'art. 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, et, selon les contextes, de la liberté des médias au sens de l'art. 17 Cst. Dans sa jurisprudence, le Tribunal fédéral défend le postulat de base selon lequel les individus doivent pouvoir entendre chaque opinion et chaque information pour pouvoir se forger leur

[43] Commission européenne, Eurobaromètre standard, L'opinion publique dans l'Union européenne, mai-juin 2023, p. 74, <https://op.europa.eu/fr/publication-detail/-/publication/12241d9a-836b-11ee-99ba-01aa75ed71a1/language-fr> (version allemande consultée le 4 mars 2024).
[44] Commission européenne, Eurobaromètre standard, L'opinion publique dans l'Union européenne, janvier-février 2022, p. 46 ss <https://op.europa.eu/fr/publication-detail/-/publication/1635332d-2d8c-11ed-975d-01aa75ed71a1/language-fr> (version allemande consultée le 4 mars 2024).
[45] Nic Newman et al., Reuters Institute, Digital News Report 2023, p. 103, <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf> (consulté le 5 mars 2024).
[46] RS **101**

propre opinion grâce à la circulation de la parole[47]. La robustesse du système d'information institutionnel est essentielle pour prévenir et endiguer les éventuelles activités d'influence et de désinformation. La politique d'information du Conseil fédéral se fonde notamment sur l'art. 180 Cst., l'art. 10 de la loi sur l'organisation du gouvernement et de l'administration, l'art. 10*a* de la loi fédérale sur les droits politiques et sur les lignes directrices de la Conférence des services d'information de la Confédération.

Selon les règles générales énumérées à l'art. 36 Cst. (base légale, intérêt public, protection d'un droit fondamental d'autrui, restriction proportionnée), la liberté d'*expression* peut être restreinte, notamment par les droits de la personnalité, pour éviter diffamation et calomnie. Des restrictions légales à la désinformation existent également en vertu de la protection de la sécurité et de l'ordre publics[48]. Certains actes commis dans l'espace de l'information peuvent en outre être qualifiés d'atteinte à l'ordre constitutionnel (art. 275 du code pénal [CP]).

Des règles spéciales s'appliquent aux domaines particulièrement sensibles de la formation de l'opinion, comme des émissions de radio ou de télévision ayant un contenu informatif, qui obéissent au principe d'objectivité (art. 4, al. 2, de la loi fédérale sur la radio et la télévision [LRTV][49]). Tout contenu manipulé empêchant le public de se forger sa propre opinion bafoue ce principe. Toute personne peut saisir l'organe de médiation de la radio et de la télévision et, sur rapport de celui-ci, déposer une plainte auprès l'Autorité indépendante d'examen des plaintes en matière de radio-télévision (art. 91 à 98 LRTV). La surveillance des contenus publicitaires incombe à l'OFCOM. D'une manière générale, les émissions de radio et de télévision ne doivent pas, en vertu de l'art. 4, al. 3, LRTV, nuire à la sûreté intérieure ou extérieure de la Confédération ou des cantons ni à leur ordre constitutionnel. Cette disposition s'applique également à la publicité, même si aucun cas concret ne s'est encore présenté[50]. Il n'existe pas encore de réglementation légale spécifique aux intermédiaires, mais celle-ci est en cours d'élaboration.

La loi sur le renseignement (LRens) définit les compétences du Service de renseignement de la Confédération (SRC) en matière d'activités d'influence. Le SRC peut ainsi suivre des activités d'influence à l'étranger dans la mesure où celles-ci affectent la politique de sécurité. Il est davantage limité en ce qui concerne les activités d'influence se produisant dans le pays. Seules les menaces pour la sûreté en lien avec le terrorisme, l'espionnage, la dissémination d'armes ou leur commerce illégal, les attaques contre des infrastructures critiques et l'extrémisme violent (art. 6, al. 1, let. a, ch. 1 à 5, LRens) peuvent faire l'objet d'une prévention de sa part. Le SRC n'est en principe pas autorisé à rechercher ni à traiter des informations relatives aux activités politiques ou à l'exercice de la liberté d'opinion, d'association ou de réunion en Suisse (art. 5, al. 5, LRens).

Les activités d'influence et la désinformation peuvent, selon leur ampleur, relever de la police et, selon le délit, donner lieu à des procédures pénales cantonales ou fédérales. Il peut s'agir de crimes et de délits contre la paix publique (art. 258 ss CP), comme des menaces alarmant la population (art. 258 CP), mais aussi de l'utilisation frauduleuse d'un système de traitement de données (art. 147 CP) et de la discrimination et de l'incitation à la haine (art. 261bis CP).

---

[47] Cf. ATF 135 I 292, cons. 4.1, p. 296 (arrêt disponible en allemand uniquement, regeste en français) ; dans sa jurisprudence relative à l'art. 261*bis* du Code pénal (CP), le Tribunal fédéral a en outre retenu que « *dans les débats publics, il n'est souvent pas possible de savoir d'emblée avec certitude si une critique est fausse, à moitié fausse ou justifiée* » (traduction libre d'après l'arrêt disponible en allemand uniquement ATF 131 IV 23, cons. 3.1, p. 28, regeste en français) ; Schefer Markus, Kommunikationsgrundrechte (texte en allemand uniquement, traduction libre : *Droits fondamentaux de la communication*), in : Diggelmann Oliver et al. (éditions), Droit constitutionnel suisse, tome II, 2020, p. 1413-1452, ch. 89 ; Raphaela Cueni, Informations fausses ou trompeuses dans le droit constitutionnel suisse (texte en allemand, résumé en français), ex/ante vol. 2019, nº 1, 3, p. 12

[48] Cf. Tribunal fédéral 1P.336/2005 (arrêt du 20 septembre 2005), consid. 5.3 ; Cour européenne des droits de l'homme (CEDH), Mouvement raëlien suisse contre la Suisse (arrêt du 13 juillet 2012), requête nº 16354/06.

[49] RS **748.40**

[50] Son activité de surveillance pourrait permettre à l'OFCOM de prendre des mesures à l'encontre d'un diffuseur qui propagerait de la désinformation à travers sa publicité en nuisant à la sûreté intérieure ou extérieure de la Confédération ou des cantons. La procédure de surveillance ne vise que les diffuseurs suisses aux conditions prévues à l'art. 89, al. 1, LRTV. Les circonstances concrètes sont censées permettre d'estimer le moment où le risque devient effectif. L'autonomie des diffuseurs en matière de programmation incite à ne pas prendre cette menace à la légère.

L'Office fédéral de la police (fedpol) peut saisir, par mesure policière de prévention, du matériel pouvant servir à des fins de propagande et dont le contenu incite de manière forte et concrète à la violence contre des personnes ou des objets. En cas de soupçon d'un acte punissable, l'autorité chargée de la saisie transmet le matériel à l'autorité pénale compétente (art. 13*e* de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure [LMSI][51]). En cas de diffusion de propagande incitant à la violence par le biais d'internet, fedpol peut, après consultation du SRC, ordonner la suppression du site concerné si le matériel se trouve sur un serveur suisse ou recommander au fournisseur d'accès suisse de bloquer un site étranger. Si des organisations criminelles exercent des activités d'influence et de désinformation, fedpol peut, en vertu de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)[52], conduire de manière autonome des enquêtes de police préliminaires et coordonner également les investigations menées aux échelons intercantonal ou international. Cette qualification de fedpol a tout son sens pour faire face, par exemple, aux acteurs étatiques russes qui instrumentalisent des organisations criminelles à leurs propres fins.

Quand une personne de nationalité étrangère menace la sûreté intérieure ou extérieure de la Suisse par ses activités d'influence (art. 67, al. 4, et art. 68 de la loi sur les étrangers et l'intégration [LEI][53]), fedpol peut prononcer contre elle une interdiction d'entrée dans le pays ou un renvoi. En outre, il prend des mesures de protection lorsque la désinformation touche des personnalités protégées par la Confédération (comme les conseillers fédéraux) ou nécessite de davantage sécuriser les bâtiments fédéraux. Ainsi, dans le cas de la fausse affiche sur les risques de pénurie énergétique (cf. 4.2), fedpol a ouvert une enquête pour atteinte aux emblèmes suisses de souveraineté (art. 270 CP).

Dans ce même contexte, d'autres délits graves relèvent de la compétence fédérale : atteinte à l'indépendance de la Confédération (art. 266 CP), entreprises menées de l'étranger contre la sécurité de la Suisse (art. 266bis CP), actes exécutés sans droit pour un État étranger (art. 271 CP), espionnage (art. 272 ss CP), délits contre la volonté populaire (art. 279 ss CP ; art. 23, al. 1, let. h, du code de procédure pénale suisse [CPP][54]) et violence ou menace contre les autorités et les fonctionnaires (art. 285 CP).

6. Compétences et mesures prises jusqu'à présent en Suisse

Dans son rapport de 2021 sur la politique de sécurité, le Conseil fédéral constate qu'il est de plus en plus probable que la Suisse devienne la cible de tentatives d'influence et de désinformation. Dans sa lutte, il vise à renforcer l'observation de la situation et l'intervention précoce (6.1), la résilience du pays et de sa population dans un but de prévention (6.2), la réglementation et les sanctions (6.3), la communication et l'accès aux informations des autorités (6.4), la coordination interne et externe et les échanges (6.5).

6.1 Observation de la situation et intervention précoce

Pour l'instant, il n'existe aucune structure en Suisse susceptible de détecter systématiquement les influences dans l'espace de l'information, d'en déterminer les intentions et la paternité et, le cas échéant, d'y réagir.

Les organes de coordination de la politique de sécurité de la Confédération, notamment la Délégation du Conseil fédéral pour la sécurité (Délséc) et le Groupe sécurité (GS), présidés par le DDPS, ont pour tâche d'évaluer la situation et de coordonner les affaires interdépartementales en matière de politique de sécurité[55]. Ils se sont d'ailleurs penchés à plusieurs reprises sur le sujet. Le GS peut soumettre à la Délséc les propositions issues de ses délibérations.

---

[51] RS **120**
[52] RS **360**
[53] RS **142.20**
[54] RS **312.0**
[55] Selon les directives du Conseil fédéral du 25 janvier 2023, basées sur l'art. 30 de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). La Délséc est composée des chefs du DDPS, du DFJP et du DFAE, accompagnés de leurs secrétaires généraux, des secrétaires d'État du DFAE et du SEPOS, des directeurs du SRC et de fedpol, et du vice-chancelier.

Le SRC est très limité en ce qui concerne les informations sur les activités d'influence qu'il peut collecter, examiner ou traiter à l'intérieur du pays. Quant aux activités d'influence à l'étranger qui affectent la politique de sécurité, il peut s'occuper des plus graves, en se concentrant sur les menaces directes, concrètes ou potentielles que les rivalités entre grandes puissances font peser sur la Suisse. Parmi les activités d'influence en lien avec des conflits hybrides, le SRC explore en particulier celles qui viennent de Russie et de Chine. Ses recherches portent sur des acteurs et des activités à l'étranger qui cherchent à saper la libre formation de la volonté politique en Suisse ou dans son environnement stratégique, et sur des acteurs et des activités en Suisse qui ont des liens avec le terrorisme, l'espionnage, la dissémination d'armes, des attaques contre des infrastructures critiques ou l'extrémisme violent.

Les départements, les offices fédéraux et la Chancellerie fédérale effectuent un monitoring général et permanent des médias. Au Département fédéral des affaires étrangères (DFAE), Présence Suisse observe la diffusion de comptes rendus sur la Suisse dans les médias étrangers et fournit un rapport régulier à ce sujet. La Chancellerie fédérale et les cantons procèdent à des évaluations des risques en vue d'utiliser le vote électronique lors des scrutins fédéraux, qui portent aussi sur d'éventuelles attaques de désinformation.

L'OFCOM veille au respect de la LRTV, des concessions et dispositions d'exécution. Il vérifie que la Société suisse de radiodiffusion et télévision (SSR) et les diffuseurs privés remplissent leurs mandats de prestations en matière de services journalistiques, au moyen notamment d'analyses quantitatives des programmes réalisées périodiquement par des instituts de recherche. La Chancellerie fédérale et la plupart des départements et offices fédéraux réalisent également, à des degrés divers, des monitorings médias portant sur des thèmes précis ou des offices en particulier.

Il est nécessaire de suivre les évolutions technologiques pour dresser un état des lieux des activités d'influence. Le campus cyberdéfense et armasuisse Sciences et technologies travaillent sur différents projets de recherche portant sur des aspects technologiques des activités d'influence et de la cyberdéfense, en collaboration avec certaines hautes écoles suisses. À titre d'exemple, un projet de recherche réalisé avec la Haute école spécialisée du Nord-Ouest de la Suisse analyse le potentiel de menace des images générées par l'IA. La recherche dans le domaine de la science des données contribue de manière significative à la détection des bulles de filtres et à la plausibilisation des tendances sur les réseaux sociaux. Le campus cyberdéfense s'en occupe, mais sa recherche est limitée en partie par le cadre juridique posé par armasuisse Sciences et Technologie. Ainsi, il n'est pas autorisé à utiliser dans des travaux de recherche les données provenant des médias sociaux, même en les anonymisant.

La désinformation peut influencer les militaires avant même leur entrée en service ou pendant une mission. L'armée observe donc l'espace de l'information au quotidien, en particulier pendant les engagements et les opérations, en essayant de protéger les militaires et les prestations de base de l'armée contre toute action. Les enseignements correspondants sont intégrés au rapport de situation hebdomadaire du commandement des Opérations. Le domaine CyMon *(Cyber-Monitoring*), une unité du commandement Cyber, analyse les informations provenant des sites web et des médias sociaux. Il procède à l'évaluation préalable des données correspondantes et contribue ainsi à la détection des activités d'influence contre la Suisse qui n'impliquent aucune participation suisse. La loi sur l'armée l'autorise à le faire au profit de l'armée et du Renseignement militaire, si ces informations sont pertinentes pour l'armée, ou au profit du SRC sur mandat de ce dernier et sur la base de la LRens.

L'administration fédérale travaille avec des tiers, notamment des chercheurs, pour déterminer l'exposition de la Suisse aux activités d'influence et de désinformation. Le rapport de l'Université de Zurich sur la désinformation en Suisse (2021), mandaté par l'OFCOM[56], constitue l'étude la plus complète sur le sujet. L'OFCOM a compilé les ouvrages disponibles sur la désinformation pour lancer la recherche scientifique dans ce domaine en Suisse en se concentrant sur les contenus, le comportement de réception, les caractéristiques des publics et les approches en matière de gouvernance. Les activités d'influence relèvent de cette recherche, qui est toutefois plus large et ne se concentre pas spécifiquement sur la désinformation d'État[57].

---

[56] Vogler et al., Fausses informations, médias alternatifs et théories du complot (en allemand seulement, cf. note 36).
[57] Pour certaines conclusions de ces études, cf. points 3.1 et 3.3.

6.2 Résilience par la sensibilisation, la formation et la compétence médiatique

La résilience et la prévention comprennent la sensibilisation au phénomène, à son ampleur, à ses conséquences possibles et à l'exposition de la Suisse. Les groupes cibles des activités correspondantes sont le personnel fédéral (y c. les représentations à l'étranger), les autorités cantonales, la population, les acteurs politiques (p. ex. les partis) et les professionnels des médias.

Concrètement, des participants de la Confédération et des cantons ont été sensibilisés à cette thématique lors de l'exercice du Réseau national de sécurité de 2019. Ils se sont exercés à réagir à des activités d'influence et de désinformation lors d'un événement de crise majeure. Sur le thème global de la menace terroriste, les simulations ont porté sur la manière dont les menaces politiques, la propagande et la désinformation pouvaient donner un sentiment d'insécurité aux autorités et à la population, y compris à travers des cyberattaques contre des portails d'information de la Confédération et des cantons et à travers la manipulation ciblée des médias. Le groupe terroriste menant l'action était certes fictif, mais des acteurs étatiques sont susceptibles de tels agissements dans l'espace de l'information, posant des défis comparables.

Dans la perspective des élections au Conseil national de 2019 et de 2023, la Chancellerie fédérale a invité les partis, les grandes plateformes, le Centre national de cybersécurité (NCSC, qui est devenu depuis l'Office fédéral de la cybersécurité [OFCS]) et le préposé fédéral à la protection des données à une rencontre consacrée aux campagnes politiques dans l'espace numérique. Les discussions ont porté sur la menace que les activités d'influence représentent et sur les mesures de protection possibles. En outre, des accès privilégiés ont été négociés avec Google, Meta et Tiktok avant les élections au Conseil national. En cas de manipulations, des contacts directs étaient prévus pour mettre en avant les informations officielles sur ces plateformes.

Des médias de qualité appliquant des normes journalistiques de haut niveau et disposant d'un public intéressé et critique, comme c'est le cas en Suisse d'une manière générale, contribuent à limiter l'impact des activités d'influence. En réponse au postulat Christ 21.3781 « Réfléchir dès aujourd'hui à la stratégie d'aide aux médias de demain », le Conseil fédéral a présenté dans un rapport différents modèles et options de financement pour encourager les médias qui peuvent être mis en œuvre indépendamment des canaux de diffusion. Pour encourager la formation et le perfectionnement des journalistes, l'OFCOM travaille à la mise en œuvre de l'initiative parlementaire Chassot 22.417 « Mesures d'aide en faveur des médias électroniques » pour soutenir les institutions qui proposent des formations et des perfectionnements aux collaborateurs de leur rédaction. En outre, l'OFCOM a adopté en 2023 un plan d'action national pour la sécurité des journalistes[58] en Suisse. Il s'agit notamment de mieux protéger les journalistes contre les menaces, les violences et les tentatives d'intimidation, qui sont toutes susceptibles d'être favorisées aussi par des activités d'influence.

La formation est un élément central de la résilience et de la prévention contre les activités d'influence et la désinformation. Elle est utile à tous les âges, de l'enfance à l'âge adulte en passant par l'adolescence. Par contre, il est beaucoup plus difficile d'atteindre les adultes d'un certain âge par des mesures de formation. L'école obligatoire relève de la compétence des cantons. Les plans d'études intègrent désormais l'instruction civique et l'éducation numérique comme disciplines à part entière[59]. L'objectif est de développer les capacités des jeunes à s'informer sur la vie politique et sociale et à y participer. Concrètement, les plans d'études cantonaux visent à transmettre des compétences techniques, de jugement, d'action et de méthode afin d'aborder les médias et les informations de manière critique et responsable. Les plans d'études cadres révisés concernant les cours de culture générale pour la formation professionnelle de base et la maturité professionnelle encouragent aussi une gestion critique de l'information et des médias. De même, les responsables de la formation professionnelle contribuent à la promotion des compétences numériques[60]. Une décision du Conseil

---

[58] <https://www.bakom.admin.ch/bakom/fr/page-daccueil/medias-electroniques/politique-des-medias/plan-action-national.html#:~:text=Le%20plan%20d%27action%20se,Une%20meilleure%20protection%20physique>.
[59] Département fédéral de l'économie, de la formation et de la recherche (DEFR), Conférence des directeurs cantonaux de l'instruction publique (CDIP), Valorisation optimale des chances. Déclaration 2023 sur les objectifs politiques communs concernant l'espace suisse de formation, 26 octobre 2023, <https://www.sbfi.admin.ch/dam/sbfi/fr/dokumente/2023/10/erklaerung-chancen-2023.pdf.download.pdf/erklaerung-chancen-2023_f.pdf> (version allemande consultée le 5 mars 2024).
[60] Selon les plans d'études cadres révisés pour les responsables de la formation professionnelle.

fédéral et de la Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP) datant de 2018 rend les cours d'informatique obligatoires dans toute la Suisse pour les élèves du secondaire II, à partir de l'année scolaire 2022-2023 au plus tard. Pour ce qui concerne les hautes écoles, la Confédération soutiendra probablement le programme *Open Education & Digital Competencies* à travers une contribution liée à des projets (20252028). Il s'agit d'encourager les enseignants à développer la culture numérique dans leur enseignement, en mettant l'accent sur la qualité des outils numériques, et d'encourager les étudiants à développer leurs compétences en matière d'évaluation des données numériques pour relever les défis de l'IA.

À travers leurs propres projets[61], les associations de médias, comme Médias Suisses, participent à accroître les compétences médiatiques (numériques) des adolescents. Le portail ch.ch, plateforme d'information de la Confédération, des cantons et des communes sur la vie en Suisse, explique à la population comment reconnaître la désinformation en ligne et comment y réagir. L'Office fédéral des assurances sociales gère la plateforme nationale Jeunes et médias visant à promouvoir les compétences médiatiques.

6.3 Réglementation et sanctions

En 2021, l'OFCOM a publié, avec la participation de la Chancellerie fédérale, le rapport « Intermédiaires et plateformes de communication. Effets sur la communication publique et approches de gouvernance », qui montre le potentiel et les effets positifs comme négatifs des plateformes sur la communication publique et se penche sur l'approche de l'UE pour une gouvernance en la matière[62]. Le 5 avril 2023, le Conseil fédéral a chargé le DETEC (OFCOM) d'élaborer un projet de consultation sur la réglementation des plateformes de communication. Le projet abordera notamment les défis posés par l'absence de régulation face aux plateformes numériques. S'inspirant du règlement de l'UE sur les services numériques, il vise à contraindre les très grandes plateformes à assumer leurs responsabilités en leur imposant des obligations de diligence et de transparence (à travers des rapports sur leurs activités de modération). Toutefois, la réglementation ne traite la désinformation qu'en ce qui concerne les contenus illicites.

La Suisse n'a notamment pas repris les sanctions que l'UE a imposées le 1er mars 2022 à RT et à Sputnik, d'importants portails de diffusion russes transnationaux proches de l'État russe. Même si ces canaux sont des outils de propagande et de désinformation russes ciblées, le Conseil fédéral estime plus efficace de contrer les propos mensongers et nuisibles par des faits plutôt que de les interdire. La portée de ces médias en Suisse est jugée faible par ailleurs.

6.4 Communication

Il convient de distinguer, d'une part, les moyens de communication visant à gérer des activités d'influence et de désinformation et à y réagir et, d'autre part, les informations régulières destinées à la population et aux acteurs politiques dans un but de prévention.

Une activité d'influence n'a pas besoin d'enfreindre le droit en vigueur pour être indésirable sur le plan politique. Le Conseil fédéral et l'administration fédérale peuvent rectifier des informations manifestement fausses ou trompeuses propagées auprès d'un large public (procédure de démystification, ou *debunking* en anglais), mais ils font un usage modéré de cette possibilité. Car la diffusion de fausses informations relève de la liberté d'expression, sauf pour les attaques qui tombent sous le coup du code pénal. Du fait de l'effet de vérité illusoire, qui consiste à croire dans la véracité d'une information, même fausse, après y avoir été exposé de manière répétée, la démystification peut même avoir un effet contreproductif. Il suffit que les rectifications des autorités soient perçues comme particulièrement virulentes pour renforcer la méfiance et la croyance dans un possible fond de vérité d'une fausse information. Les lignes directrices de la Conférence des services d'information de la

[61] Cf. dossier (en allemand seulement) de l'association Médias Suisses sur les compétences médiatiques <https://www.schweizermedien.ch/medienkompetenz>.

[62] Office fédéral de la communication, rapport « Intermédiaires et plateformes de communication. Effets sur la communication publique et approches de gouvernance », 17 novembre 2021, <https://www.bakom.admin.ch/dam/bakom/fr/dokumente/bakom/elektronische_medien/Zahlen%20und%20Fakten/Studien/bericht-kommunikationsplattformen-und-intermediaere-2021.pdf.download.pdf/Rapport%20Interm%C3%A9diaires%20et%20plateformes%20de%20communication.pdf> (version allemande consultée le 5 mars 2024).

Confédération concernant les médias sociaux définissent les critères pour réagir aux informations fallacieuses sur les nouvelles plateformes d'information « lorsqu'elles se propagent au-delà de la communauté dont elles sont issues ou de communautés proches de celle-ci ou qu'elles sont dommageables ». En principe, l'administration fédérale ne corrige les fausses informations que dans ces cas-là[63]. Le DETEC a communiqué par exemple au sujet de la fausse affiche en rapport avec les risques de pénurie d'énergie (cf. 4.2).

La recherche montre que la prévention, à travers des mesures de sensibilisation et de responsabilisation (approche dite de *pre-bunking*)[64], est bien plus efficace que la démystification. Pour l'instant, le Conseil fédéral ne mise néanmoins pas sur le *pre-bunking* immédiat, visant à démasquer ou à invalider les activités d'influence spécifiques avant même leur diffusion, car cette démarche présuppose de bénéficier au préalable d'une image détaillée de la situation.

Toutefois, la politique d'information du Conseil fédéral est en général directe, globale, multilingue, transparente et continue, ce qui complique toute tentative d'influence. Les informations sur les affaires du Conseil fédéral, sur les activités de l'administration, sur les votations et sur les élections[65] sont diffusées en plusieurs langues et par différents canaux, notamment à travers des conférences de presse régulières auxquelles participent personnellement des conseillers fédéraux. Le Conseil fédéral complète de plus en plus souvent ses informations par des vidéos explicatives et des infographiques. L'application VoteInfo est un canal d'information directe développé avec les cantons et les communes. Elle met à la disposition du grand public toutes les informations sur les scrutins fédéraux et cantonaux et leurs résultats. Ces mesures de communication sont susceptibles d'étendre la portée des informations auprès de certains groupes cibles. Mais elles ne surmontent qu'en partie le défi qui consiste à contrer les activités d'influence.

La Chancellerie fédérale est en train de concevoir une application d'information pour la communication du Conseil fédéral servant de canal direct avec la population. Selon une étude réalisée par l'institut de sondage gfs.bern en 2022, 70 % des personnes interrogées trouvent une telle application d'information intéressante et 75 % considèrent que l'approche est pertinente. Son indépendance vis-à-vis des grandes plateformes doit protéger ce canal des activités d'influence potentielle. Il pourrait en outre pouvoir être utilisé (sous forme de notifications push) en cas de crise ou d'activités d'influence nécessitant une réaction du Conseil fédéral.

En temps de crise, quand la protection de la population est en jeu, la désinformation peut avoir de graves conséquences, en cas de défaillance du réseau électrique par exemple. Elle peut entraver la capacité des institutions étatiques à réagir à la crise. Ainsi, de fausses informations sur les causes d'une panne d'électricité pourraient éveiller la méfiance de la population, l'incitant à ne pas suivre les instructions des autorités, comme les ordres d'évacuation ou les consignes de sécurité. L'application et le site web Alertswiss, utilisés par la Confédération et les cantons comme instrument d'alerte, d'alarme et d'information de la population pour gérer les catastrophes et les situations d'urgence, jouent un rôle clé dans ce contexte. Alertswiss peut servir de canal de communication direct pour informer la population des situations d'urgence liées à un événement et pour lutter contre la propagation de la désinformation au moyen d'informations précises et vérifiables, transmises rapidement. Afin d'optimiser l'efficacité d'Alertswiss par rapport à la désinformation, il importe de sensibiliser davantage les parties prenantes (utilisateurs à l'échelon de la Confédération et des cantons) à travers des formations, des organes spécialisés et les plateformes d'information disponibles.

Enfin, il faut mentionner que d'autres mesures de communication seraient nécessaires en cas de conflit armé impliquant la Suisse. L'Armée suisse engage donc des moyens dans tous les espaces d'opération, y compris l'espace de l'information en cas de conflit. Mais cet aspect ne sera pas développé dans le présent rapport. En cas de conflit armé, l'armée doit, en tant qu'instrument de la politique de sécurité, pouvoir mener des actions militaires dans l'espace de l'information de

---

[63] Chancellerie fédérale, lignes directrices Médias sociaux, mai 2021, art. 7, <https://www.newsd.admin.ch/newsd/message/attachments/67322.pdf> (version allemande consultée le 5 mars 2024).
[64] Jon Roozenbek et al., A Practical Guide to Prebunking Misinformation, 2022, (en anglais seulement) <https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf> (consulté le 5 mars 2024).
[65] Dans le cadre des dispositions légales ; pour les textes soumis à une votation fédérale, cf. notamment les art. 10*a* et 11, al. 2, de la loi fédérale sur les droits politiques (161.1 ; LDP) et, pour le renouvellement intégral du Conseil national, l'art. 34 LDP.

manière autonome ou en collaboration avec les autorités civiles, en suivant les directives stratégiques de la Confédération.

6.5 Coordination et échanges

La complexité et l'ampleur du sujet exigent une coordination et un échange d'informations étroits au sein de l'administration fédérale, ainsi qu'avec et entre les médias, les plateformes, le secteur de la recherche, et des institutions et des partenaires internationaux.

La répartition des compétences empêche pour l'instant une coordination centralisée et un tableau complet de la situation. La coordination et les échanges ont toutefois fait des progrès ces dernières années. Afin de déterminer l'ampleur des activités d'influence et d'encourager la coordination, le GS et la Chancellerie fédérale ont mené en janvier 2021 une enquête sur cette thématique au sein de l'administration fédérale. Il s'agissait d'obtenir une vue d'ensemble des travaux en cours ou prévus dans l'administration fédérale concernant les activités d'influence et la désinformation. Dans ce but, le GS a répertorié les services chargés de la détection précoce et du suivi des activités d'influence. L'enquête a montré que pratiquement toutes les unités administratives étaient potentiellement concernées. Depuis août 2022, les départements et les offices disposent d'un réseau de personnes de contact pour les activités d'influence et le DFAE organise des ateliers sur ce thème. Des plateformes de coordination et de discussion multilatérales existent aussi, de même qu'entre l'administration fédérale et des parties prenantes externes.

La Suisse échange également des informations sur la gestion des activités d'influence et de la désinformation avec des États partenaires et dans des forums multilatéraux. Ces échanges sont importants dans la mesure où les activités d'influence ont des effets transnationaux. La coopération et la coordination internationales peuvent contribuer à améliorer les réactions et à clarifier l'image de la situation. N'étant pas membre de certaines institutions, comme l'OTAN, l'UE ou le G7, la Suisse n'a pas forcément accès à toutes les informations. Pour y remédier, des réunions d'experts sont organisées avec l'UE. Un rapprochement a aussi eu lieu avec le Royaume-Uni en 2023, instaurant des échanges annuels.

Au niveau européen, le Comité directeur du Conseil de l'Europe sur les médias et la société de l'information élabore des mesures et des recommandations pour lutter contre les fausses informations. Un comité d'experts présidé par la Suisse a par exemple publié une note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits de l'homme[66]. En 2020, la Coalition pour la liberté en ligne, dont la Suisse fait partie, a publié une déclaration commune sur la propagation de la désinformation en ligne (*Joint Statement on Spread of Disinformation Online*). À la fin août 2023, elle a annoncé la création d'une task force sur la fiabilité des informations en ligne (*Task Force on Information Integrity Online*). L'OFCOM participe en outre aux travaux du *Digital Policy Lab* (DPL, laboratoire de politique digitale) de l'*Institute for Strategic Dialogue* (institut pour le dialogue stratégique). Issu d'une initiative allemande, le DPL est un espace d'échanges avec un groupe de pays affinitaires sur les thèmes de la désinformation, du discours de haine et de la réglementation des plateformes. Le Secrétariat d'État aux migrations a contribué, lors des Consultations intergouvernementales sur le droit d'asile, les réfugiés et les migrations en 2022, à mettre au point une boîte à outils en 10 points pour renforcer les mécanismes de l'OTAN et de l'UE visant à contrer les menaces hybrides, y compris l'instrumentalisation des mouvements migratoires, dans l'espace de l'information aussi.

7. Autres mesures et domaines d'action

Il ne suffit pas de prendre des mesures isolées, au niveau d'une autorité ou d'une institution, pour lutter efficacement contre les activités d'influence et la désinformation. Les développements technologiques, les ressources engagées par des acteurs étatiques étrangers et leur action coordonnée rendent nécessaire une approche globale ciblant la société tout entière. Dans une société libre, il est

[66] Conseil de l'Europe, Note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits de l'homme, décembre 2023, <https://rm.coe.int/cdmsi-2023-015-msi-inf-guidance-note/1680add25f> (version anglaise consultée le 5 avril 2024).

impossible d'endiguer la menace, encore moins avec la diffusion des nouveaux moyens technologiques. Par contre, il est possible de renforcer et de compléter certaines des mesures déjà mentionnées, surtout concernant l'observation de la situation, la détection précoce et la coordination.

Observation de la situation et détection précoce

Il est prévu que le GS aborde régulièrement – au moins deux fois par an – la thématique des activités d'influence et de la désinformation, et qu'il puisse saisir la Délséc et le Conseil fédéral si nécessaire. Les départements représentés à la Délséc et au GS – le Département fédéral de la défense, de la protection de la population et des sports (DDPS) avec le SRC et le Secrétariat d'État à la politique de sécurité (SEPOS), le Département fédéral de justice et police (DFJP) avec fedpol, le DFAE avec son Secrétariat d'État – peuvent demander au Conseil fédéral de prendre des décisions concernant d'éventuelles mesures. Des réflexions seront menées quant à la manière de coordonner l'analyse future de la situation en matière de désinformation dans le but d'identifier les influences exercées par des acteurs étatiques dans l'espace de l'information, leurs auteurs et leurs intentions, et les mesures à prendre. Il faut tirer les enseignements du suivi et des travaux menés par les offices concernés, en partageant des informations pour compléter l'image de la situation. Il convient également d'examiner comment développer et institutionnaliser la coopération et les échanges internationaux en vue d'affiner l'image de la situation, notamment en ce qui concerne l'accès et la participation aux bases de données et aux analyses du système multilatéral, d'une part avec le Royaume-Uni et d'autre part avec le SEAE. En outre, il faut examiner la possibilité de mettre en place un portail public centralisé pour la vérification des faits, éventuellement à travers une autorité de surveillance indépendante ou un institut de recherche.

Résilience par la sensibilisation, la formation et la compétence médiatique

L'exercice intégré 2025 (EI 25), organisé par la Chancellerie fédérale en collaboration avec le DDPS et les cantons, portera sur une menace hybride contre la Suisse. Dans ce contexte, les activités d'influence et de désinformation et la manière de les gérer joueront un rôle central. De son côté, l'OFCOM a lancé un soutien à la recherche, avec un nouveau programme qui met l'accent sur l'impact de la désinformation à court, moyen et long termes, afin d'étudier la désinformation dans le contexte de la formation de l'opinion. Une meilleure compréhension des effets de la désinformation dans le contexte suisse permettra de mieux évaluer la situation et de renforcer les efforts de sensibilisation et de prévention.

Les plans d'études de l'école obligatoire dans les trois régions linguistiques et les plans d'études cadres du secondaire II comprennent désormais l'instruction civique et l'éducation numérique. Plusieurs services étatiques disposent de canaux pour renseigner sur la désinformation et proposent des cours d'éducation aux médias et à la politique. L'offre étant déjà très vaste, il n'est pas nécessaire à court terme de l'étendre ni de l'approfondir. Une action rapide est déjà possible en cas de besoin grâce à la grande flexibilité des acteurs de la formation et à l'étroite collaboration avec et entre eux.

Réglementation et sanctions

L'OFCOM est en train d'élaborer un projet de consultation sur la réglementation des très grandes plateformes de communication. Le Conseil fédéral évaluera la reprise d'éventuelles nouvelles sanctions de l'UE contre des portails qui propagent de la désinformation, compte tenu du contexte particulier de la Suisse, de la proportionnalité et de leur bénéfice pour la politique étrangère et de sécurité.

Communication

Le Conseil fédéral et l'administration fédérale peuvent faire rectifier la désinformation, mais ils font un usage modéré de cette possibilité dans le contexte de la liberté d'expression. Des lignes directrices ont été établies dans ce domaine par la Conférence des services d'information de la Confédération[67]. Le Conseil fédéral s'en tient au principe de communiquer de manière directe, globale et transparente à travers plusieurs canaux, ce qui rend les tentatives d'influence plus difficiles. Quand il s'agit de

[67] Chancellerie fédérale, lignes directrices applicables à la communication au moyen des médias sociaux, mai 2021, art. 7, <https://www.newsd.admin.ch/newsd/message/attachments/67322.pdf> (version allemande consultée le 5 mars 2024).

prévoir la communication en cas d’incident ou de mesures diplomatiques, il importe d’intégrer les travaux complémentaires et les échanges visant à analyser la situation et à établir l’image de la situation à l’échelle fédérale.

Coordination et échanges

Depuis 2022, l’administration fédérale dispose d’un réseau de personnes de contact pour les activités d’influence, et le DFAE organise plusieurs ateliers sur ce thème pour les employés de la Confédération. Ces échanges ont pour but de parvenir, à l’échelon fédéral, à une perception commune de la situation, des évolutions et des activités importantes, des menaces dans le domaine de la politique de sécurité, et des mesures qui en découlent. Pour bénéficier de toutes les compétences, il importe d’intégrer des experts scientifiques, suisses ou étrangers, ainsi que des responsables d’autres pays. Les échanges internationaux, avec des États partenaires ou au sein de forums multilatéraux, sont utiles pour approfondir les connaissances spécialisées et se faire une image plus précise de la situation. Ils sont constamment favorisés et développés partout où cela a du sens. Il faut aussi continuer à développer les échanges au sein de l’administration fédérale et les institutionnaliser si nécessaire. Il convient d’examiner aussi, dans ce contexte, une coordination des efforts de la Confédération en matière de désinformation et de répression transnationale. L’importance des activités d’influence et de la désinformation pour la politique de sécurité et la menace qu’elles représentent se sont accrues, et avec elles le besoin de coordination. Il convient donc de renforcer la concertation entre les différents organes de la Confédération qui sont chargés de la politique de sécurité. Mieux coordonnées, l’analyse et l’évaluation de la situation qui en découleront devront aussi être davantage intégrées aux réflexions de ces organes et aux échanges au sein de l’administration fédérale.

8. Glossaire

Activités d'influence
Les activités d'influence dans l'espace de l'information comprennent tout un arsenal de mesures, dont la désinformation. Elles visent à manipuler les perceptions, les pensées et les actions des individus, des groupes et des sociétés. Elles peuvent être menées par des acteurs étatiques comme non étatiques (cf. point 2.1).

Campagne d'influence
Une campagne d'influence consiste, pour un acteur qui dispose de ressources et de capacités importantes, à coordonner plusieurs opérations d'influence. Les activités sous-jacentes à une campagne d'influence peuvent mobiliser différents moyens d'influence (désinformation, cyberattaques, pressions et autres).

Désinformation
La désinformation consiste en informations trompeuses ou entièrement inventées pour influencer ou saboter des processus politiques, pour attaquer la crédibilité des institutions et des médias, ou tout simplement pour semer le doute sur la fiabilité des informations (cf. point 2.1).

Fausses informations ou fake news
Les fausses informations consistent en affirmations volontairement fausses, exprimées de mauvaise foi et diffusées dans un but de manipulation politique, pour des intérêts financiers ou d'autres motifs et qui tirent leur pouvoir de nuisance de la dynamique imprimée par les réseaux sociaux[68].

FIMI
L'UE utilise la notion de *Foreign Information Manipulation and Interference*, qu'elle traduit par *manipulation de l'information et ingérence depuis l'étranger*. Pour l'UE, la FIMI recouvre un type de comportement qui n'est pas pour l'essentiel illicite, mais qui menace les valeurs, les procédures et les processus politiques, ou qui peut les influencer de manière négative. Il s'agit d'activités de manipulation menées délibérément et de manière concertée. L'UE a mis au point des normes de vérification des faits pour les contrer.

Malinformation
La malinformation est une information qui se fonde sur la réalité, mais qui est diffusée en vue de porter préjudice à une personne, à une organisation ou à un pays. Il s'agit souvent de faire fuiter des informations qui n'étaient pas destinées au grand public.

Mésinformation
La mésinformation (*misinformation* en anglais) consiste aussi à propager des informations factuellement incorrectes, erronées ou trompeuses, mais indépendantes de l'utilisation qui en est faite et sans intention de tromper.

Opération d'influence
Une opération d'influence peut comprendre plusieurs activités d'influence coordonnées par un acteur dans l'espace de l'information.

Propagande
La propagande est un instrument d'influence des opinions. Elle se fonde en principe sur des vérités, mais elle les choisit, les interprète et les expose de sorte à créer ou à favoriser certaines conceptions ou visions. Quand un canal diplomatique considéré comme légitime, par exemple le compte X/Twitter d'une représentation étrangère, diffuse de la désinformation, il devient difficile de faire la distinction. La propagande est un élément des activités d'influence dans l'espace de l'information qui se distingue (en partie) de la désinformation par le fait qu'elle peut aussi être véridique. En effet, la propagande se

[68] Rapport du Conseil fédéral, Un cadre juridique pour les médias sociaux. Nouvel état des lieux. Rapport complémentaire du Conseil fédéral sur le postulat Amherd 11.3912 « Cadre juridique pour les médias sociaux », mai 2017, <https://www.bakom.admin.ch/dam/bakom/fr/dokumente/informationsgesellschaft/social_media/social%20media%20bericht.pdf.download.pdf/social-media-bericht-2017-FR.pdf> (version allemande consultée le 5 mars 2024).

fonde souvent sur des faits avérés, mais qui sont interprétés, manipulés, décontextualisés ou contextualisés de manière unilatérale.