LIVRE BLANC

FACE THE UNPREDICTABLE

LA GUERRE DE L'INFORMATION :

LA NOUVELLE ARME CYBER

SOMMAIRE

1. TEHTRIS

Fondé en 2010, TEHTRIS est un **éditeur leader mondial dans la neutralisation automatique et sans action humaine des cyberattaques** avec la TEHTRIS XDR Platform. Avec son ingénierie « Security & Ethics by design », cette solution apporte aux spécialistes de la cybersécurité une vision holistique de leur infrastructure, tout en garantissant la confidentialité de leurs données. OPEN XDR, elle est compatible avec les solutions de sécurité du marché au moyen de ses APIs. Grâce à sa technologie, TEHTRIS se positionne en tiers de confiance européen. Avec ses partenaires internationaux, TEHTRIS XDR Platform surveille, analyse, détecte et neutralise les menaces dans plus de 100 pays au profit d'acteurs majeurs de l'industrie, des transports, de l'ingénierie et des services, et des administrations. En veille permanente sur la cybercriminalité et à l'écoute de ses clients, notre volonté est de réduire au maximum les risques, pour faire face à l'imprévisible.

2. LA GUERRE INFORMATIONNELLE : LA NOUVELLE GUERRE CYBER

En 2021 Florence Parly annonçait que des pratiques désinhibées peuvent affecter le fonctionnement de notre démocratie (...) dans de nouveaux champs : le cyber, l'espace, la désinformation. Cette déclaration introduit bien l'idée que la perception de la guerre cyber a évolué. Elle se joue désormais au-delà du terrain purement matériel, géographique, ou physique. Elle se joue aussi, sur le terrain psychologique. Cette évolution confirme la nécessité de maîtriser cette nouvelle arme informationnelle afin d'étoffer son arsenal et d'assurer un avantage stratégique.

Cette menace se traduit à travers la diffusion d'information, voire de désinformation. Elle est d'autant plus dangereuse qu'elle n'a pas de frontière géographique, n'a pas de limite dans le temps. Dans une époque où la lecture des contenus est réduite, où la fréquence des partages augmente, la diffusion des informations se fait à une vitesse incontrôlable.
Tout le monde peut être victime et acteur de désinformation. Tous ces éléments font de la guerre cognitive une technique de manipulation des plus dangereuses.

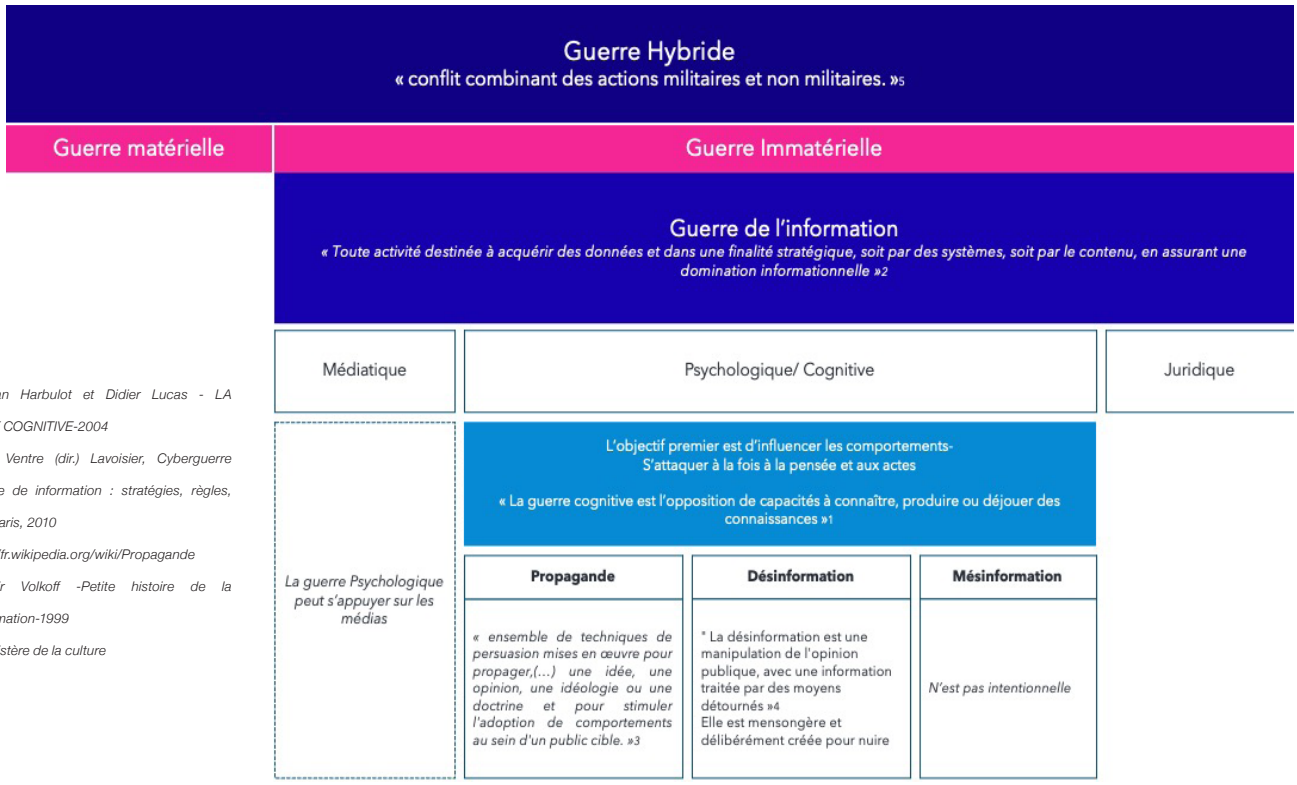
Quel est ce nouveau modèle de guerre cyber ? Comment fonctionne-t-il ? A qui s'adresse-t-il ? et comment s'en prémunir ?

2.1 UN NOUVEAU TERRAIN DE COMBAT

De nombreux termes apparaissent pour parler de guerre cognitive.

On parle de guerre psychologique, de manipulation, de désinformation, de fake news, de guerre hybride.

Tentons de faire le point sur toutes ces dénominations ci-dessous (il n'existe aucun consensus à ce jour), car il est important de comprendre chacun de ces termes, pour mieux appréhender cette nouvelle guerre. Cette dernière est complexe, autant par l'utilisation de techniques (comme la propagande ou la désinformation) qu'elle emploie, que par le fait qu'elle se base sur les failles humaines. Les attaquants, en effet, vont encore et toujours s'appuyer sur les fameux biais cognitifs auxquels nous sommes tous soumis. Nous verrons comment ultérieurement. Nous parlerons de guerre psychologique, plus globalement dans cet article, car elle reste une des principales formes de guerre de l'information.



1.Christian Harbulot et Didier Lucas - LA GUERRE COGNITIVE-2004

2.Daniel Ventre (dir.) Lavoisier, Cyberguerre et guerre de information : stratégies, règles, enjeux-Paris, 2010

3.https://fr.wikipedia.org/wiki/Propagande

4.Vladimir Volkoff -Petite histoire de la désinformation-1999

5.Le ministère de la culture

Si la technique de la guerre psychologique est bien maîtrisée, elle peut devenir une vraie arme très acérée. Comment fonctionne-t-elle ? Sommes-nous tous concernés ? Nous allons tenter de répondre à ces questions, au travers d'exemples précis, qui ont fait la une de l'actualité. Avant ça, faisons un premier constat sur les raisons du succès de cette nouvelle guerre ?

Les causes des manipulations de l'information peuvent être à la fois individuelles et collectives.

CAUSE SOCIALE ET ÉCONOMIQUE

Face à une concurrence entre nations de plus en plus forte, nous sommes confrontés à une mutation des menaces. La déstabilisation joue un rôle fondamental et tous les coups sont permis. Les États l'ont compris et vont user de stratagèmes psychologiques. Le cyberespace est l'un de ces lieux où s'expriment les rapports de force et où apparaissent de nouveaux types de vulnérabilités. Maîtriser la guerre psychologique c'est maîtriser ses capacités géopolitiques, économiques, politiques, financières, scientifiques, culturelles et religieuses. Le cyber espace est un lieu de compétition stratégique.

On voit bien que les États n'hésitent pas à en faire usage pour déstabiliser l'ennemi, pour le tromper sur ses propres intentions, influencer sa prise de décision. Bien sûr, il n'était pas question d'ignorer le fait que l'ennemi peut être à l'intérieur même du pays : les gouvernements peuvent manipuler l'information auprès de leur propre population, pour renforcer leur pouvoir (nous le verrons plus en détails plus tard) pour faire perdre confiance dans les démocraties ou à l'extérieur de leur pays, pour manipuler un autre État à des fins stratégiques.

Les fausses nouvelles ont des conséquences dans le monde réel. Les gens, les parties politiques, sont prêts à inventer des informations pour gagner de l'argent facile, pour permettre de ré élire un candidat. Les fausses données publiées sur les réseaux peuvent générer de la terreur ou des doutes. On le voit très concrètement au sein des organisations, quand ces dernières sont attaquées, menacées de divulguer des informations, vraies ou fausses. Elles ont alors été victimes de chantages et de sabotages.

Partant de ce fait, il est important d'adopter dans sa stratégie de défense, une arme adaptée et proportionnelle à cette nouvelle menace. Néanmoins, on se heurte rapidement à des questions d'ordre éthiques et juridiques. C'est le droit pénal interne qui entre en jeu, et notamment les droits de l'homme. Or, les autres nations nient bien souvent les actes de désinformation ou de manipulation psychologique et agissent à la limite de la légalité.

CAUSE PSYCHOLOGIQUE OU INDIVIDUELLE

> Une « idée fausse mais claire et précise, aura toujours plus de puissance dans le monde, qu'une idée vraie, mais complexe ». - Alexis de Tocqueville

L'Homme a horreur du vide et va chercher à le combler. C'est donc ce qui se passe quand il se retrouve face à une absence d'information : il va en créer une ou plusieurs, quitte à ce que ce soit faux. C'est ainsi que naissent d'ailleurs la majorité des théories du complot.
En témoigne l'origine de la plupart des virus qui suscite généralement les plus folles idées. L'assassinat de JFK, ou la mort de Lady Di, ont alimenté de nombreux journaux. D'autres théories sont encore plus saugrenues, comme celles qui disent que Mickael Jackson ou Elvis Presley ne seraient pas morts ! Ces théories les plus farfelues ne datent pas d'aujourd'hui, puisque l'idée même que la terre serait ronde a été remise en cause. Tout cela est d'autant plus exagéré, et transposé, avec l'avènement des réseaux sociaux. Ces derniers deviennent un moyen de communication ouvert où tout le monde peut s'improviser « journaliste », ou porteur de fausses informations, d'ailleurs 79%* des personnes croient à une théorie complotiste.

L'anonymat favorise la diffusion d'informations valides ou non valides, de propos haineux, de diffamations... Ces informations peuvent avoir des sources diverses comme venant de militants un peu trop actifs, de personnes qui cherchent de la notoriété, d'agences spécialisées, ou de trolls, de supporters politiques sans scrupules...
Le besoin de contrôle, la recherche de valorisation de soi, ou d'appartenance à un groupe social favorisent la désinformation, c'est un remède à l'incertitude.

Le contexte socioculturel, le manque de confiance dans les institutions et la corruption, la méfiance et le ressentiment envers les politiciens, les médias ou les experts peuvent être des vecteurs favorisant la désinformation.

*Le Figaro le 07/01/2018

2.2 CONSÉQUENCES

Les fake news ont un effet sur la démocratie, la santé, l'environnement, la politique, les sciences mais ont aussi un impact économique.

On a encore trop tendance à l'oublier. Les pertes dues à la désinformation peuvent être directes, d'une part et indirectes d'autre part.

IMPACT INDIRECT

- La prolifération de fausses nouvelles peut avoir un impact politique et ternir l'image d'un partie, d'un candidat.
- Au niveau militaire, elles créent la confusion et bloquent les décisions de l'adversaire.
- Sur le plan social, elles peuvent entrainer des polémiques voire des cas de violences. C'était le cas lors du mouvement QAnon au Capitole.
- Au niveau individuel, elles vont avoir un impact sur les émotions : comme la peur, le dégoût, l'angoisse, l'anxiété. Elles peuvent même entraîner un accroissement des divisions socioculturelles, voire la recrudescence de comportements à risque. L'exemple des fausses informations qui circulaient lors de la pandémie le prouve.
- Au niveau institutionnel, la recrudescence de vraies informations combinées à de fausses informations va provoquer la confusion et la perte de confiance dans certaines institutions politiques, médiatiques, ou sociales. «89% des Français considèrent que les fakes news peuvent avoir un effet important sur la renommée d'une société ou d'une marque»*.
- Quand un fake new touche une entreprise, on constate une baisse de l'innovation, un impact sur la réputation. (Par exemple, Starbucks a dû démentir la campagne «Dreamer Day» qui annonçait offrir des boissons à prix réduit aux immigrants sans papiers**).

IMPACT DIRECT

La création de fake news est tout aussi importante. Entre avril et juin 2020, Facebook a révélé 98 millions de posts contenant des fausses informations rien que sur le Covid***. Selon l'université de Baltimore, cette prolifération de fausses informations aurait coûté 78 milliards d'euros aux entreprises en 2019. Elles étaient estimées en 2018 à 100 milliards de dollars de dommages par an dans le monde selon une étude menée par Princeton toujours****.

* Viavoice pour Syntec Conseil en Relations Publics-2021 ** https://www.teenvogue.com/story/starbucks-dreamer-day-campaign-hoax *** Capital, Fake news : quel est le coût caché des intox et du complot pour la France ?
**** Étude Princeton- Andrew M. Guess, Brendan Nyhan et Jason Reifler, Exposure to untrustworthy websites in the 2016 U.S. election.2018

L'acquisition d'information est donc coûteuse à la fois en termes comptable et en termes d'opportunités. Pour diffuser une information, il faut comptabiliser le coût pour identifier la source, la vérifier, et enfin la diffuser. Ce temps de vérification coûte. Rappelons que nous vivons dans une société où le temps c'est de l'argent. Certains médias préfèreront valider une information fausse que prendre le temps de la contrôler.

Nous l'avons vu dans un exemple précèdent, la désinformation n'épargne pas les entreprises. Par exemple, une grande entreprise a été victime de fake news annonçant le licenciement de son directeur financier. Ce qui a entraîné une baisse de cours de Bourse de près de 20% en quelques minutes.

On le voit les entreprises, les politiques, les médias… personne n'échappe aux fakes news, mais alors comment peut-on expliquer une telle recrudescence ?

2.3. COMMENT SE NOURRIT CETTE NOUVELLE GUERRE ?

Les fausses informations se nourrissent d'un écosystème et arrivent à se financer facilement. Il existe désormais un environnement culturel qui s'est bâti et qui alimente les fausses informations. Afin de répondre à ces objectifs tactiques et stratégiques, les États ou les pirates informatiques, vont se servir de cette nouvelle forme de guerre, dans le but de déstabiliser une population voire un pays entier, le tout avec beaucoup de discrétion. Ces campagnes peuvent être préparées sur du plus ou moins long terme. Essayons donc de comprendre leur fonctionnement.

LES FACTEURS SOCIAUX

TECHNIQUE DE MANIPULATION DE MASSE

Il existe une multitude de manœuvres de manipulation de masse. Chomsky, comme Sylvain Timsit* en ont étudié quelques-unes. Timsit a mis en exergue 10 stratégies de manipulation pour contrôler la société (par exemple : le fait de détourner l'attention du public sur un problème majeur, faire accepter une décision en l'appliquant progressivement, de créer des problèmes, puis offrir des solutions…).

> « À la guerre, la vérité est une chose si précieuse qu'elle doit être entourée d'un rempart de mensonges ». - Winston Churchill

Dans l'histoire de la guerre on parlait de simulation, de dissimulation, ou déception (qui est « le travestissement volontaire de la réalité dans le but de gagner un avantage compétitif »)**, d'intoxication (qui consiste à déstabiliser un adversaire en lui fournissant de fausses informations.). Nous avons fait le choix d'aborder d'autres techniques, que l'on vous présente ci-dessous.

COMMENT SE PROPAGE LA GUERRE COGNITIVE ?

Astroturfing	Manipulation de l'opinion dont le but est de faire croire à l'émergence d'un mouvement populaire.
Trolling	Relaie et amplifie une information. Peut même menacer.
Stalking	Harcèlement, traque sur Internet.
Hacking	Vol par intrusion d'information.
Outing	Révélation par un tiers de l'orientation sexuelle d'une personne, sans son accord.
Fake News	Informations falsifiées. Détournement de l'information.
Sponsoring	Exploitation des megadonnées permettant aux institutions et aux états de mieux connaître nos informations et de les utiliser pour modifier notre façon de penser.
DDOS	Méthode qui vise à rendre un serveur empêchant l'accès à une plateforme ou à un site de fonctionner.

*Sylvain Timsit- Les 10 stratégies de manipulation de masse- 2002 ** Rémy Hémez, « Opérations de déception – Repenser la ruse au xxie siècle », Études de l'IFRI, juin 2018

L'INTELLIGENCE ARTIFICIELLE

Ces méthodes peuvent s'appuyer sur l'intelligence artificielle qui va simuler un comportement authentique, créer l'impression d'une opinion majoritaire, ou encore analyser les comportements des utilisateurs.

N'avez-vous pas reçu sur votre smartphone, à la suite de la consultation du dernier modèle de téléviseur sur Internet, toute une série de publicités sur différents téléviseurs sur le marché ? Votre plateforme de réseau social, elle, sait que vous cherchez à vous meubler et elle va vous encourager à faire l'acquisition de produits que vous n'auriez pas acheté sans son insistance. On parle d'une forme de chambre d'écho. Il s'agit de « dispositifs de personnalisation des contenus en ligne et auraient pour conséquence d'isoler intellectuellement les internautes et de réduire la diversité des informations auxquelles ils sont exposés (Eli Pariser, The Filter Bubble: What the Internet is Hiding from You, Penguin Press, 2011) ».*

Les médias sociaux conservent la trace de nos intérêts. Qu'en est-il de nos fréquentations ? De nos opinions ? Des articles de presse recommandés pour notre lecture ? N'avez-vous pas l'impression que votre tablette, votre téléphone, votre ordinateur, vous connaissent mieux que vous ne vous connaissez vous-même ?

LA SOURCE D'INFORMATION

Les fausses informations constituent un réel enjeu pouvant à la fois être utilisées dans le cadre de désinformation, ou dans le but d'augmenter le trafic d'un article. De façon générale, la guerre psychologique va s'appuyer sur les réseaux sociaux pour toucher tout type de population.

LinkedIn est envahi par les faux profils. Des attaquants de Corée du Nord, début 2021, ont créé de faux comptes prétextant offrir des voyages d'affaires ou des invitations à des conférences dans le but de récupérer des informations confidentielles. D'autres histoires similaires fleurissent dans l'actualité cyber. De faux profils avec de fausses photos (crée par l'IA) sont typiquement employés dans les opérations d'espionnage d'ailleurs, le cas d'une affaire révélée par le magazine Capital** (à la suite d'investigations du service de renseignement allemand) le prouve. La Chine avait utilisé ce même réseau pour espionner plus de 10 000 personnes, en créant de faux profils divers et variés (consultant, chef de projet, etc.). Il s'agissait en fait des services secrets chinois qui ont pu ainsi récupérer des informations sur les habitudes des utilisateurs, les centres d'intérêts et les opinions politiques des internautes.

*Fondation DESCARTES **Capital - décembre 2017

En définitive, la source d'information fournit d'importants indices sociaux qui influencent la formation des croyances. Les gens feront plus confiance aux sources d'information qu'ils perçoivent comme plus attrayantes, puissantes et en accord avec ce qu'ils sont. Les valeurs personnelles ou morales auront plus de poids que des preuves objectives dans la formation d'une opinion. Malheureusement, le lecteur a tendance à ne pas tenir compte de la qualité du média ou même de la source d'information.

LES FACTEURS COGNITIFS

LES BIAIS COGNITIFS (nous croyons que ce que nous voyons)

Toutes ces méthodes, utilisées dans le cadre de la guerre psychologique, amoindrissent nos capacités cognitives et renforcent les biais cognitifs qui nous dirigent tous et nous amènent à prendre de mauvaises décisions. Beaucoup de ces biais sont exploités par les attaquants ou les États à des fins d'endoctrinement, de propagande, de manipulation. Ces biais ont pour effet de dégrader l'information. On peut citer parmi les nombreux biais (plus de 200 référencés) :

- Le **biais de confirmation**, qui est la tendance à sélectionner uniquement les informations qui confirment des croyances ou des idées préexistantes. Ceci afin d'éviter tout inconfort psychologique.
- Le **biais de simple exposition** consiste lui à penser que si l'information est véhiculée par tout le monde c'est qu'elle est forcément juste.
- L'**effet d'ancrage** est la tendance à surévaluer un critère dans un choix et à négliger les autres. Les moteurs de recherches, les réseaux sociaux fonctionnent selon des algorithmes qui profitent de ces biais.
- L'**effet de l'influence** continue. Si une personne apprend qu'une information, qu'il pensait vraie initialement s'avère fausse, alors elle continuera à croire cette information. L'information discréditée continue d'influencer le raisonnement.

Même les robots sont victimes de biais, cela a été le cas du petit dernier de Google nommé Tay*, accusé de complotisme et de négationnisme, quelques heures après sa naissance.

L'ENCODAGE

À l'instar des biais cognitifs, un autre facteur va avoir une incidence sur la perception de l'information, il s'agit de l'encodage. Lorsque des informations sont encodées dans la mémoire, et que nous intégrons de nouvelles informations qui vont à l'encontre de l'information mentionnée, alors ces nouvelles données sont momentanément remplacées mais ne seront jamais effacées et seront fort probablement récupérées plus tard.

* Siècle digital-Intelligence artificielle : quelle approche des biais algorithmiques ? - mai 2021

Une théorie basée sur l'étude de Kahneman et Tversky, selon laquelle l'humain raisonne à partir de deux systèmes : le système 1 (rapide et intuitif) et le système 2 (analytique) a été reprise par des chercheurs en psychologie que l'on retrouve dans la revue Judgment and Decision Making en 2021. Ils avancent que dans le système 2, il existerait un sous-système dit « motivé » ou système de raisonnement (SR2M). Les personnes ayant une bonne capacité à mobiliser leur raisonnement analytique (CRT) distingueraient mieux les vraies des fausses informations. Selon eux « plus les personnes pensaient analytiquement, plus elles avaient tendance à accepter ce qui allait dans leur sens, et rejeter ce qui les contrariait. » Cette étude fait l'objet de controverse, car il faut bien distinguer la détection de la fausse information et le ralliement à la désinformation ou encore ce que pense les personnes et la façon dont chacun pense. Autre élément constaté, les personnes avec un score élevé au CRT auraient tendance à partager beaucoup moins de fausses informations. Bien sûr toutes ces nouvelles théories restent encore trop récentes et nécessitent des preuves empiriques pour soutenir leur existence.

LES ÉMOTIONS

« Une abondance de l'information crée une rareté de l'attention ».
- Herbet Simon

On reçoit une grande quantité d'informations dans un temps record, souvent peu contextualisées, sans nuance, sans réelle source… Et si en plus on y ajoute des images chocs, alors la manipulation est totale ! L'information va circuler très vite, être relayée sans aucune forme de contrôle…Les infox se diffusent « plus vite, plus profondément et plus largement » que les vraies*. Nous aurons tendance à suivre notre « instinct » plutôt que de délibérer ou de remettre en question l'information.
Comment ne pas s'y perdre ? Comment bien interpréter ? On doit penser vite, réagir vite, et on se fait happer par le système. On clique, on achète, on vote !

Les attaquants l'ont compris et vont faire appel à l'émotionnel, plutôt qu'à la réflexion. Ce sont les émotions qui guident nos décisions, nos ressentis et pilotent notre jugement. Les réseaux sociaux, entres autres, vont perturber notre raisonnement en agissant sur notre impulsivité cognitive (le sentiment permanent d'urgence, le manque de planification, le manque de persévérance, la recherche de sensations). La guerre psychologique s'appuie sur : l'insolite, l'humour, la peur.

*Gérald Bronner - Apocalypse cognitive - janvier 2021

3. TYPE D'INGÉRENCE À TRAVERS LE MONDE

Toutes les grandes puissances sont dotées d'unités dédiées à la désinformation.

3.1. LE MONDE CYBER ET LA GUERRE PSYCHOLOGIQUE

Les Etats aujourd'hui n'hésitent pas à utiliser l'arme psychologique dans leurs attaques cyber. Et les superpuissances comme la Chine, les États-Unis et la Russie ont mis en œuvre des stratégies d'influence impressionnantes. On pourrait en citer d'autres…

LA STRATÉGIE RUSSE : LA CLANDESTINITÉ

La manipulation de l'information fait partie intégrante de la doctrine militaire russe, qui comprend d'ailleurs une division officielle de la désinformation. Le but de ces organes est de réduire la confiance dans « les sources du savoir ». On ne peut pas cacher que la Russie est l'un des acteurs les plus actifs dans ce domaine.

D'ailleurs, les Etats européens en ont été la cible. Les fausses informations ont toujours circulé. Les Etats Unis également, pour preuve, on peut citer les opérations de manipulation de l'information lors de l'élection de Donald Trump ou la diffusion des données du QG de campagne des démocrates de Hillary Clinton.

Depuis de très nombreuses années, la Russie invente, crée un ensemble d'informations mensongères que ces organisations comme l'IRA (Internet Research Agency) diffuse.

Moscou est régulièrement accusée de manipuler les opinions et de faire usage de désinformation. Dans le contexte du conflit russo-ukrainien, la Russie menace notamment les journalistes de 15 ans de prison en cas de publications qui vont à l'encontre du pouvoir en place. Autre fait, le Conseil de sécurité de l'ONU a été le théâtre, en mars 2022, d'un « combat » de désinformation et de manipulation entre l'Occident et la Russie, Moscou accusant Kiev de fabriquer des armes chimiques. Rien ne permet actuellement d'affirmer ces propos.

Un pays utilisant la théorie du complot n'est pas nouveau. En 2018, la Russie avait déjà accusé les États-Unis de mener secrètement des expérimentations biologiques dans un laboratoire de Géorgie. En temps de guerre les nations se livrent bien souvent à des campagnes de désinformation pour couvrir les opérations militaires.

De nombreux organes d'influence sont très présents sur le sol Russe.

- L'unité 54777 (appartenant au GRU) est en charge des opérations de « guerre psychologique ». De nombreux groupes Russes sont connus pour user de la manipulation. Cozy Bear (APT 29), Turla, le groupe Fancy Bear (l'unité 26615) est connu pour mettre en application ces techniques de manipulation. Il est d'ailleurs l'auteur de l'attaque de la chaine de TV5 Monde, les MacronLeaks de 2017. Il a également été accusé d'interférence dans le processus électoral américain de 2016. Fancy Bear associé à Sandworm Team (l'unité 74455 du GRU) a été impliqué dans l'affaire des « DNC Leaks ». De nombreux groupes sont d'ailleurs visés par la justice américaine, pour exemple, le ministère américain de la Justice (DOJ) a condamné le Russe : Aleksandr Zhukov, pour stratagème de Methbot. Il s'agit de robots qui génèrent de faux trafic vers les sites, créant ainsi de fausses impressions sur les publicités.

- Au-delà de ces groupes qui mènent la vie durent à de nombreux organismes, la Russie a même créé son usine à Troll : L'Internet Research Agency (IRA), fondée par Evgueni Prigojine. Cette organisation existe depuis 2013. Elle est constituée d'informaticiens, journalistes, bloggeurs, dont leurs rôle est de promouvoir le discours du pouvoir en place. Ces personnes ont eu un poids prépondérant dans le piratage des élections américaines et ont été accusés d'ingérence dans d'autres pays.

- La Russie s'arme également de trickster. Un trickster symbolise un personnage dont sa caractéristique est de duper, de tricher. Ces tricksters sont généralement présents au sein des institutions afin de les subvertir.

À présent déplaçons nous en Biélorussie, pour évoquer une campagne qui a fait grand bruit dans le domaine cyber : la campagne ghostwritter. Entre 2017 et 2020, des hackers ont mené une campagne de désinformation massive, de piratage de sites d'information, dans le but de discréditer l'OTAN. Au départ attribué à un groupe Russe, il semblerait qu'elle provienne de UNC1151, groupe Biélorusse. Quatorze personnalités se sont fait passer pour de faux journalistes et analystes afin d'exploiter des compromis de sites Web ou des comptes de messagerie falsifiés pour diffuser de faux contenus y compris des articles de presse falsifiés. La particularité de cette campagne réside dans le fait que la désinformation ne se propage pas via les réseaux sociaux, mais en abusant des systèmes de gestion de contenu (CMS).

LA CHINE MISE SUR LA PROPAGANDE

Le pouvoir chinois semble de plus en plus verrouiller la circulation de l'information. L'empire du milieu fait figure d'élève studieux et ambitieux en matière de désinformation. En plus d'employer des millions de personnes pour protéger son image sur Internet, elle déploie une communication de démenti automatique. Ainsi, certaines fermes à trolls ont recours à l'intelligence artificielle pour générer du contenu. Le régime chinois a toujours mis en œuvre une stratégie de propagande numérique redoutable et colossale.

Le rapport de l'IRSEM* intitulé « Les Opérations d'influence chinoises, un moment machiavélien » atteste de l'existence de ce corpuscule employé par la propagande chinoise. Plusieurs faits confirment l'influence à la fois au niveau national et au niveau international. Le rapport révèle l'existence notamment de la ferme KanWatch, il s'agit de pigistes payés pour créer des contenus viraux.

La Chine axe son combat sur trois guerres (la base 311 est dédiée à ces trois guerres**) : la guerre de l'opinion publique, la guerre du droit, la guerre psychologique. Ainsi, on constate un renforcement des opérations d'influence, on en veut pour preuve :

- De très nombreux sites sont désormais bloqués : Twitter, Facebook, YouTube, Instagram, et les médias sinophones à l'étranger sont contrôlés.
- Internet est sous la juridiction de la souveraineté chinoise.
- Le gouvernement a mis en place un texte de loi, imposant un système de classification du risque, qui renforce le contrôle des transferts de données à l'étranger. Le gouvernement entend ainsi éviter que toutes informations sensibles ne soient accessibles aux puissances étrangères.
- L'État maitrise les informations entrantes et sortantes. Selon un rapport de l'IRSEM*** datant de 2021, la Chine s'inspire du modèle russe, en payant plus de 2 millions de citoyens chinois pour relayer la propagande de Pékin. On les surnomme « l'armée des 50 centimes », car chacun serait rémunéré 0,5 yuan par post.
- L'éducation est également visée. Les universités en Chine sont dépendantes financièrement du gouvernement chinois. Ce dernier peut ainsi surveiller les contenus, les évènements et les matériels.
- Le pays ne s'arrête pas là, puisqu'il a mis également en place un département de propagande afin de contrôler les médias.****

Pour illustrer cette mainmise sur l'information, la dernière application ZAO, illustre le danger d'une application deepfake virale chinoise. Cette dernière demande à l'utilisateur d'enregistrer votre visage, au risque de vous faire apparaître dans des situations fausses mais tout à fait crédibles. Cette technologie peut mettre en danger la sécurité nationale. Aussi, le gouvernement a récemment mis en place une loi pour que la publication d'un deepfake soit considérée comme une infraction criminelle.

*Paul Charon et Jean-Baptiste Jeangène Vilmer, « Les Opérations d'influence chinoises, un moment machiavélien » IRSEM. ** Les opérations d'influence chinoises. Un moment machiavélien ; Paul CHARON et Jean Baptiste JEANGENE VILMER - 2021
Institut de Recherche Stratégique de l'École Militaire * Département du Travail de Front uni (DTFU), Liaisons internationales (DLI), Bureau 610.

- Ajoutons encore le China Brain Project, le projet de 15 ans « destiné à la recherche sur les bases neurales de la fonction cognitive »* inquiète les États-Unis entres autres. Même si ce projet s'est terminé en 2020, le pays continue à travailler sur une interface homme-machine, où l'information du cerveau est transmise sur un ordinateur à distance connecté à internet. Cette innovation serait utile à la médecine mais pourrait être utilisée pour d'autres secteurs et servir cette nouvelle guerre de l'information**. Même si ce procédé n'est pas encore en circulation, il mérite de se poser quelques questions.

- Au niveau étatique toujours, le ministère de la Sécurité d'État (MSE) : l'agence civile de renseignement, et le bureau des Affaires taïwanaises (BAT) qui assure la propagande à destination de Taïwan sont engagés dans les opérations d'influence.

- Pour illustrer l'influence des groupes cyber, APT 31 (Zirconium, Judgement panda, Bronze Vinewood) s'est fait passer pour McAfee dans le but d'ébranler la campagne politique du candidat américain Joe Biden. Ce même groupe est dans le scope des agences de renseignements françaises.

- L'opération « Dragon Spamouflage » de 2019-2020 est une campagne de propagande pro-Chine sur les médias sociaux. Cette campagne visait à créer de faux « followers » via l'IA, attaquant la politique américaine.

- Autre campagne d'amplification***, l'opération « Wilson Edwards », il s'agit d'une campagne de désinformation orchestrée par le gouvernement chinois faisant pression sur l'Organisation mondiale de la santé (OMS), le texte dirait que "les Etats-Unis font pression sur l'organisation afin qu'elle désigne le laboratoire de Wuhan comme responsable de la pandémie".

LES ÉTATS-UNIS ET LE MONOPOLE DE LA COMMUNICATION

Les États-Unis ont le monopole des vecteurs de communication, Facebook, Twitter, Google, WhatsApp qui sont les relais parfaits pour distiller de la bonne ou de la mauvaise information.

L'implication de Cambridge Analytica dans les élections présidentielles américaines de 2016 illustre bien l'ingérence des sociétés américaines dans la politique. Rappelons que, dans cette affaire, des profils psychologiques particuliers d'utilisateurs étaient ciblés via des publicités, dont certaines « fake news », afin de les inciter au vote. À la suite de cela, lors du vote pour le Brexit, Meta a informé ne plus permettre aux annonceurs de faire de la publicité ciblée en se servant de certaines données « sensibles ».

Un autre phénomène, qui s'exporte désormais dans le monde est le nouveau mouvement complotiste QAnon, qui est apparu en 2016. La lettre Q désigne un très haut niveau d'habilitation au sein de l'administration américaine, Anon, pour anonyme. Ce relai de désinformation est né aux États-Unis et sa nouveauté réside dans l'usage du numérique pour faire irruption dans le monde réel. Ce mouvement est, entre autres, à l'origine de la manifestation au Capitole à Washington.

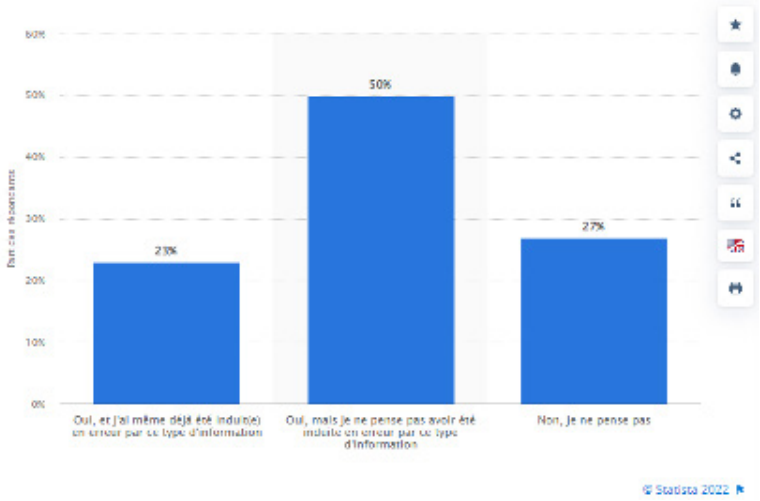
*Armée de trolls, «loups guerriers», web vitrines : plongée dans la nouvelle cyberpropagande chinoise- France Culture - 20/09/2021 **China Brain Project: Basic Neuroscience, Brain Diseases, and Brain-Inspired Computing, Mu-ming Poo, 2016
***Un faux utilisateur publie un message, relayé par des de faux comptes. Plus l'information est diffusée, plus elle a de chance d'être repérée.

Le groupe pro Trump « Stop the Steal », apparu en novembre 2020, a réussi à mettre le chaos, simplement en publiant un communiqué contestant l'élection de Biden. Facebook a dû réagir afin de contrer la propagande de la désinformation. En une seule journée, ce groupe a obtenu 360 000 membres.

EN FRANCE

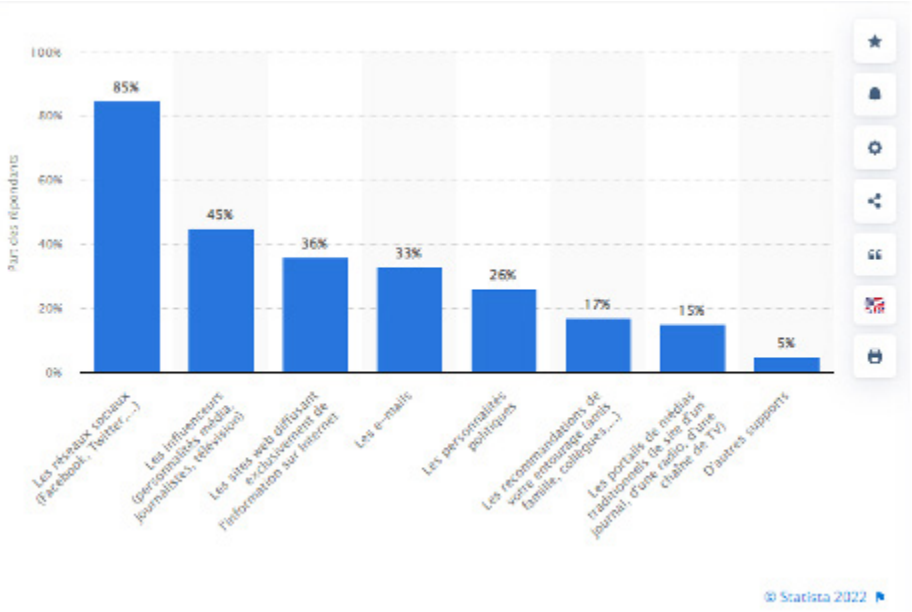
La France aussi a connu le mouvement QAnon. On y retrouve les anti-vaccins, les populistes de droite, … une population plutôt hété-roclite. Une constellation de personnalités s'est revendiquée comme porte-parole de QAnon. Sur des réseaux alternatifs, il est encore aujourd'hui difficile de mesurer l'importance du groupe. Les vidéos qui font la promotion du groupe sur YouTube font plus de 150 000 vues et leur relai sur Facebook représente 30 000 abonnés. La France n'est pas épargnée en termes de fiabilité de l'information.

À la question : "Pensez-vous avoir déjà été confronté(e) à une information fausse destinée à vous influencer ?" voici ce que l'enquête de Statista de 2022 révèle :



Selon la même source, voici les retours à la question suivante : Selon vous, à propos des informations fausses ou truquées que l'on peut trouver sur Internet, quels sont les principaux supports qui les propagent ?

*Statista 2022 - https://fr.statista.com/statistiques/827006/opinion-francais-sources-propagation-fake-news/



Dans la longue liste des tentatives d'ingérence électorale, en plus des élections visant l'état américain, la France a elle aussi était victime. « L'opération Macron Leaks » en est l'exemple le plus connue en France, où cette opération avait pour but de saper la candidature d'Emmanuel Macron. 15 giga-octets de données, dont 21 075 e-mails, ont été volés visant les ordinateurs du personnel de campagne en 2017. Cette campagne de désinformation n'a pour autant pas atteint son but, puisque les électeurs n'ont pas modifié leurs intentions de vote.

« Gagner la guerre avant la guerre » - Sun Tzu

En France, l'armée doit faire face et prendre en compte aussi ce nouvel outil non militarisé qu'est la désinformation, afin de gagner la guerre avant la guerre. La stratégie militaire passe par l'intelligence économique et ses capacités d'influence. On parle désormais de guerre d'influence. L'affaire des faux comptes Facebook de l'armée française au Mali est un parfait exemple. Le cabinet Graphica a révélé la publication de fausses informations et caricatures liées à l'armée française contre l'Etat Russe. Des pro-Français et des pro-Russes se seraient battus sur le front d'une guerre d'influence numérique. Aucune des deux parties ne confirme ou ne dément. Cette campagne a bien évidemment nui à la réputation de l'armée française au Sahel.

Le domaine informationnel peut réellement influencer un théâtre d'opération, déstabiliser les adversaires et être un levier de manipulation.

3.2 ET DEMAIN ?

Le cyber espace évolue vite, très vite, et même si la notion de guerre psychologique et les opérations d'influence sont aussi anciennes que la guerre, elles restent toujours d'actualité. En temps de guerre, les opérations psychologiques (PSYOPS) étaient beaucoup employées. Il s'agissait d'actions d'influence dans le but d'éroder la capacité de l'opposant en distillant de fausses informations, en semant la terreur. L'OTAN défini cette notion comme « ensemble d'activités destinées à modifier le comportement et les attitudes d'individus ou de groupes humains hostiles, neutres ou amicaux, en vue de contribuer à l'atteinte d'objectifs politiques ou militaires »*. Encore aujourd'hui de nombreux États ont des unités spéciales dédiées à influencer les comportements en utilisant des méthodes psychologiques.

Cette méthode ne commence à apparaître dans le monde cyber que depuis quelques années. Nous venons d'en évoquer quelques exemples.

L'OTAN, elle-même ajoute désormais, l'aspect psychologique, à ces 5 domaines opérationnels (air, terre, mer, espace et cyberespace) et déclare que : « L'humain représente très souvent la première des vulnérabilités, et il convient de le reconnaître afin de protéger le capital humain de l'OTAN, et aussi de tirer parti des vulnérabilités de nos adversaires ». Par ailleurs, nous l'avons vu, l'IA va faire accélérer l'usage de cette nouvelle arme, qu'est la guerre non matérielle en créant, améliorant des outils de cyber-influence. Ces outils sont désormais utilisés dans le monde du renseignement, des médias.

> « Ne croyez rien de ce que vous entendez, et seulement la moitié de ce que vous voyez. » - Edgar Allan Poe

Nous avons vu plus haut toute une série de méthodes utilisées pour manipuler les foules. Le plus populaire est le deepfake. Cette technique de modification des contenus ne cesse de s'améliorer. Elle propose désormais des solutions pour faire prononcer un discours par une voix virtuelle ou bien de retoucher des vidéos pour renforcer la crédibilité d'un montage vidéo.

*NATO/NSA, 2005

Il s'agit là de modification d'image, de fabrication de documents destinés à tromper, duper une cible ou semer le doute dans les esprits ou encore usurper l'identité d'une personnalité connue, ou inconnue. On parle de Phishing, par mail ou de Vishing. Nos partenaires Proofpoint définissent le vishing comme « une attaque où les cybercriminels utilisent des numéros de téléphone frauduleux, des logiciels de modification de la voix, des messages texte et des techniques d'ingénierie sociale pour inciter les utilisateurs à divulguer des informations sensibles. Le vishing utilise généralement la voix pour tromper les utilisateurs. »

Les cybers attaquants vont tout faire pour jouer sur les émotions en perturbant la capacité de jugement. Ils peuvent demander à donner de l'argent ou de communiquer des informations personnelles. Ils vont jouer sur le caractère urgent
Parmi les exemples de fraudes on peut trouver :

- Les compromissions des comptes bancaires, les escrocs contactent leurs victimes pour les informer que leur compte en banque a été compromis et qu'il pourrait être la cible d'une cyberattaque.
- L'escroc prétendant être un employé des impôts
- Fraude à l'assurance, les personnes victimes sont souvent les personnes âgées

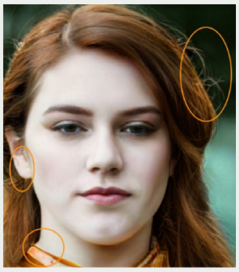
Il en existe beaucoup d'autres, encore plus réalistes. C'est ce qui est arrivé à un directeur de banque qui a autorisé une opération de virement de 35 millions de dollar, pensant que la demande émanait de son PDG. Il s'agissait en fait d'un algorithme d'apprentissage automatique (MLA), qui se faisait passer pour la voix de son patron.

On repense aussi à la vidéo de Barak Obama, et son discours un peu « atypique ». Le deepfake permet de faire dire ce que l'on veut à qui l'on veut. Certes tout n'est pas parfait, mais la technique s'améliore de jour en jour. Selon une étude* « près de 50% des Américains pourraient être convaincus de la véracité d'un faux scandale qui leur est présenté par une vidéo truquée. ».

Jusqu'ici l'imitation de la voix était médiocre, et pourtant tout dernièrement une société ukrainienne : Respeecher, a fait la une des journaux avec son clonage vocal de Richard Nixon. Elle a même été récompensée aux Emmy Awards, rien que ça ! Le clonage passe par une phase d'apprentissage et l'intelligence artificielle fait le reste. De telles avancées font froid dans le dos, imaginez jusqu'où cela pourrait aller ? Aussi les défenseurs tentent de trouver les solutions pour déjouer ce nouveau fléau et détecter ces trucages.

*Soubhik Barari-Christopher Lucas-Kevin Munger - Political Deepfakes Are As Credible As Other Fake-Media And (Sometimes) Real Media - 2021

Le jeu est d'identifier quelle est la photo issue de l'IA. L'application à une fonction pédagogique et de sensibilisation.



Le faux visage ici était celui-ci : les pixels ne sont pas alignés.

Avez-vous déjà entendu parler de eye tracking ? La technologie a toujours un temps d'avance et elle le prouve encore, avec cette nouvelle technologie. Elle permet de produire une carte visuelle de la façon dont la personne voit une scène, on obtient ainsi un aperçu des comportements que nous adoptons instinctivement. Outre le domaine de la santé, le suivi oculaire peut fournir des informations détaillées sur les comportements des consommateurs, les processus de prise de décision et ainsi être utilisé à mauvais escient.

Finissons ce chapitre par une note positive. Pensons que ces mêmes technologies peuvent être utilisées afin de contrer ces manipulations que nous subissons au quotidien. L'IA peut être une arme afin de détecter les tentatives d'intrusion, de manipulation.

4. GUERRE PSYCHOLOGIQUE : COMMENT SE PROTEGER ?

4.1. DES SOLUTIONS TECHNOLOGIQUES

Parmi les solutions pour lutter contre les cyber attaques et détecter ces nouvelles menaces, TEHTRIS propose la XDR Platform qui classifie les menaces grâce à l'IA, et permet un contrôle en temps réel et de façon hyper automatisé. Aujourd'hui notre offre Cyberia permet de prétraiter les alertes, et d'ouvrir automatiquement des tickets. Imaginons demain cette même technologie pour lutter contre les campagnes de désinformation.

L'APPRENTISSAGE AUTOMATIQUE

L'IA et l'apprentissage automatique peuvent donc être des atouts dans la lutte contre les fake news, en repérant les nouvelles campagnes. De la même façon qu'il existe un suivi d'alerte d'incident, il pourrait être pertinent d'avoir un suivi d'alerte de guerre cognitive. Ce système permettrait de détecter et d'alerter sur les campagnes en cours.

Twitter a ajouté par exemple dans son arsenal de détection, un outil permettant d'identifier les publications qui font débat et alerte les internautes. L'entreprise a par exemple mis en place l'application Birdwatch, cette fonctionnalité participe à la lutte contre la désinformation, en signalant des tweets litigieux. En 2017, 15% des comptes Twitter étaient des bots, ces derniers jouent un rôle majeur dans la désinformation*.

Autres initiatives : WeVerify et InVID ont été financés par l'Union Européenne afin de détecter les deepfakes. Il existe également des outils permettant de repérer les fausses informations, comme Fakey, Hoaxy.

On observe en parallèle de plus en plus dans les journaux télévisés notamment, apparaitre le Fact checking, ou vérification des faits. Cela consiste à vérifier la véracité de propos tenus par des responsables politiques ou d'autres personnalités publiques. Facebook collabore avec plus de quatre-vingts organismes de fact-checking pour éviter la désinformation et 15 000 personnes sont dédiées à la modération de contenu.

Lié à l'intérêt porté aux questions de sécurité en temps d'élection, un système de vérification des faits en temps réel pour la campagne électorale avait également été développé en 2020 aux États-Unis par des chercheurs de l'‘université de Duke. Cet outil est accessible via une application mobile, et repère des phrases clés, qui sont comparées avec une base de données et vérifiées, permettant ainsi de détecter des infox. Un message est ensuite renvoyé sur le mobile indiquant si l'‘information est fausse ou pas. L'application renvoie enfin vers un site Internet.

*Données OSoME - Observatoire des médias sociaux de l'université de l'Indiana à Bloomington

LA SOUVERAINETÉ

Nous avons vu que nos données peuvent être exploitées à des fins d'espionnage favorisées par les deep fake. Les réseaux sociaux et plus globalement les GAFAM ont un rôle à jouer dans la régulation des contenus. Mais jusqu'où peut-on leur faire confiance ? La commercialisation de nos données personnelles engendre des profits colossaux auprès des géantes de la Tech. Aussi, autant que possible, il est important d'avoir comme système de protection des solutions souveraines. C'est le cas des solutions proposées par TEHTRIS. Assurons-nous au maximum que nos données restent en France et en Europe.

OUTILS DE DETECTION DES MENACES

La technologie présente en soi des vertus pour contrer les fausses informations, mais il ne faut pas s'arrêter là. Connaitre son ennemi constitue aussi un moyen de se protéger, il est donc important de bien maîtriser les tactiques qui sont utilisées par les attaquants pour transmettre cette information, et de connaitre également les cibles et les victimes. Une bonne CTI permettra d'anticiper cette menace. TEHTRIS grâce à son équipe de CTI apporte cette brique supplémentaire qui permet d'identifier, les futures tactiques et menaces, sources de désinformation. Tous ces éléments vont servir de base au phishing, le premier vecteur utilisé pour la désinformation. TEHTRIS offre cette protection non seulement avec ses propres produits comme l'est la technologie EDR (https://tehtris.com/fr/produits/edr-endpoint-detection-response/) et aussi grâce à son partenariat avec Proofpoint (https://tehtris.com/fr/partenaires/technologie/eco-system-by-tehtris/)

Le développement de toute cette technologie permet de détecter les fausses informations, les algorithmes deviennent de plus en plus performants ; en supplément il faut ajouter à son arsenal de sécurité des solutions dites immatérielles.

4.2. DES SOLUTIONS IMMATERIELLES

PRISE DE CONSCIENCE

Nous devons tous être conscient que la guerre cyber ne se fait pas qu'à travers le matériel, elle s'appuie aussi sur l'immatériel et nous sommes tous concernés. L'accessibilité des médias sociaux permet à l'adversaire de cibler chacun d'entre nous et de nous proposer des informations, des produits, en fonction de nos intérêts, dans le but de nous manipuler et de nous faire prendre des décisions. Nous devons être conscients de cela et en conséquence avoir une bonne hygiène cyber.

Elle passe par :

- La vigilance et la sensibilisation.
- L'investissement dans l'éducation pour renforcer la vigilance et la maîtrise de la désinformation dans les écoles. Expliquer la démarche d'investigation, observer la manière dont un énoncé est présenté, etc., permettrait de mieux identifier une fausse information. L'Estonie est très active sur ce sujet et a lancé son Global Hack. 1 million de participants ont pu échanger en ligne et trouver des solutions pour freiner la propagation de fake news sur le coronavirus.
- L'encouragement à garder un esprit critique, à croiser les sources, à privilégier les sources d'informations reconnues et à s'assurer de l'indépendance de ces sources. Toujours garder à l'esprit qu'il peut y avoir une une violation. Observer les détails. Le concept zéro trust, zéro confiance s'applique aussi ici. Il faut se rappeler qu'une information doit être factuelle et vérifiée.
- L'interrogation. Il faut amener les personnes à se poser des questions en leur demandant de s'expliquer sur le « pourquoi », le « comment » telle information leur semble exacte ou pas.
- Une représentation claire et le plus simple possible. Un langage simple et des graphiques informatifs facilitent la révision des connaissances. Il est préférable de privilégier un langage compris par tous, à un langage trop expert.
- Une formation ou une sensibilisation aux biais cognitifs, être conscients de nos vulnérabilités, à la manipulation de façon générale. Gardez l'œil !
- Une approche préventive : le prebunking ou « inoculation psychologique » Cela peut être une première ligne de défense. C'est « le processus de démystification des mensonges, des tactiques ou des sources avant qu'ils ne frappent ». dont le but est de faire en sorte que « les croyances initiales fortes sont plus efficacement immunisées contre la persuasion en les préexposant à des contre-arguments »*. Cette solution permet de devancer la désinformation, en favorisant par exemple l'exposition des personnes à des arguments contrant les éventuels fakes news ou complots.
- Une approche Réactive : le debunking. Il s'agit de démystifier, de discréditer une fausse information. Cela se fait en vérifiant les sources, en consultant des sources alternatives, en prenant directement contact avec la source initiale.

*Papageorgis, D., & McGuire, W. J. (1961). The generality of immunity to persuasion produced by pre-exposure to weakened counterarguments.

APPROCHE DU PREBUNKING

MESURES ORGANISATIONNELLES

D'autres solutions pourraient être privilégiées, elles consisteraient à freiner le développement de fausses informations en mettant en place des sanctions (si le préjudice et l'intention sont établis) pour la création et/ou la diffusion de désinformation, sans pour autant brimer la liberté d'expression ou favoriser la censure.

Aujourd'hui les États, les gouvernements, les institutions ont pris la mesure du problème et agissent. Voici quelques exemples d'actions prises.

Des organismes ont vu le jour afin de nous éclairer. C'est le cas de :

- L'EGE (Ecole de Guerre Economique) qui propose des webinars, des formations aux entreprises, aux RSSI, afin de rester informé sur l'actualité cyber.
- Viginum*, qui est le service de vigilance et de protection contre les ingérences numériques étrangères créées en 2021. Soixante-dix personnes (experts en réseaux sociaux, techniciens et journalistes), constituent l'équipe dont le but est de lutter contre les fausses informations sur internet, de surveiller les manipulations de l'information en provenance de pays étrangers. Trois comités seront ainsi constitués, le premier est opérationnel, afin de lutter contre la désinformation, le second est stratégique, afin de comprendre d'où vient un fake new et enfin le dernier est éthique, il concerne la liberté publique et le droit de la presse. Cette initiative est née à la suite des « Macronleaks » où des dizaines de milliers de courriers électroniques du mouvement En Marche ! d'Emmanuel Macron ont fuité.
- Les lumières à l'ère numérique, cette commission crée par Emmanuel Macron aura pour but de lutter contre les diffuseurs de haine et de la désinformation. Cette commission sera composée de chercheurs, historiens, sociologues, mais aussi de professeurs des écoles ou de juristes.
- Des initiatives comme la galerie de la Fondation EDF a même fait une exposition sur l'histoire des fausses informations (mai 2021-janvier 2022), l'objectif étant d'informer les plus jeunes sur les risques de la désinformation.

*Service de vigilance et de protection contre les ingérences numériques étrangères

- La création de groupe comme Bellingcat qui est composé de chercheurs, journalistes indépendants qui sont à l'origine d'enquêtes révélant par exemple l'identité des agents secrets russes, responsables de l'empoisonnement de Alexeï Navalny, et de l'affaire Skripal.

- Le projet MYRIADE, porté par le ministère des Armées, va également être lancé d'ici la fin de l'année 2022 afin de répondre aux questions sur les menaces cognitives.

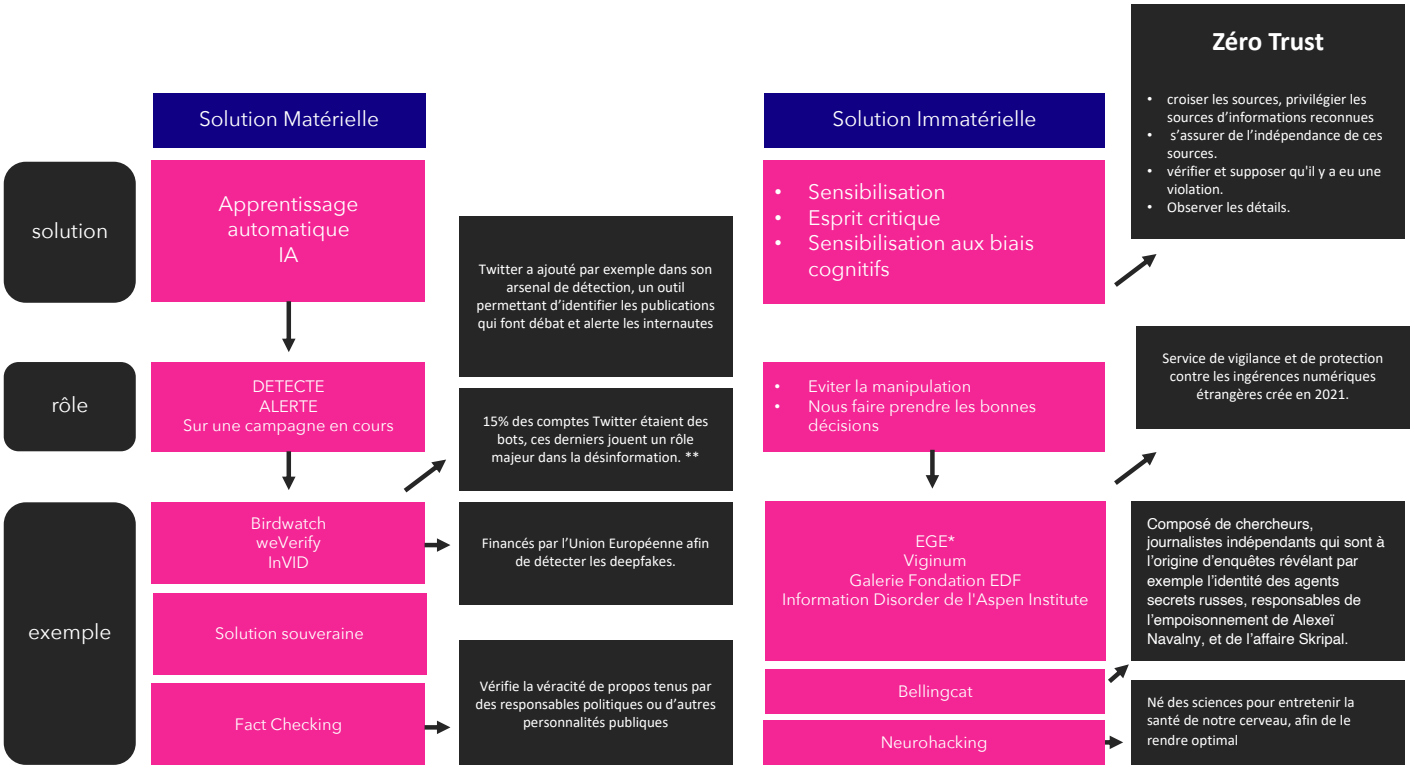
- Le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) a proposé la mise en place d'une agence nationale de lutte contre les manipulations de l'information. Une soixantaine de personnes travailleront à partir d'outils OSINT Les services de renseignement français seront mobilisés.

- Le groupe de travail East StratCom a également vu le jour. Cette task force a pour but « de développer des produits de communication et des campagnes visant à mieux expliquer les valeurs, les intérêts et les politiques de l'UE » dans les pays des Balkans. Et d'analyser les tendances de désinformation.

Sur le front de la législation aussi les lignes commencent à bouger. Le rapport de la « Commission on Information Disorder » de l'Aspen Institute, encourage les législateurs à mettre en place des lois qui rendraient les plateformes de médias sociaux plus transparentes et responsables, sous peine de sanction.

Les lois sur les fakes news sont encore beaucoup controversées. Pour plus de renseignement : https://www.justifit.fr/b/guides/droit-informatique/fake-news/

COMMENT SE PROTÉGER DE LA NOUVELLE CYBERGUERRE : LA GUERRE DE L'INFORMATION ?



*Ecole de Guerre Economique

** Données OSoMe- Observatoire des médias sociaux de l'université de l'Indiana à Bloomington

5. EST-ON PRÊT FACE À LA DÉSINFORMATION ?

Face à ce potentiel dévastateur dans le monde politique, et à quelques semaines des élections en France, on est en droit de se demander, comment on réagirait si le pays subissait une attaque de quelque nature que ce soit. Sommes-nous prêts ?

L'AFP et Google France ont anticipé en lançant un projet de lutte contre les infox appelé Objectif Désinfox, basé sur la coopération de médias et d'organisations de fact-checking. Est-ce que cela sera suffisant ? Les États ont-ils les moyens de leurs ambitions ?

Via la puissance des GAFAM, 235 millions de dollars sont réinjectés dans des sites de désinformation, tous les ans via la publicité en ligne*. L'Europe est-elle en capacité de bloquer de telles tendances ?

Les États, les gouvernements sont désormais confrontés à de nouveaux défis. L'introduction de nouvelles technologies œuvrant dans le monde cyber en est un exemple. Mais la technologie issue des media sociaux est la petite dernière, elle ouvre la voie à un nouveau terrain de combat qu'est la guerre cognitive. On parle de combat sans combat. La finalité de cette nouvelle guerre ? Manipuler, influencer les croyances et les comportements individuels et collectifs. Ce nouvel espace de compétition devient un enjeu stratégique non négligeable qui ne doit plus être subi mais au contraire maîtrisé.

Toutes les disciplines, tous les outils et techniques sont impliquées dans la guerre cognitive. La prise en compte de cette nouvelle dimension va devenir indispensable si l'on veut combattre cette nouvelle forme de manipulation dont usent les états ou les pirates informatiques.

En résumé il est important de rester neutre face à une information, au risque de voir ses propos détournés, mais aussi d'anticiper sur chaque menace et risque de désinformation, afin d'être prêt pour ne pas se laisser manipuler. Ce travail de transparence doit être un travail de chaque instant. Enfin nous l'avons vu le travail d'éducation est primordial. Une société éclairée sera moins vulnérable à des opérations de ce type.

ANNEXES

https://cf2r.org/tribune/guerre-economique-et-guerre-cognitive/
https://cf2r.org/tribune/guerre-economique-et-guerre-cognitive/
https://www.entelekheia.fr/2021/10/12/otan-la-guerre-cognitive-est-lancee-seconde-partie/
https://www.anoraa.org/articles/20995-quest-ce-que-la-guerre-hybride
https://operationnels.com/2019/08/06/quest-ce-que-la-guerre-psychologique-1-3/
https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf
https://www.dynamique-mag.com/article/fake-news-menace-entreprises.10645
https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf
https://portail-ie.fr/short/2873/lagence-nationale-de-lutte-contre-les-manipulations-de-linformation-nouvelle-arme-anti-fake-news-du-gouvernement
https://www.lesechos.fr/politique-societe/gouvernement/fake-news-la-france-se-dote-dune-agence-de-surveillance-des-reseaux-1320268
https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en
https://www.irsem.fr/

BIBLIOGRAPHIE

Jérôme REMANJON Colonel. Directeur du groupe d'action, études, cohérence, synthèse du Commandeur au NATO Allied Command Transformation (ACT). J
Ron Mac LAURIN, Military propaganda: Psychological warfare and operation, New York, Praeger Publishers, 1982
Cyberattaque et cyberdéfense, Daniel Ventre, 2011, Paris, Lavoisier
Christian Harbulot et Didier Lucas LA GUERRE COGNITIVE-2004
Laure DE ROCHEGONDE Élie TENENBAUM -CYBER-INFLUENCE-Les nouveaux enjeux de la lutte informationnelle- -mars 2021
Daniel Ventre (dir.) Lavoisier, Cyberguerre et guerre de l'information : stratégies, règles, enjeux.Paris, 2010
Soubhik Barari-Christopher Lucas-Kevin Munger- Political Deepfakes Are as Credible As Other Fake-Media And (Sometimes) Real Media-2021
Ullrich K. H. Ecker. The psychological drivers of misinformation belief and its resistance to correction.2022
Sylvain Timsit- Les 10 stratégies de manipulation de masse- 2002
Rémy Hémez, « Opérations de déception — Repenser la ruse au xxie siècle », Études de l'IFRI, juin 2018
Fondation DESCARTES
Gérald Bronner-Apocalypse cognitive-janvier 2021
Koch, AS & Forgas, feeling good and feeling truth: The interactive effects of mood and processing fluency on truth judgments. 2013
Koch, AS & Forgas, mood effects on cognition.2013
Les opérations d'influence chinoises. Un moment machiavélien ; Paul CHARON et Jean Baptiste JEANGENE VILMER. 2021
Institut de Recherche Stratégique de l'École Militaire
Département du Travail de Front uni (DTFU), Liaisons internationales (DLI), Bureau 610.
Armée de trolls, „loups guerriers", web vitrines : plongée dans la nouvelle cyberpropagande chinoise- France Culture-20/09/2021
NATO/NSA, 2005
Soubhik Barari-Christopher Lucas-Kevin Munger- Political Deepfakes Are As Credible As Other Fake-Media And (Sometimes) Real Media-2021
Données OSoMe- Observatoire des médias sociaux de l'université de l'Indiana à Bloomington
Papageorgis, D., & McGuire, W. J. The generality of immunity to persuasion produced by pre-exposure to weakened counterarguments.1961.
Service de vigilance et de protection contre les ingérences numériques étrangères
Global desinformation Index-2018
Mathias Osmundsen,partisan polarization is the primary psychological motivation behind political fake news sharing on Twitter.March 25,2020
Eli Pariser, The Filter Bubble: What the Internet is Hiding from You, Penguin Press, 2011
Paul CHARON & Jean-Baptiste JEANGÈNE VILMER, Les opérations d'influences chinoise.Un moment machiavelien,2021.
Ben Nimmo, Camille François, C. Shawn Eib, Léa Ronzaud, IRA Again: Unlucky Thirteen Facebook Takes Down Small, Recently Created. Network Linked to Internet Research Agency,2020.
Nicu Popescu and Stanislav Secrieru, Hacks, leaks and disruptions. Russian cyber strategies, 2018.