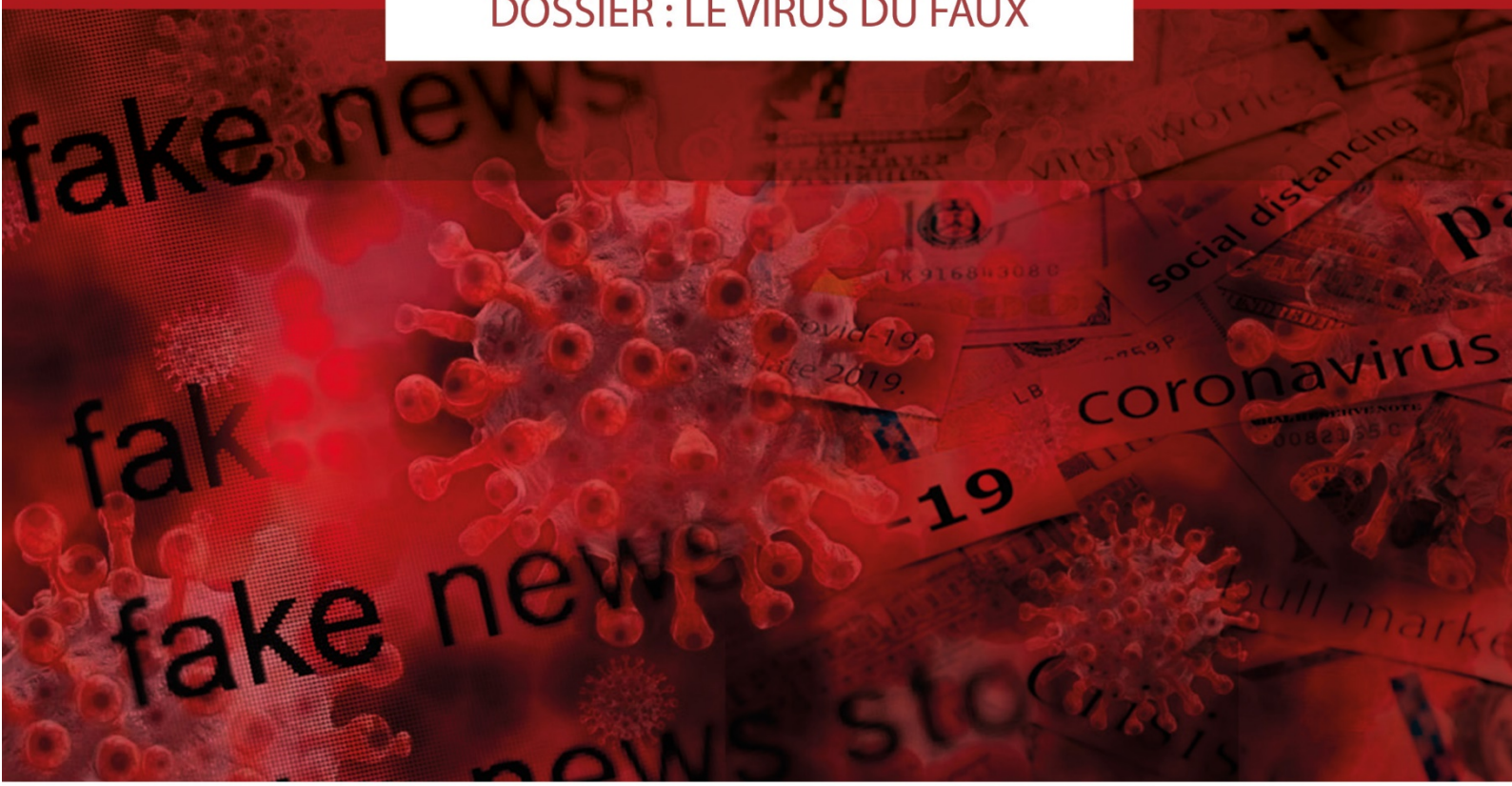
iris-france.org

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

GLOSSAIRE

DOSSIER : LE VIRUS DU FAUX



Dossier dirigé par François-Bernard Huyghe, directeur de recherche à l'IRIS.

iRiS
INSTITUT DE RELATIONS
INTERNATIONALES
ET STRATÉGIQUES

FRANÇAIS

A

Attaque informationnelle : action visant à espionner, à priver la cible de contrôle sur son système d'information, à se substituer à elle (par exemple obtenir des données confidentielles ou prendre les commandes d'un système), soit enfin à causer un dommage par des messages trompeurs.

Attribution : fait de pouvoir notamment désigner le responsable d'une attaque informatique.

Authenticité : qualité de ce qui émane réellement de l'auteur auquel on l'attribue.

B

Biais cognitif : propension du cerveau humain à reproduire des erreurs de jugement (y compris en mésinterprétant le sens des messages) aggravée par sa tendance à adopter des conduites en contradiction visible avec les données de l'expérience ou les connaissances facilement accessibles. Exemple : le biais de confirmation par lequel nous recherchons des informations qui nous prouveront que nos idées et préjugés sont confirmés par les faits.

Bouc émissaire : groupe, homme (ou animal des sacrifices, d'où l'origine de l'expression) auquel une communauté fait porter une culpabilité supposée (s'exonérant elle-même de toute faute).

C

Cohérence : le fait pour une information d'être compatible avec l'ensemble des connaissances préalables que l'on possède, mais pas forcément preuve de vérité.

Communauté virtuelle : groupe qui n'est pas réuni physiquement, mais qui, communiquant par des moyens électroniques par exemple, entretient des habitudes d'échange (ludique, savante, amicale, militante, experte, etc.) sur un thème qui en réunit les membres.

Communication de crise : procédures et méthodes mises en œuvre pour rassurer les médias et les parties prenantes lorsqu'une organisation est confrontée à de graves accusations pour son image, à une catastrophe ou à un dysfonctionnement entraînant des dommages inhabituels. Ou est indirectement mise en cause par un accident ou une crise extérieure.

Communication publique : délicat euphémisme pour lobbying.

Confiance : disposition à croire en la vérité d'affirmations ou dans le comportement favorable ou la sincérité de gens ou institutions. En informatique : techniques destinées à vérifier la sécurité ou l'authenticité des échanges.

Confidentialité : fait pour l'information d'être accessible uniquement à ceux qui y sont autorisés.

Conspirationnisme : théorie utilisée en propagande et attribuant des événements négatifs à des complots fomentés par des groupes secrets et presque tout-puissants.

Couches : Internet est composé de trois "couches" : sémantique (ce qui a du sens, les messages), physique (les appareils, terminaux et vecteurs qui permettent à Internet de fonctionner) et logistique (les codes et protocoles qui permettent à l'ensemble de fonctionner, aux appareils de communiquer entre eux, etc.).

Crise : la crise, d'après son étymologie, est le fait de séparer la décision, le jugement ; c'est aussi la phase décisive d'une maladie à partir de laquelle celle-ci peut s'orienter vers la guérison ou vers l'aggravation. Il y a crise là où tout est possible. Elle traduit l'anomalie, voire l'anomie, soudain révélée par contraste avec un fonctionnement présupposé « ordinaire ».

Cyberattaque : action menée à travers Internet, souvent anonymement, éventuellement sous « faux drapeau » et malveillante : voler des informations, compromettre le fonctionnement d'un système informatique, ou à produire un effet psychologique (subversion, déstabilisation) ...

Cyberdissuasion : méthode destinée à décourager les cyberattaques, transposition plutôt problématique dans le monde numérique du principe de dissuasion de la Guerre froide. En effet, comment savoir qui menacer, qui frapper, qui accuser et comment mesurer riposte et rétorsion dans le cyberespace ?

Cyberespace : métaphore désignant le domaine des interactions entre données et réseaux et accessible par ordinateurs, puis, au sens large, le monde global de tous les ordinateurs et systèmes connectés par Internet.

Cygne noir : expression lancée par Nassim Nicholas Taleb pour décrire les événements à très forte improbabilité (ou ceux que personne n'avait prévus) et qui bouleversent toutes les données du jeu.

D

Déception : dans la terminologie militaire, mesure de tromperie, trucage, falsification, mise en scène. Elle est destinée à amener l'adversaire à agir de façon préjudiciable à ses propres intérêts. Ce terme est repris dans le vocabulaire économique.

Déchiffrement : action consistant à retrouver l'information initiale contenue dans le message chiffré à l'aide de la clef secrète appropriée.

Décryptage : restitution en clair d'une information sans avoir accès à la clef secrète qui permet son déchiffrement normal.

Déni de service : attaque logique paralysant une ressource informatique, par exemple en saturant artificiellement les services d'un site sur Internet.

Désinformation : mot se prêtant à un usage abusif, surtout lorsqu'il finit par désigner toute opinion diffusée par les médias et que l'on croit fausse ou biaisée. La désinformation consiste à propager délibérément des informations fausses pour influencer une opinion et affaiblir un adversaire.

Déstabilisation : forme d'action contre une organisation visant à y aggraver les conflits internes et à lui faire perdre ses alliés ou son image positive.

Diabolisation : technique de base de la propagande consistant à présenter l'adversaire comme mauvais par essence et, à un degré incommensurable, à lui attribuer des crimes (propagande d'atrocité) et à le comparer aux pires ennemis du genre humain par amalgame.

Discrétion : au sens ordinaire, le fait de ne pas attirer l'attention, ou de ne pas chercher à savoir ce qui est inutile ou gênant. Soit, enfin, le fait pour un signal d'être « discret », c'est-à-dire de se compter en unités présentes ou pas, et de produire du sens par cette présence/absence, et non pas par le degré ou l'intensité comme c'est le cas pour un signal analogique.

Disponibilité : qualité de l'information accessible au moment voulu. Provoquer un déni d'accès (par exemple en bloquant l'accès à un site) revient à s'en prendre à la disponibilité de l'information.

Dissonance cognitive : processus par lequel un sujet a tendance à modifier ses opinions et ses attitudes afin de les mettre en harmonie, comme à moindre coût, avec ses autres opinions, notamment avec celles qu'il professe en accord avec son groupe social.

Dissuasion : fait de persuader un éventuel adversaire de ne pas vous attaquer en le persuadant que ses pertes - notamment du fait de votre riposte - seraient très supérieures à ses gains et surtout très probables.

Doxa : idées reçues, opinion dominante reposant davantage sur le conformisme que sur l'examen sur le fond ou la recherche de preuves.

E

Élément de langage : terminologie à la mode, surtout en politique, pour désigner les arguments et les thématiques auxquels doivent recourir les membres d'une organisation pour assurer la cohérence de sa communication

Éristique : art du débat ou de la controverse.

F

Fugacité : le fait de ne durer qu'un instant, caractéristique de nombre de cyberattaques.

Fuite d'information : perte ou vol de données, d'origine volontaire ou non .

G

Garde-barrière : notion traditionnelle de la sociologie des médias, les *gatekeepers*, ceux qui gardent l'accès aux mass medias (un directeur de programmation, par exemple) ou en sont les "passeurs". Aujourd'hui, chacun devient un peu garde-barrière, dans la mesure où tout internaute peut publier, commenter, signaler, être repris, cité, engendrer un débat, etc.

Geek : fanatique de culture informatique

Guerre de l'information : acquérir données et connaissances (et à en priver l'adversaire) dans un but stratégique, s'attaquer à ses systèmes (vecteurs et moyens de traitement de l'information), viser à une domination informationnelle. Plus couramment : toute opération recourant à la rumeur, à la propagande, à un virus informatique qui corrompt ou détourne le flux des informations ou des données d'un adversaire, un État, une armée, une entité politique ou économique.

I

Influence : stratégie indirecte visant à obtenir d'autrui un assentiment ou un comportement, par le prestige de son image, par une forme quelconque de persuasion ou de « formatage » des critères de jugement, soit, enfin, par la médiation d'alliés ou de réseaux. Art de faire vouloir à autrui ce que vous voulez.

Information : concept qui pose davantage de problèmes qu'il n'en résout. À la fois des données qui se stockent quelque part sur un support ou se transportent, des « nouvelles » (des récits ou des descriptions de la réalité nouveaux et surprenants à un degré ou à un autre pour le destinataire), des messages délivrés par moyen de communication à travers l'espace et de transmission à travers le temps, et enfin des informations devenues des connaissances dans le cerveau de quelqu'un, contextualisées, reliées à d'autres informations, faisant sens, donc un vrai savoir.

Ingénierie sociale : du jargon informatique anglais *social engineering*, toutes les méthodes et astuces pour conduire un sujet à faire de son plein gré ce que désire le manipulateur, comme lui révéler un code confidentiel. Forme de l'antique stratagème.

Intégrité : qualité de l'information qui n'a pas été altérée.

Intoxication : opération consistant à faire parvenir à un adversaire une information fabriquée qu'il croira avoir saisie à votre insu pour l'amener à prendre des décisions qui tourneront à son détriment.

L

Levier : expression fréquemment employée pour désigner les mécanismes psychologiques par lesquels la propagande tente d'agir sur le psychisme. On distingue ainsi le levier de conformisme ou d'unanimité, le levier d'adhésion associant un parti ou une personne à un symbole positif, le levier de rejet reposant sur la diabolisation de l'adversaire et la peur qu'il suscite, etc.

Lien : revêt le double sens de lien sémantique (comme l'hyperlien qui mène du texte A au site B en fonction de son sens) et de lien social, notion qui inclut à la fois l'intensité des échanges sociaux et leur dimension psychologique.

M

Manipulation : le fait de présenter des informations de façon à susciter une réaction prévisible et souhaitée chez le destinataire. Concept fourre-tout à employer avec précaution : on risque d'attribuer toute réaction que l'on désapprouve.

Mésinformation : toute situation où le sujet n'accède pas au degré de connaissance de la réalité auquel il pourrait prétendre au regard de ses sources d'information. Une altération physique de données peut nous mésinformer comme en cas de mauvaise réception ou de conservation défectueuse de signaux. Elle peut aussi résulter de rapports avec nos « sources d'information », médias ou réseaux humains dont nous proviennent des « nouvelles ». Ou de la façon dont nos cerveaux interprètent le réel pour le réduire au connu, au prévisible ou au souhaitable.

Métadonnées : littéralement données à propos de données. Tout système (informations techniques ou descriptives) permettant d'indexer des contenus comme le catalogue d'une bibliothèque, ou encore les tags.

N

Notoriété : simple fait d'être connu (ne pas confondre avec la réputation qui suppose un contenu ou les connotations qu'évoque cette notoriété dans l'esprit d'un public).

Novlangue : langue imposée par Big Brother dans le roman d'Orwell *1984* et destinée à paralyser la pensée critique. Par extension, synonyme de langue idéologique fixe que ses partisans parlent tous de manière figée et prévisible.

Numérique : le mot correspond à l'anglais digital et désigne la caractéristique des signaux codés sous forme de données binaires (0 ou 1). Ces signaux sont discrets au sens mathématique (le signal est là ou pas). Le terme a fini par prendre le sens beaucoup plus large de « lié à l'informatique ».

P

Paralogisme : raisonnement faux ayant les apparences de la rigueur et de la validité. À la différence du sophisme, le paralogisme traduit une erreur de raisonnement de bonne foi et non pas une volonté de tromper.

Pensée de groupe : tendance au sein d'un groupe à rechercher le consensus et la cohérence, souvent au détriment de l'efficacité de la décision ou de la cohérence des opinions avec la réalité.

Persuasion : processus délibéré visant à faire accepter une proposition pour vraie ou pour désirable par quelqu'un, voire à l'amener à se comporter de la façon souhaitée.

Propagande : moyens et techniques destinés à faire adhérer une communauté (nous recevons la propagande en tant qu'individus, mais elle nous vise en tant que membres d'un groupe) ou à faire adhérer à une communauté (tel parti, telle église, tel courant de pensée). Cette adhésion porte sur un contenu idéologique contesté dans le cadre d'un conflit avec une autre communauté porteuse d'autres croyances.

Propagation : troisième dimension de la vie de l'information. Avec la communication, qui doit lui faire franchir l'espace et susciter le partage, avec la transmission censée vaincre le temps et garantir sa conservation, la propagation a pour fonction de vaincre des résistances mentales (autres croyances, indifférence...) et de rendre l'information (en particulier la croyance) "contagieuse".

R

Référencement : le fait de mentionner quelque chose ou quelqu'un suivant un certain code ou un système (par exemple une note de livre). Le mot a pris un sens nouveau sur Internet : le fait d'être signalé notamment par les moteurs de recherche et la quête d'un bon référencement (discipline qui s'enseigne) est devenu l'alpha et l'oméga de l'influence sur le Web.

Réseaux sociaux : groupe d'internautes réunis sur la Toile par un centre d'intérêt commun, une cause, un thème, mais aussi l'ego de quelqu'un (son "capital" d'amis et de correspondants).

Résilience : capacité de revenir à son état initial sans trop de délai ou de dégâts, par exemple après une attaque informationnelle.

Rhétorique : technique de l'art oratoire ayant tantôt le sens de « bien parler » (au sens de faire des discours admirés et émouvants), tantôt le sens plus précis d'un art de persuader par les mots (discours ou écrits). Les sémiologues parlent même d'une rhétorique de l'image (à propos par exemple de la publicité) pour désigner sa capacité à nous convaincre.

Risque : éventualité d'un événement négatif, donc probabilité et possibilité d'un dommage.

Rumeur : souvent présentée comme « le plus vieux média du monde » puisque le bouche-à-oreille, le cancan, le potin, le commérage, le bruit, souvent la médisance seraient nés avec le langage. Au sens strict, elle doit porter sur l'énoncé d'un fait (« X a fait à Y », « en réalité Z a fait ceci pour tel motif caché », « il existe tel risque qu'on nous dissimule ») et non d'une simple opinion, même injurieuse.

S

Sabotage : initialement, le fait de travailler "comme un sabot" pour punir son patron. Le sabotage, au sens de mener des actions destinées à empêcher une organisation, une machine ou un dispositif de fonctionner, est une des fonctions les plus significatives des logiciels malicieux.

Sophisme : raisonnement fallacieux présentant les apparences d'un syllogisme irréfutable. Il existe des listes de sophisme (renversement de la charge de la preuve, argument d'autorité, argument *ad hominem* s'en prenant à la personne plus qu'à l'argument, fausses alternatives et des dizaines d'autres).

Source : origine d'une information en veille. Les sources formelles sont des documents (livre, base de données, article, émission, déclaration), les sources informelles résultant d'observations, de bouche-à-oreille, etc.

Stéréotype : images préconçues, clichés simplificateurs associés généralement par le public à un nom ou un thème, servant autant à la manipulation des masses qu'à une forme d'économie mentale, comme réducteurs de la complexité excessive du réel (sans compter qu'un stéréotype comporte souvent une part de vérité).

Stratégie d'influence : ensemble de moyens et d'actions délibérées, hors la force, l'autorité et les contreparties tangibles, coordonnés et destinés à produire un effet sur l'évaluation ou sur la décision d'un individu, d'un groupe ou d'une organisation.

Surinformation : situation que chacun peut éprouver quotidiennement, résultant de la surabondance de données disponibles, à tel point que leur utilisateur ne peut plus en retirer une connaissance pertinente. Selon la formule célèbre, "trop d'information tue l'information ".

Surveillance : l'extension des systèmes de surveillance sous prétexte d'anticipation des dangers est une tendance lourde à l'ère numérique. Les possibilités de recueillir et de croiser des données pour prédire des comportements et identifier des responsabilités en est le prolongement.

T

Temps de cerveau humain : valeur économique. Notre faculté d'attention étant limitée, on peut « créer de la valeur » en dirigeant l'attention de consommateurs sur des publicités ou des formes de spectacle dont la consommation présente un intérêt pour un acteur économique. Le négoce du temps de cerveau humain est souvent la rançon d'une économie que l'on dit de la gratuité.

V

Veille : opération de surveillance, souvent par simple collecte et analyse de documentation, composante essentielle de l'intelligence économique. Elle se subdivise en veille technologique, concurrentielle, géopolitique, sociétale.

ANGLICISMES

FRÉQUEMMENT EMPLOYÉS À PROPOS DE L'INFODÉMIE OU LA DÉSINFORMATION

A

A.P.T., Advanced Persistent Threats : piratage informatique durable et difficile à déceler, visant souvent une organisation et une entreprise dans une stratégie à long terme, par extension, nom des groupes de *hackers* d'élite (souvent désignés comme APT 21, APT 19, etc.) qui le pratiquent.

Astroturfing : faire croire artificiellement en l existence d un mouvement d opinion, surtout en ligne avec des employés ou des algorithmes ; dit aussi « similitantisme ».

B

Big Data : énormes volumes de données dépassant les capacités de traitement des logiciels ordinaires.

Bot (robot) : algorithme imitant une identité et un comportement humain en ligne.

Botnet : réseau de robots, machines compromises dont un manipulateur (un réseau de mercenaires et de pirates, par exemple) a pris le contrôle à distance.

Brand, branding : vanter la marque, nation branding, "vendre" l'image de son pays.

Bullshit : baratin, discours qui n a aucun sens ou ne se réfère à rien de réel.

Buzz : bruit qui se propage sur la Toile de clavier à écran.

C

Clickbait : piège à clicks, sites dont l unique fonction est d attirer des visites d internautes, revendues à des annonceurs, où l annonce des contenus sensationnels, même invraisemblables, attire un maximum de secondes de cerveau humain.

Conspiracy theories : théories conspirationnistes attribuant des événements cruciaux à des complots fomentés par des groupes secrets.

Crowdsourcing : faire appel à des internautes pour résoudre un problème de façon coopérative.

Crowdfunding : faire appel à des financements en ligne, etc.

Cyber : préfixe pour les objets, lieux ou événements liés de près ou de loin à Internet. On parle de cyberespace, cyberculture, cyberpunk...

D

Deep fakes : hypertrucage, falsification de vidéos très sophistiquée, basée sur le deep learning, ce qui permet par exemple de changer le visage ou les propos d une personne filmée.

Deep learning : apprentissage « profond », basé sur l intelligence artificielle et les big data, et permettant à la machine travaillant comme des neurones de reconnaître des images ou la parole, éventuellement pour les anticiper ou les imiter.

Doxing (*kompromat* en russe) : mise en ligne de données sensibles (authentiques ou truquées) sur une personne afin de détruire sa réputation. Exemple le *revenge porn* : publier les ébats sexuels de quelqu'un pour pourrir sa vie.

F

Fact-checking : vérification des "faits" pratiqués nombre de médias *mainstream* (avec l'aide de compagnies du numérique) pour combattre les "*fakes*".

Fakes : fausses informations (de *fake* : objet contrefait, fabriqué) bobard en français ou infox.

Follower : "suiveur", nom donné à la personne qui s'abonne au compte Twitter d'une autre par exemple

G

Gate-keepers : infomédiaires, ceux qui gardent l'accès aux mass medias (un directeur de programmation, par exemple) ou en sont les "passeurs".

H

Hacktivism : activité militante recourant aux techniques des hackers, le piratage informatique, et s exprimant en ligne.

Hack & leak : méthode consistant à pirater des informations confidentielles (par exemple d un parti politique), mais pour les mettre sur la place publique et compromettre l adversaire.

Hate speech : discours de haine attaquant une personne sur la base de sa race, nationalité, religion, sexualité, etc. Concept utilisé par le juge ou les Gafa pour justifier des retraits de contenus ou de comptes.

Hoax : faux bruit sur Internet, canular ou légende.

Hybrid warfare : concept-valise cher aux think tanks, le mélange d utilisation d armées classiques, de groupes paramilitaires, de cyberattaques et de désinformation que mèneraient les Russes contre l'Occident.

I

Infodemics : infodémie, néologisme pour l'épidémie de nouvelles fausses ou douteuses qui accompagne la pandémie.

Information operations (ou influence operations) : délicat euphémisme pour propagande.

Infowar : infoguerre, lutte pour le contrôle de l information, visant aussi à dégrader les informations et fonctions informationnelles adverses.

L

Leader d opinion : membre d un groupe sachant susciter ou traduire l intérêt ou l interprétation dominants. Exemple : les « e-influents » dont l opinion compte beaucoup sur Internet.

Leak : la fuite de données confidentielles, de l'intérieur d une organisation ou par un piratage/espionnage informatique (*hack*) ou par un lanceur d'alerte

Lobby : groupe d intérêts (économiques, identitaires, éthiques, idéologiques…) cherchant à obtenir certaines décisions de la puissance publique

M

Mainstream : "courant dominant", désignation des produits des industries culturelles dont le succès est universel ou aux formes médiatiques de l'idéologie dominante.

Malware : logiciel « malicieux » destiné à nuire à un système informatique, tels un virus ou un cheval de Troie.

Marketing politique : application aux élections (ou à la gestion de l opinion publique) des méthodes commerciales d'étude des attentes des populations, d amélioration de l image de marque du candidat et de communication persuasive.

Mass media : hybride d anglais et de latin désignant les appareils de diffusion d information construits sur le modèle « un-tous », apparus avec les rotatives : presse grand public, radio, télévision…). Volontiers opposés aux médias sociaux**.**

Media litteracy : apprentissage critique du fonctionnement des mass médias, processus étendu aux réseaux sociaux.

Misinformation : mésinformation ou malinformation, état de confusion, pas forcément provoqué par la volonté de tromper (désinformation), mais résultant de la surabondance et du caractère douteux des informations disponibles.

N

Narrative et counter-narrative : "récit", l'argumentaire justificatif d'un camp contre un autre.

Variante, **storytelling** : narrer un cas exemplaire pour illustrer une idée.

P

Post-truth : post-vérité, phase de l'histoire humaine où la mauvaise information concurrencerait la bonne et où une large fraction de l opinion serait indifférente à la vérification des informations dont elle se nourrit pourvu qu elles flattent ses passions.

Privacy : tout ce qui touche à la protection de la vie privée.

Proxy : en informatique, élément placé entre deux hôtes pour faciliter ou surveiller leurs échanges. Par extension, intermédiaire comme dans l expression « guerre par proxy », ou pour désigner des groupes de hackers utilisés comme quasi mercenaires.

Psyops (Psychological operations) : en terminologie militaire, ce sont les actions politiques, militaires, économiques et idéologiques destinées à créer sur une opinion neutre, amicale ou non hostile, des attitudes émotionnelles ou comportements favorables aux objectifs visés. Devenues MISO (Military Information Support Operations).

Public diplomacy : initialement l action visant à « promouvoir l'intérêt national des États-Unis par la compréhension, l information et l'influence des publics étrangers », influence idéologique hors frontières notamment *via* des médias internationaux.

R

Ransomware : ou rançongiciel qui chiffre les données d un ordinateur contre le gré de son propriétaire et peut être enlevé moyennant une rançon en bitcoins.

Ranking : classement des pages dans les recherches d un moteur de recherche et qui en détermine très largement la visibilité donc la popularité.

S

Sharp power : terme dépréciatif pour désigner l influence chinoise ou russe assimilée non à un soft power mais à une manipulation de l opinion étrangère en vertu du principe « je dis la vérité, vous faites de la propagande. ».

Smart power : combiner utilement hard et soft power, puissance et influence, force et séduction pouvoir militaire + économique + culturel.

Social learning : imposer ses concepts et ses idées en amont des marchés par une norme culturelle, la promotion d un style de vie, le formatage intellectuel des décideurs d un pays. Ne pas confondre avec *social engineering* (élicitation).

Soft power : capacité d influencer ou amener à penser comme vous par séduction, attraction ou formatage des esprits.

Spin doctor : spécialiste de la manipulation de l opinion, conseiller en marketing politique guidant un candidat par exemple

T

Think Tanks : Centres de recherche de droit privé à but non lucratif produisant des idées et propositions dans le domaine politique, économique, stratégique, écologique, etc.

Trolling : pourrir le débat par une controverse qui s enlisera sur les réseaux sociaux.

W

Watchdog : « chiens de garde », organisations ou groupes de citoyens dénonçant les scandales.

Weaponization (of information) : transformation de l'information en arme (ah, bon ce n'était pas le cas depuis toujours ?), façon de désigner l'influence et la « guerre à la réalité » (désinformation) russes.

Whistle Blower : « siffleur » (de pénalités), celui qui dénonce un abus qu il a constaté dans son entreprise ou son organisation, les révèle par des *leaks.*

GLOSSAIRE

DOSSIER : LE VIRUS DU FAUX

DOSSIER DIRIGÉ PAR FRANÇOIS-BERNARD HUYGUE, DIRECTEUR DE RECHERCHE À L'IRIS
DÉVELOPPÉ DANS LE CADRE DE L'OBSERVATOIRE (DÉS)INFORMATION ET GÉOPOLITIQUE AU TEMPS DU COVID-19 DE L'IRIS.

INSTITUT DE RELATIONS
INTERNATIONALES ET STRATÉGIQUES
2 bis, rue Mercœur
75011 PARIS / France

+ 33 (0) 1 53 27 60 60
contact@iris-france.org

@InstitutIRIS
iris-france.org