Lettre trimestrielle – Mars 2018

Table des matières

HOAX, FAKE NEWS ET GUERRE INFORMATIONNELLE : TECHNOLOGIES DE LA DESINFORMATION ET OUTILS DE LUTTE CONTRE L'INTOX.

Les *fake-news* ont fait et défait l'actualité ces derniers mois, s'imposant dans le paysage médiatique et politique au point d'être sacrées « mot de l'année 2017 » par le dictionnaire Collins. Du pizzagate[1] aux soupçons d'ingérence russe dans les élections présidentielles américaines en passant par les comptes cachés d'Emmanuel Macron aux Bahamas ou la Rolex de Jean-Luc Mélenchon, les campagnes de désinformation plus ou moins fantasques se sont multipliées et ont émaillé les échéances électorales de 2016 et 2017, démontrant leur potentiel déstabilisateur pour nos processus démocratiques. Plus récemment, la publication sur le site de l'agence de presse qatari QNA d'un faux communiqué attribué à l'Emir Tamim ben Hamad al-Thani a été à l'origine d'une crise diplomatique qui aurait pu compromettre les alliances et la stabilité régionales.

Le phénomène n'est pas nouveau bien sûr, mais il a été accéléré et amplifié par la vitesse et l'amplitude de diffusion de l'information que permettent les nouveaux moyens de communication, à commencer par Internet et les médias sociaux. Ces derniers ont ainsi fait sauter les dernières barrières qui prémunissaient les démocraties de la propagation massive des « fausses nouvelles ». À l'ère de la communication de masse, tout un chacun est en mesure de créer ou diffuser des informations erronées, qu'il s'agisse de plaisanteries sans conséquence ou de réelles tentatives de manipulations, de stratégies d'influence, ou de propagande. Ainsi, selon une étude Gartner, la majorité des individus dans les économies dites avancées consommeront plus de fausses que de vraies informations d'ici à 2022.[2]

Au-delà du contenu des messages véhiculés et de leur nouvelle « viralité », ce qui frappe est la dimension technologique de ces campagnes de désinformation sans cesse plus sophistiquées. Au centre de ces prouesses technologiques, l'intelligence artificielle (IA) et le *machine learning*, dont les derniers développements permettent de créer de toutes pièces des publications, enregistrements et vidéos de plus en plus réalistes et de plus en plus difficile à détecter. Si ces mêmes technologies permettent aussi de lutter contre la propagation des *fake news* en permettant de détecter de plus en plus rapidement et efficacement les modifications ou fabrications de fichiers, elles ne permettent pas à elles seules de lutter contre l'influence de ces contenus. Les outils technologiques doivent donc s'accompagner de réponses politiques, éducatives et sociétales visant à sensibiliser aux dangers des fausses informations et à faciliter leur détection par les utilisateurs.

[1] http://www.lefigaro.fr/secteur/high-tech/2016/12/06/32001-20161206ARTFIG00110-politique-pedophilie-et-desinformation-comment-le-pizza-gate-pourrit-la-vie-d-un-petit-restaurant-americain.php

[2] https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

La fabrique des *fake news*

Rien de plus facile aujourd'hui que de lancer une campagne de désinformation massive. La recette est simple et les ingrédients assez basiques puisqu'il suffit d'un logiciel de transformation des sons et/ou des images pour fabriquer la (fausse) information, et d'un réseau social grand public pour s'assurer de sa diffusion large et pratiquement instantanée.

Des technologies de plus en plus sophistiquées

Dans la lignée de Photoshop et des filtres des appareils photos ou de certains réseaux sociaux, les logiciels et solutions de retouche d'images permettaient déjà de manipuler de façon plus ou moins grossière mais toujours facilement et rapidement les images et photos de notre quotidien. Les technologies de l'IA, notamment les machine et deep learning, donnent à ces outils une dimension supplémentaire. S'appuyant sur des réseaux de neurones artificiels, c'est à dire des algorithmes programmés pour imiter le fonctionnement des neurones du cerveau humain et capables d'apprendre tout seuls à partir de bases de données, elles permettent désormais de reproduire ou fabriquer des images, d'imiter ou de récréer des voix, et même de synchroniser les voix et images reconstituées pour donner naissance à de nouvelles vidéos fabriquées de toutes pièces et de plus en plus réalistes.

➢ *(Re)-produire des images*

Les progrès considérables réalisés dans la retouche d'image au cours des dernières années sont principalement attribuables aux apports de l'IA. Quand elle est intégrée à des logiciels de retouche d'images comme la technologie « Sensei » d'Adobe dans Photoshop CC, l'IA permet en effet de rechercher des correspondances entre des millions d'images, d'analyser les pixels d'une image pour rajouter sur les photos des éléments qui n'y figuraient pas, de reconnaître des typographies pour recréer des polices, de reconnaître des visages et de placer des repères sur certains éléments pour en modifier l'expression,… Rendant ainsi les modifications de plus en plus réalistes et de moins en moins visibles à l'œil nu.

Mais le véritable bouleversement en matière de transformation de l'image est ailleurs. L'apprentissage automatique, et plus précisément l'apprentissage non supervisé[3], permet aujourd'hui de créer des images de toutes pièces, et notamment des portraits. C'est en s'appuyant sur des réseaux antagonistes génératifs (GAN), une classe particulière d'algorithmes d'apprentissage non supervisé qui mettent des réseaux neuronaux en concurrence plutôt que de les faire travailler ensemble, que la société Nvidia a réussi à créer des visages humains en haute définition à partir de photos de personnalités[4]. Le premier réseau neuronal a d'abord créé des images de visages totalement nouveaux, tandis que le second évaluait les résultats en les comparant aux « vraies » photos et se retournait vers le premier pour lui faire retravailler ses productions. Si certains visages apparaissent encore clairement déformés et que la taille des photos reste relativement réduite (1024 pixels), ce type de solution n'en constitue pas moins un outil extrêmement efficace de production de contrefaçons.

[3] Consiste pour un système à classer/regrouper/étiqueter des nouveaux éléments à partir de données qui n'ont pas été répertoriées/classées au préalable.

[4] https://www.youtube.com/watch?v=36lE9tV9vm0

- ***(Re) créer des voix***

Des progrès comparables ont été réalisés en matière de transformation de la voix. Le logiciel Voco d'Adobe, développé avec les chercheurs de l'Université de Princeton, a été le premier à permettre, à partir d'un enregistrement de 20 minutes, de reproduire la diction, la tonalité, et surtout la tessiture d'une voix pour modifier une phrase, y ajouter ou retirer des mots, et ce tout en conservant son empreinte vocale. Son concurrent direct, la solution WaveNet de Google DeepMind, permet quant à elle de générer des voix humaines plus vraies que nature à partir d'échantillons de discours, en copiant la forme des ondes des voix ciblées.

La solution Eerie Tech de la start-up américaine LyreBird, qui s'inspire de ces technologies et s'appuie sur des modèles de deep learning développés par le laboratoire MILA de l'Université de Montréal, va encore plus loin dans le développement d'outils de synthèse de la parole. D'abord, contrairement aux deux précédentes, son API n'exige pas de ressources systèmes puisqu'elle s'appuie sur des ressources cloud. Ensuite, Lyrebird n'a besoin que d'une minute, et non 20, pour comprimer l'empreinte vocale en une clé unique et utiliser cette clé pour générer un élément audio avec une voix correspondante. En utilisant des clusters GPU, elle est capable de générer non moins de 1000 phrases en moins d'une demi-seconde. Les chercheurs de Lyrebird vont même encore plus loin et prétendent que leur technologie permettra à terme de « contrôler l'émotion de la voix générée »[5], en y infusant de la colère, de la sympathie, du stress et d'autres émotions, dans le but de rendre la voix encore plus naturelle. Les résultats sont convaincants : à l'oreille, il est pratiquement impossible de faire la différence entre un discours réellement prononcé et un discours créé artificiellement. De quoi faire dire à un individu tout ou son contraire, comme en témoignent les fausses annonces de Donald Trump réalisées par Lyrebird[6]. On voit facilement l'usage qui pourrait être fait de ces enregistrements factices et les dangers qu'ils représentent. Le risque est d'autant plus grand qu'il est également possible de synchroniser les discours ainsi créés avec des vidéos retouchées.

- ***Synchroniser le son et l'image***

Toujours en s'appuyant sur les mêmes technologies de l'IA, l'Université d'Erlangen-Nuremberg, l'Institut Max Planck et l'Université de de Stanford ont présenté le projet Face2Face, qui permet de plaquer la voix et l'expression faciale d'un acteur sur la cible animée d'une vidéo. L'application analyse le visage de la cible de l'extrait vidéo ainsi que celui de l'acteur source, puis applique les expressions de ce dernier sur l'intervenant de la vidéo. Et ce, en quasi temps réel, puisque le décalage entre la source et la cible n'est que de 3 images, soit environ 100 ms pour une fréquence d'image de 30 images par seconde. L'image qui en résulte conjugue la position de la tête ainsi que la forme et la particularité du visage de la cible, avec les mimiques de l'acteur source. Le programme a ainsi réussi à faire bouger et parler, en temps réel et à l'aide d'une webcam, George

[5] https://www.developpez.com/actu/132426/Lyrebird-indique-etre-parvenu-a-creer-un-algorithme-capable-d-imiter-la-voix-apres-une-minute-d-ecoute-de-la-voix-originale/

[6] https://lyrebird.ai/demo/

W. Bush, Vladimir Poutine ou encore Arnold Schwarzenegger[7]. Bien sûr cette solution est encore perfectible, et le rendu peutêtre de moins bonne qualité si la séquence est trop courte, si les ombres sont trop contrastées, ou en présence de reflets sur le visage. De même, les cheveux ou la barbe qui cachent une partie du visage peuvent rendre la manipulation plus difficile.

Plus récemment, l'Université de Washington a développé un réseau de neurones artificiels capables d'apprendre à reconnaître la voix et la façon de parler d'un individu à partir de plusieurs heures d'enregistrement vidéo, et de convertir les éléments audio d'enregistrements vidéo en reproductions visuelles des lèvres de son auteur. Cet outil permet ainsi pour la première fois de synchroniser le mouvement des lèvres et les paroles entendues afin de superposer n'importe quelle bande son à n'importe quelle vidéo. Dans son expérience la plus convaincante, « *Synthetizing Obama* », l'équipe a ainsi créé une vidéo de Barack Obama prononçant son discours à la suite de la tuerie d'Orlando sur des images bien plus anciennes[8]. Associée à des solutions comme celle de LyreBird, cette innovation permettrait réellement de faire dire n'importe quoi à n'importe qui.

Mais aussi sophistiquées soient-elles, ces *fake news* n'auraient qu'un impact très limité si leurs auteurs ne pouvaient pas s'appuyer sur des canaux de diffusion garantissant leur propagation pratiquement instantanée à l'échelle mondiale. C'est en effet leur « viralité », c'est à dire leur diffusion rapide via des relais gratuits, qui fait l'influence et l'impact des *fake news*. Les réseaux sociaux constituent à ce titre un moyen de communication particulièrement efficace.

[7] http://www.clubic.com/telecharger/logiciel-montage-video/actualite-800728-face2face-comment-dire.html

[8] https://grail.cs.washington.edu/projects/AudioToObama/

Les outils d'une diffusion massive et immédiate.

- ***Des canaux de transmission mondiaux au rôle controversé***

Facebook et Twitter comptent respectivement 2 milliards et 330 millions d'utilisateurs répartis sur tous les continents et représentant pratiquement toutes les classes d'âges et les catégories sociales, et qui passent plusieurs heures par semaine à consulter leurs comptes, « murs », « flux » et autres messageries. Ils assurent donc une visibilité et une audience aussi large que diverse à tous les inconnus et anonymes qui publient des articles, informations ou contenus de toutes sortes dont l'origine n'est pas toujours avérée. De fait, les GAFA et autres réseaux sociaux ont fini par s'imposer comme une alternative aux médias traditionnels, et sont devenus de véritables « diffuseurs d'information »[9]. Selon le Reuters Institute, 51% de la population de 26 pays s'informe par les réseaux sociaux dont 44% par Facebook, et 12% en a fait sa première source d'information[10].

Or plateformes et réseaux sociaux restent aux yeux de la loi des « hébergeurs » et ne sont donc pas soumis aux règles qui encadrent l'activité des médias traditionnels, à savoir la loi de 1881 qui régit le droit de la presse. Et c'est bien là que réside une partie du problème, car comme ils se contentent de publier du contenu rédigé par des tiers et non d'en produire, ils ne peuvent pas « voir leur responsabilité pénale engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services qui n'avait pas effectivement connaissance de leur caractère illicite ». Ils bénéficient donc d'un régime de responsabilité atténuée, et n'ont pour seule obligation que de retirer les contenus illicites ou d'en interdire l'accès. Contrairement aux journalistes dont les fonctions impliquent des règles de déontologie leur imposant de distinguer pour leurs lecteurs les informations brutes, des prises de partie idéologiques ou partisanes, les médias sociaux et hébergeurs qui ne sont pas soumis à ces exigences constituent de fait des espaces de propagande.

- ***Des réseaux sociaux aux médias sociaux***

Et pourtant, les réseaux sociaux, comme les médias traditionnels, « trient » bien les informations qu'ils mettent à disposition de leurs utilisateurs. Mais leurs critères de sélection et de hiérarchisation de l'information sont loin de garantir l'objectivité des contenus publiés. C'est ce qu'on appelle les « *filter bubbles* » ou « bulles de filtrage » : à partir de données collectées sur les internautes, et notamment sur leurs données de navigation qui reflètent de fait leurs préférences, les algorithmes de tri de l'information des réseaux sociaux sélectionnent les contenus qui seront visibles aux utilisateurs de façon à ce que chacun accède à une vision unique du web. Le fil d'actualité (*newsfeed*) de Facebook est particulièrement représentatif. Celui-ci compile les messages « d'amis » et les publications de pages « likées », c'est à dire à la fois des commentaires et images personnels, et des articles partagés ou republiés provenant tant de sources médiatiques que de blogs personnels. Or l'ordre des publications qui apparaissent sur le fil d'actualité d'un internaute ne dépend pas seulement de leur chronologie, mais aussi des interactions entre l'utilisateur et l'auteur de la publication, du format et du type de

[9] http://www.lefigaro.fr/vox/medias/2018/01/05/31008-20180105ARTFIG00103-fake-news-les-geants-du-web-devraient-respecter-les-memes-regles-que-les-medias-traditionnels.php

[10] https://www.nouvelobs.com/societe/20160913.AFP7595/comment-facebook-filtre-notre-connaissance-du-monde.html

média (vidéo, images, textes), et de la popularité de ladite publication auprès des autres utilisateurs. Et comme un internaute ne lit en moyenne que 10% des 2000 publications de son *newsfeed*, il n'accède de fait qu'à celles que les algorithmes de la plateforme en question ont jugé prioritaires sans qu'elles soient les plus fiables. Même Google News, qui pourtant reprend les contenus de médias professionnels, les hiérarchise selon ses propres règles éditoriales, contribuant comme les réseaux sociaux à « filtrer » notre connaissance du monde[11].

Le cas des « chaînes » introduites par la messagerie Telegram en 2015 est à ce titre particulièrement intéressant. Celles-ci ne sont visibles que par un nombre limité d'utilisateurs désignés, l'identité de leurs auteurs est protégée et leurs contenus sont chiffrés et non modifiables. Contrairement aux réseaux sociaux dont les contenus sont en théorie régulés et sont donc susceptibles d'être censurés, les chaines Telegram échappent à tout contrôle des autorités et aux tentatives de trolling. Très populaires en Russie, elles offrent aux militants et groupements politiques pro et anti-gouvernementaux des plateformes d'expression, comme la chaîne Politota ou la chaine d'information satirique Lentach.

C'est en fait tout le modèle économique des GAFAM et autres réseaux sociaux qui est en cause, eux dont la rentabilité repose en grande partie sur les publicités et contenus sponsorisés publiés sur leurs plateformes. À l'ère de « l'économie de l'attention » en effet, tout est fait pour que les utilisateurs restent en ligne le plus longtemps possible et « cliquent » sur ces contenus sponsorisés. Les géants du Net mettent ainsi à disposition de leurs utilisateurs, sans même que ces derniers aient à les rechercher, des contenus considérés par leurs algorithmes comme correspondant à leurs centres d'intérêts, et leur proposent des pages/sites/contenus aux sujets similaires mais dont la fiabilité n'a pas été vérifiée. Une étude publiée par le quotidien britannique *The Guardian* le 13 février dernier montre ainsi que les algorithmes de Youtube mettent en avant les vidéos aux contenus extrémistes car celles-ci généraient un nombre de vues important et permettaient par la même d'attirer la publicité sur la plateforme de partage de vidéos, et donc les revenus pour Google. Ces stratégies d'addiction et de manipulation qui favorisent la propagation des *fake news* et accroissent leur impact sont désormais largement dénoncées, notamment par Tristan Harris, ancien « philosophe produit » chez Google, qui les qualifie de « piratage de l'esprit »[12].

Les « médias sociaux », en permettant une diffusion à la fois immédiate et globale des informations publiées sur leurs plateformes, sont tout aussi responsables de l'essor des *fake news, hoax* et campagnes de désinformation que les technologies qui leur donnent le jour. Il n'est donc pas surprenant que la lutte contre les *fake news* s'articule autour de deux axes : le développement d'outils technologiques permettant de les détecter et de les déconstruire, et des mesures de sensibilisation et d'éducation visant à réduire leur impact.

[11] https://www.nouvelobs.com/societe/20160913.AFP7595/comment-facebook-filtre-notre-connaissance-du-monde.html

[12] http://inspired.epochtimes.fr/captologie-et-economie-de-lattention-116769.html

La riposte médiatique : contrer l'influence des *fake news*

Le rôle des médias sociaux dans la propagation des *fake news* est incontestable. Selon une étude du MIT, qui a étudié près de 126 000 « histoires » diffusées sur Twitter entre 2006 et 2017, les *fake news* se propagent plus vite et touchent davantage d'utilisateurs que les articles dont la véracité a pu être établie. [13] Il n'est donc pas étonnant que la première véritable offensive d'ampleur contre les *fake news* et la désinformation soit venue des médias traditionnels soutenus par les médias sociaux, avec l'objectif affiché de contrer leur influence trompeuse et d'endiguer leur propagation pour en réduire l'impact.

De fait, les initiatives et projets dits de « vérification des faits » ne constituent pas en eux-mêmes une nouveauté. Ainsi, le site Snopes[14] traque et recense les *hoax* et les *fake news* depuis 1994 grâce à son équipe de journalistes et d'experts qui évaluent la véracité des informations en analysant leurs sources, le contexte dans lequel elles ont été publiées, le profil et le domaine d'expertise de leur auteur, etc. Les informations analysées sont ensuite classées dans 10 catégories allant de « vrai » à « faux » en passant par « non prouvé », « légende » ou encore « arnaque ». *Snopes* est ainsi l'une des solutions choisies par Facebook pour faire la chasse aux fausses informations et contrôler ses contenus. De même, les chercheurs du projet FactCheck de l'Annenberg Public Policy Center de l'Université de Pennsylvanie assurent une veille permanente des discours et annonces des principales personnalités politiques du pays et décortiquent les arguments avancés pour détecter le vrai du faux. Leurs conclusions reposent sur un travail de recherche extrêmement rigoureux en sources ouvertes et un réseau d'experts nationaux et internationaux.

Mais les initiatives les plus récentes se distinguent de leurs prédécesseurs par leur composante technologique. En témoigne l'initiative française Crosscheck, lancée en février 2017 à quelques mois du premier tour des élections présidentielles sous la forme d'un travail de vérification collaboratif entre une trentaine de rédactions locales et nationales et pilotée par First Draft et Google News Lab. Crosscheck s'était donnée pour mission d'évaluer la viralité des contenus publiés sur Internet, laquelle se caractérise notamment par le nombre de partages, de « like » ou de commentaires importants d'une publication, qu'il s'agisse de photos, de vidéos, de « mêmes », de commentaires ou de sites d'actualités. Ses analyses reposaient notamment sur des logiciels de veille des réseaux sociaux comme NewsWhip, ou des solutions de mesure du « buzz » comme **CrowdTangle**, dont la plateforme de type analytics mesure l'impact des contenus déposés sur les réseaux sociaux. L'intervention des journalistes participants permettait ensuite de vérifier les informations relayées sur la base de leurs contenus et des images ou vidéos qui les accompagnaient. 400 posts « viraux » par jour ont ainsi été relevés pendant deux mois et 267 articles « vérifiés » ayant trait avec l'élection présidentielle ont été publiés.

Les solutions les plus avancées de détection et de signalement des fake news reposent toutefois sur les technologies liées à l'IA, qui s'avèrent pour ainsi dire, aussi efficace dans ce domaine que dans la création de fausses informations. Par exemple, la société Storyzy a recensé dans une base de données en français et en anglais près de 2 800 sites diffusant des contenus classés en 10 catégories dont « fausses informations »,

[13] http://www.sciencemag.org/about/science-licenses-journal-article-reuse?_ga=2.58498282.1118037145.1522337216-950727266.1522337216

[14] https://www.snopes.com/

« propagande », « extrémiste » ou « conspirationniste »… Storyzy utilise pour ce faire une technologie propriétaire basée sur le traitement automatique du langage (TAL), une discipline qui emprunte à la fois à la linguistique et à l'IA et qui imite la compréhension humaine des mots et des phrases pour permettre aux modèles d'apprentissage automatique de fournir des réponses précises à des questions tout aussi précises. La liste ainsi constituée par Storyzy est régulièrement mise à jour et permet notamment de constituer des « black lists » dynamiques. Les opérateurs de campagnes digitales comptent parmi les principaux utilisateurs de cette solution, qui leur permet de garantir à leurs clients un environnement publicitaire digital sécurisé.

L'application AdVerif.ai va encore plus loin en automatisant le processus d'identification de fausses nouvelles avec un taux de précision de près de 90%. Son algorithme identifie d'abord la source d'information d'un article à partir d'un catalogue de sites considérés comme diffuseurs de fausses nouvelles, satire, *clickbait*, ou de la propagande politique. Il vérifie aussi si les faits cités ont été réfutés par des sites de vérification comme Snopes et FactCheck.org, ou s'ils ont été corroborés par des sites d'information établis. Il analyse ensuite les modèles linguistiques utilisés dans les articles, en partant du constat que le langage utilisé pour des histoires fausses a tendance à contenir plus de langage émotif et opiniâtre et se caractérise par un manque de guillemets, un nombre anormalement élevé d'adjectifs ou de phrases courtes.

La réponse technologique : la déconstruction des *fake news*

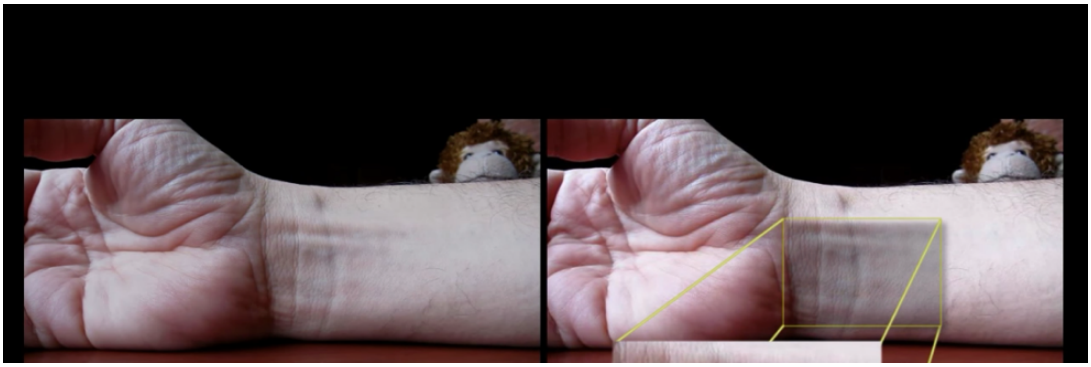
En s'appuyant sur les mêmes technologies qui ont permis le développement et la sophistication des *fake news*, leurs opposants ont mis au point des solutions permettant de détecter les retouches, modifications et créations artificielles d'images, d'enregistrements audio et de vidéos.

Comme pour les contenus en format texte, des solutions existent depuis longtemps pour détecter des images modifiées ou retouchées. Des moteurs de recherche d'images comme TinEye.com proposent par exemple de lister tous les sites Internet affichant une image donnée, à partir de son lien. Cet outil permet ainsi de retrouver la source d'image, son contexte, ou encore sa version originale avant ou sans retouches éventuelles, et propose également de classer les images listées en fonction de l'ampleur des retouches. D'autres logiciels comme regex.info ou addons.mozilla.org, analysent les métadonnées exif d'une photo (date de prise du cliché, type d'appareil utilisé, taille de l'image, utilisation d'un logiciel de retouche, …), ou, comme *Fotoforensics*, les différences de compression d'une image, caractéristiques des retouches photo. La détection de photomontages s'appuie aussi très largement sur des logiciels d'assistance à la photo-interprétation avancée permettant de détecter les altérations dans les images numériques comme Tungstène, développé en 2009 à la demande du ministère de la Défense. Ce logiciel permet par exemple de détecter des incohérences et altérations à la fois dans les statistiques profondes de l'image numérique et dans la diffusion des rayons de lumière et de la chrominance. Il propose aussi une méthodologie d'interprétation des résultats dans le but d'aider l'opérateur à identifier les véritables tentatives de désinformation et d'ingérence par l'image.

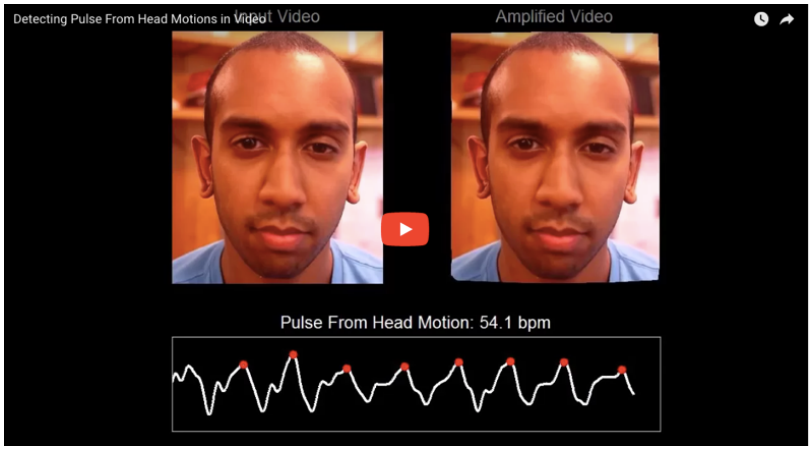
Le développement de l'IA et des technologies qui lui sont liées a permis des avancées considérables en matière de détection des modifications ou créations d'image. Des projets de recherche plus récents comme Video Magnification[15], lancé en 2012, vont encore plus loin dans l'analyse et la déconstruction d'une vidéo en repérant les variations colorimétriques et les variations des formes présentes dans une vidéo pour en calculer les fréquences et les amplitudes et repérer ainsi les modifications. Il est notamment possible d'extraire le pouls

[15] https://www.youtube.com/watch?time_continue=24&v=ONZcjs1Pjmk

et la respiration du sujet filmé et d'analyser son pouls à travers les changements (imperceptibles à l'œil nu) de la couleur de la peau qu'il génère, ainsi que d'étudier la respiration par le déplacement de la poitrine du sujet filmé.



D'autres projets[16] s'attachent quant à eux à détecter le pouls par l'amplification d'un mouvement, imperceptible ici encore, de la tête du sujet balancée au grès des battements du cœur, et ce même si le visage est masqué ou que le sujet tourne la tête.



Mais ces outils, tout aussi sophistiqués et performants soient-ils, interviennent a posteriori, c'est à dire une fois que le contenu retouché /modifié ou créé de toutes pièces a été détecté, donc bien souvent une fois la fausse information diffusée à grande échelle. Quelle peut donc être l'efficacité des outils de détection face à la viralité des *fake news* et au « buzz » qu'elles peuvent générer ? Pour être réellement efficaces, les solutions de lutte contre les fausses nouvelles et campagnes de désinformation doivent également cibler les canaux et modes de diffusion, et doivent avoir pour vocation première d'empêcher la propagation des *fake news*. Il s'agit par exemple de responsabiliser les médias sociaux et de les obliger à exercer un contrôle plus rigoureux sur les contenus publiés sur leurs plateformes. C'est notamment l'objectif de la loi française « de fiabilité et de

[16] https://www.youtube.com/watch?v=EhZXDgG9oSk

confiance de l'information », née d'une volonté affichée de prévenir et éviter la diffusion de campagnes de désinformation comme celles qui ont émaillé et déstabilisé les dernières élections présidentielles.

Conclusion

La loi de fiabilité et de confiance de l'information se distingue par sa volonté d'intervenir en amont, avant la diffusion sur les plateformes et les réseaux sociaux de contenus pouvant être identifiés comme des *fake news*. L'une de ses dispositions principales consiste en effet à étendre aux réseaux sociaux les obligations incombant aux médias traditionnels par la loi de 1881 sur la liberté de la presse, qui fixe et punit le délit de « *fake news* ». Les contenus sponsorisés sont également dans le viseur du législateur, qui impose désormais aux plateformes plus de transparence sur ces publications et un devoir de coopération en matière de publication des montants et auteurs des sponsorings. Certaines plateformes ont d'ailleurs déjà pris des mesures dans ce sens. Par exemple, Facebook a annoncé courant janvier 2018 une série de mesures visant d'une part à réduire la présence sur les fils d'actualité des contenus publiés par des marques ou des médias au profit de ceux publiés par les « amis », et d'autre part à revoir ses critères de hiérarchisation des sources d'information pour privilégier celles jugées « fiables » par les utilisateurs. Ces mesures ne mettent toutefois pas fin au système du sponsoring. Les marques les plus puissantes pourront donc toujours promouvoir leurs publications au détriment de celles de médias reconnus. Ces mesures semblent donc non seulement contreproductives, mais permettent aussi d'accroître les interactions entre les utilisateurs, donc d'affiner leurs profils par agrégation de données les concernant. Elles permettent donc *in fine* aux réseaux sociaux de conserver (et exploiter) leur monopole sur les données personnelles. Ce n'est pas la première fois que les initiatives des géants du Net en matière de lutte contre les *fake news* sont sujettes à controverses. Facebook a ainsi dû renoncer à son programme de signalement des *fake news*, identifiées par un petit drapeau sur les fils d'actualité avant d'être censurées ou retirées, après qu'il ait été démontré que ces contenus attisaient de fait la curiosité des utilisateurs et représentaient les articles les plus lus et les plus partagés. L'efficacité des nouvelles obligations imposées aux médias sociaux et visant à lutter contre les *fake news* avant même leur diffusion reste donc dépendante de la bonne volonté des plateformes concernées et de leur disposition à jouer le jeu et à coopérer avec les autorités.

Quant aux deux autres instruments de lutte contre les *fake news* prévus par la loi de fiabilité et de confiance de l'information, ils interviendront au contraire *a posteriori*, pour freiner la propagation des campagnes de désinformation. L'une de ces dispositions sera destinée à contrer l'influence des médias étrangers en période électorale, et permettra au Conseil Supérieur de l'Audiovisuel (CSA) de suspendre ou révoquer la convention d'un média considéré comme étant sous influence d'un État étranger, s'il juge que ce média contribue à diffuser de fausses informations. La dernière disposition mettra en place un outil législatif permettant d'agir rapidement contre les *fake news*, en donnant aux citoyens la possibilité de saisir un juge des référés pour « faire cesser la diffusion massive et artificielle d'une fausse nouvelle ». L'efficacité de ces mesures dépendra donc de la réactivité des entités chargées de contrôler les contenus détectés grâce aux technologies liées à l'IA, et tout l'enjeu pour elles sera d'agir avant que les *fake news* aient pu toucher un nombre trop important d'utilisateurs.

LE CADRE JURIDIQUE DES ENTREPRISES PRIVEES DE *CYBER THREAT INTELLIGENCE*

Depuis quelques années, dans un contexte de très forte augmentation des cyberattaques et de leur niveau de sophistication, le renseignement sur les menaces cyber (CTI, *Cyber Threat Intelligence*) est apparu comme un des éléments essentiels de la cybersécurité. Alors que le renseignement était considéré jusqu'à un passé assez récent comme le domaine réservé des agences spécialisées de l'État, on assiste désormais à une prolifération d'entreprises privées proposant des outils, des services ou des rapports de CTI[17].

En quoi consiste la CTI, pourquoi les entreprises privées occupent-elles – dans l'espace médiatique au moins – un rôle de plus en plus important, avec quels risques et dans quel cadre juridique exercent-elles ces fonctions ? Telles sont les questions auxquelles tente de répondre la présente note.

En quoi consiste la Cyber Threat Intelligence ?

Si la CTI est une notion au contour flou, sans définition internationalement reconnue, elle peut plus facilement être caractérisée par ses objectifs, en ligne avec ceux du renseignement[18] : acquérir, notamment dans, par et pour le cyberespace, l'ensemble des connaissances permettant de comprendre et d'anticiper les cybermenaces, y compris les plus sophistiquées, de protéger efficacement les systèmes numériques en assurant la meilleure réactivité possible des mesures de défense de ces systèmes lorsqu'ils sont attaqués, et d'identifier et de poursuivre les auteurs et les commanditaires de ces attaques.

L'avènement de la CTI a succédé à deux périodes où la défense des systèmes numériques était essentiellement assurée par l'analyse des logiciels malveillants, puis par celle des schémas d'attaque. Ces analyses, faites le plus souvent "post-mortem" sur les systèmes ayant subi des attaques réussies (d'où l'expression "forensique"), permettaient, dans les premiers temps de l'Internet, d'extraire la signature des malwares et d'alimenter ainsi la bibliothèque des antivirus utilisés pour assurer la protection périmétrique des systèmes, puis dans les années suivantes, de comprendre les techniques utilisées dans l'attaque pour paramétrer en conséquence les outils de protection (pare-feu, sondes de détection, recherche d'exécutables malveillants cachés dans les systèmes, etc.). Ces premiers outils se sont vite révélés très insuffisants face à des attaques de plus en plus sophistiquées. Ils ne répondaient en outre pas à la lancinante et difficile question de l'attribution des attaques, indispensable pour les actions postérieures, judiciaires ou diplomatiques notamment.

La CTI a décliné dans le monde cyber les principes et outils du renseignement. On y distingue par exemple aussi un niveau stratégique et un niveau tactique, tous deux complémentaires.

---

[17] Voir aussi l'article "Le rôle essentiel du secteur privé en matière de renseignement « cyber »" dans la Lettre de l'OMC d'août 2017, https://www.defense.gouv.fr/content/download/511380/8625049/file/OBS_Monde%20cybern%C3%A9tique_201708.pdf.

[18] "Ensemble de connaissances concernant l'ennemi, indispensables à l'état-major de la Défense nationale pour une action militaire efficace, à la police pour mener ses enquêtes et arrêter les délinquants", définition du Centre National de Ressources Textuelles et Lexicales (CNRTL), http://www.cnrtl.fr/lexicographie/renseignement.

- La CTI « stratégique » vise à comprendre l'écosystème de la cybercriminalité, sa nature, ses membres, leurs liens, leurs motivations, leurs capacités techniques et les méthodes d'attaque qu'ils utilisent généralement.
- La CTI « tactique » a une portée naturellement plus directement opérationnelle. S'appuyant sur la CTI stratégique, elle vise à comprendre les deux éléments qui pourraient permettre à un attaquant d'agir, et à déceler avec le meilleur préavis possible le moment de leur conjonction : d'une part, une opportunité (l'émergence d'une vulnérabilité - faille de sécurité non encore corrigée sur un logiciel, découverte d'un accès mal sécurisé ou d'un employé pouvant être instrumentalisé – ou survenance d'un évènement facilitant ou justifiant l'attaque - annonce politique ou financière de la cible, action militaire, etc.), d'autre part une capacité d'attaque (capacité déjà observée de la part du groupe suspecté de vouloir agir, ou pouvant être acquise - vente sur le Darkweb d'un outil d'exploitation d'une vulnérabilité non corrigée, par exemple).

La connaissance ainsi obtenue permet peu à peu d'améliorer les mesures de protection, de prévention et de détection des attaques. Couplée aux outils de cybersécurité d'une organisation, elle en optimise le fonctionnement. En particulier, les SIEM[19], paramétrés avec des données CTI corrélées, assurent un meilleur tri parmi les innombrables événements qu'ils collectent, limitant les faux positifs et garantissant une détection plus sûre des activités anormales correspondant à des tentatives d'attaque.

Le rôle des entreprises privées en matière de CTI

Les entreprises privées ont un rôle grandissant en matière de CTI, et constituent désormais les premiers fournisseurs de données de CTI. Plusieurs raisons expliquent cette situation :

- Tous les acteurs socio-économiques d'un pays sont aussi menacés que les institutions gouvernementales, et ont donc tout autant besoin de CTI que ces dernières pour assurer leur défense.
- Les services de renseignement étatiques, qui ont vocation à servir, d'abord et presque exclusivement, les autorités et institutions publiques, peuvent difficilement fournir aux acteurs privés le renseignement qu'ils élaborent. La culture du secret y est très forte, notamment parce que toute compromission fait courir le risque de perdre la confiance des homologues alliés avec lesquels ils échangent du renseignement, et plus encore d'informer les attaquants potentiels sur leurs capacités réelles, ainsi que sur leurs limites.
- Plus que la plupart des services de renseignement, les grandes entreprises de cybersécurité disposent de très importantes capacités de recueil dans le cyberespace et d'analyse des informations nécessaires à l'élaboration du CTI. Elles ont en particulier un accès direct et immédiat aux capteurs qu'elles mettent en place chez les clients qui leur confient la sécurité de leurs systèmes d'information, et sont donc les premières à pouvoir déceler les outils et méthodes d'attaques utilisés contre ces systèmes.

[19] Un SIEM (Security information mangement system) est un logiciel qui centralise les journaux système des équipements d'un système d'information (les "logs" issus des pare-feux, routeurs, serveurs, bases de données …), effectue des corrélations pour identifier, parmi les évènements informatiques, ceux qui pourraient résulter ou témoigner d'un incident de sécurité, et lance en conséquence des alertes.

- Ces entreprises ont souvent des liens avec les services de renseignement de leur pays d'appartenance, dans l'esprit de la coopération public – privé que demandent de nouer toutes les stratégies nationales de cybersécurité pour faire face aux dangers du cyberespace. On peut aisément supposer que les fruits de cette coopération, tout en étant rigoureusement maîtrisés par les services officiels, sont le plus souvent dévoilés par les entreprises privées, optiquement plus neutres que les services de l'État, et qui ont une liberté bien plus grande que ces derniers pour dénoncer publiquement les groupes de hackers étrangers et plus encore leurs liens supposés avec un gouvernement. Cela pourrait expliquer que les informations relatives à la cybersurveillance exercée par les Etats-Unis soient le plus souvent dévoilée par des entreprises d'origine russe, et qu'à l'inverse, les groupes de hackers a priori inféodés au pouvoir russe soient une cible privilégiée des entreprises de cybersécurité américaines.

C'est ainsi que selon les estimations du Gartner[20], le marché de la CTI devrait se développer fortement d'ici à 2020. On devrait donc assister à une augmentation d'acteurs privés de CTI dans les prochaines années.

Le secteur privé de la CTI regroupe une variété d'acteurs qui peuvent poursuivre des finalités différentes selon les intérêts qu'ils sont amenés à défendre.

Acteurs	Finalités et intérêts
Entreprises traditionnelles de cybersécurité et éditeurs technologiques	Ces entreprises fournissent des données et des outils de CTI, essentiellement de nature technique, en complément de leur offre de solutions de cybersécurité, pour en améliorer les performances.
Entreprises spécialisées de CTI	Ces entreprises peuvent être des filiales spécialisées des entreprises de cybersécurité ou des entreprises indépendantes qui peuvent également éditer leurs propres solutions techniques spécialisées en CTI. Elles protègent les intérêts de leurs clients dans l'ensemble des domaines qui concernent leurs systèmes d'information ou leur présence dans le cyberespace. Elles poursuivent de larges finalités comme la lutte contre la cybercriminalité, la protection de la propriété intellectuelle ou industrielle, la préservation de l'image de marque sur Internet ou l'intelligence économique.
Entreprises de management des risques et d'intelligence	Leur domaine d'intervention ne concerne pas principalement les cybermenaces mais plus largement l'ensemble des risques qui peuvent peser sur une organisation (juridiques, économiques, politiques, sociaux, etc.). Ces entreprises ne proposent donc pas directement des prestations de CTI. Elles développent cette discipline pour les besoins de leurs missions, notamment dans le cadre du renseignement d'origine cyber. Ces entreprises se positionnent sur le marché du management des risques et de l'intelligence économique bien qu'elles peuvent chercher à s'implanter sur celui de la cybersécurité.
Autres (chercheurs en cybersécurité et white hat par exemple)	D'autres acteurs privés pratiquent la CTI, comme par exemple les chercheurs en cybersécurité, pour des besoins de la recherche scientifique sur les cybermenaces, ou les « white hat », ces hackers qui recherchent des vulnérabilités pour le compte

[20] https://www.gartner.com/newsroom/id/3638017

	d'une organisation comme dans le cadre des programmes de bug bounty. Les motivations de ces acteurs peuvent être variées (économiques, notoriété, recherches scientifiques, respect de l'ordre public avec les lanceurs d'alerte, etc.).

Note : ce tableau propose une liste non exhaustive des acteurs privés de CTI. Par ailleurs, un même acteur privé peut entrer dans les différentes catégories du tableau.

Les risques du traitement de la CTI par les entreprises privées

Si l'apport des entreprises privées en matière de CTI est indéniable pour la sécurité du cyberespace, l'exercice de cette activité n'est pas sans risque, et fait d'ailleurs régulièrement l'objet de controverses. Et de fait, certains acteurs de la CTI peuvent agir de manière disproportionnée, voire totalement abusive au regard du droit ou de l'éthique, pour protéger les intérêts de leurs clients. A titre d'exemple, on peut mentionner certaines affaires rendues publiques, comme l'introduction illégale dans les systèmes d'information de Greenpeace[21] ou les accusations d'espionnage contre Kaspersky aux Etats-Unis[22].

Les risques sont d'autant plus avérés que les techniques de renseignement de la CTI peuvent être intrusives. D'une part, les moyens humains et techniques mis en œuvre au sein d'une organisation peuvent accéder à des informations sensibles ou interférer dans les systèmes d'information de l'organisation de manière disproportionnée. D'autre part, ces moyens peuvent servir à collecter et analyser de manière massive des informations sensibles sur des personnes ou des organisations. Enfin, certains outils techniques telles que par exemple des sondes de détection ou les honeypots et sinkholes, qui peuvent servir à collecter des informations sur les cybermenaces, peuvent constituer de véritables actes de cyberdéfense offensive dans certains cas, ce qui peut, intentionnellement ou non, impacter des systèmes d'information tiers[23].

Les limites juridiques des activités privées de CTI

Bien qu'il n'existe pas de cadre juridique international ou national spécifique aux activités privées de CTI, des règles juridiques essentiellement de nature pénale limitent ces activités, notamment pour :

- Protéger la vie privée des personnes et les données « sensibles » des organisations ;
- Protéger les systèmes de traitement automatisé de données.

La protection de la vie privée et des données « sensibles »

Etant donné que les entreprises de CTI peuvent être amenées à collecter et traiter des informations sensibles sur les personnes ou les organisations, les règles relatives au respect de la vie privée des personnes et aux

[21] http://www.leparisien.fr/environnement/espionnage-de-greenpeace-edf-relaxe-6-mois-de-prison-contre-un-ex-cadre-du-groupe-06-02-2013-2544961.php

[22] http://www.lemonde.fr/pixels/article/2017/10/26/accuse-d-espionnage-kaspersky-explique-comment-il-a-obtenu-des-outils-de-la-nsa_5206234_4408996.html

[23] Un *sinkhole* peut constituer un acte de cyberdéfense offensive lorsqu'il vise à prendre le contrôle du réseau de machines infectées ou à détruire du trafic, ce qui peut impacter des tiers de manière volontaire ou non. De même, un honeypot peut disposer de la capacité d'analyse de port permettant ainsi un accès à distance à un système d'information : *Honeypots et sinholes, outils de défense active*, Lettre n° 64, Observatoire du monde cybernétique, Juillet 2017

« secrets » des organisations s'appliquent. A titre d'exemple, les dispositions du RGPD s'appliquent aux entreprises de CTI lorsqu'elles collectent et traitent des données personnelles de citoyens de l'UE. Par ailleurs, le droit français prévoit que ces entreprises ne doivent pas porter atteinte « de mauvaise foi » au secret des correspondances[24]. Enfin, ces entreprises peuvent faire l'objet de poursuites judiciaires en cas d'accès non autorisés à des informations protégées ou de divulgation d'informations protégées d'une organisation, qu'elle soit cliente ou non de l'entreprise de CTI. Il peut s'agir par exemple d'informations protégées par le droit de la propriété intellectuelle ou par le « secret des affaires »[25] ou encore d'informations protégées par le secret de la défense nationale[26].

La protection des systèmes de traitement automatisé de données

Un certain nombre de pays ont adopté une législation sanctionnant les atteintes aux systèmes de traitement automatisé de données, notamment en Europe avec la Convention de Budapest de 2001 du Conseil de l'Europe sur la cybercriminalité[27]. De ce fait, la mise en œuvre de moyens techniques pouvant porter atteinte à des systèmes d'information par une entreprises de CTI peut constituer une infraction. En France, une entreprise de CTI peut ainsi faire l'objet de poursuites pénales si[28] :

- Elle accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données. La sanction est plus forte s'il en résulte la suppression ou la modification de données ;
- Elle entrave ou fausse le fonctionnement d'un système de traitement automatisé de données ;
- Elle introduit frauduleusement des données dans un système de traitement automatisé ou supprime ou modifie les données ;
- Elle importe, détient, offre, cède ou met à disposition, sans motif légitime, un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions mentionnées précédemment.

Une entreprise de CTI pourrait être ainsi poursuivie dans le cas où elle mettrait en œuvre des moyens techniques qui pourraient constituer des mesures de hack back par exemple. Dans un exemple moins extrême, elle pourrait également être poursuivie dans les cas où elle mettrait en œuvre des outils techniques qui perturberaient de manière disproportionnée et non autorisée les systèmes informatiques de son client ou d'un tiers. En outre, les entreprises de CTI qui éditent et/ou fournissent des logiciels de CTI doivent en justifier la légitimité. Notons qu'elles doivent également se soumettre aux régimes de contrôle de l'Arrangement de Wassenaar et de l'Union Européenne sur les biens et technologies à double usage dans les cas où elles exporteraient leurs logiciels de CTI.

[24] Article 226-15 du code pénal

[25] Actuellement un projet de loi relatif au secret des affaires transposant la directive européenne 2016/943/UE sur la protection des savoir-faire et des informations commerciales non divulguées est en discussion au Parlement : http://www.assemblee-nationale.fr/15/propositions/pion0675.asp

[26] Articles 413-9 et suivants du code pénal

[27] https://www.coe.int/en/web/cybercrime/home

[28] Article 323-1 et suivants du code pénal

Enfin, si la majorité des entreprises privées de CTI sont des entreprises de cybersécurité étrangères, notamment américaines, implantées dans le monde entier, le caractère transnational qu'elles revêtent ne fait pas obstacle aux limites juridiques précédemment mentionnées. En effet, les lois pénales françaises peuvent s'appliquer notamment[29] :

- Aux infractions commises à l'étranger qui se rattachent au territoire français ;
- Aux infractions commises à l'étranger par une personne ou une entreprise française ;
- Aux infractions commises à l'étranger liées aux intérêts fondamentaux de la nation comme le secret de la défense nationale ou lorsqu'une convention internationale prévoit l'application de la loi française.

L'adaptation du cadre juridique aux évolutions de la cybersécurité

Les entreprises privées de CTI ne peuvent pas agir de manière totalement libre, leurs activités sont strictement encadrées puisqu'elles doivent respecter de nombreuses exigences pénales. Néanmoins, les évolutions des cybermenaces et de la cybersécurité conduisent à adapter les règles juridiques en la matière, notamment pour apporter plus de sécurité juridique à des entreprises ou acteurs privés qui agissent pour la cybersécurité comme les entreprises de CTI.

Depuis 2016, la loi pour une République numérique prévoit qu'Il est désormais possible pour une personne de signaler une faille de sécurité ou une vulnérabilité à l'ANSSI sans qu'il soit nécessaire d'avertir l'autorité judiciaire[30]. Le texte garantit également que l'ANSSI préserve la confidentialité de l'identité de la personne à l'origine du signalement. Ainsi, un acteur privé de CTI qui découvrirait de bonne foi une faille de sécurité ou une vulnérabilité dans les systèmes d'information d'une organisation mais de manière non autorisée pourrait être protégé par la loi s'il coopère avec l'ANSSI.

En outre, l'article 25 de la loi de programmation militaire (LPM) de 2013 a précisé les « motifs légitimes » pour lesquels les entreprises privées peuvent détenir et fournir un moyen techniques susceptible de commettre une infraction aux systèmes de traitement automatisé de données. Ces motifs peuvent être la « recherche » ou la « sécurité informatique »[31]. Cette disposition assure plus de sécurité juridique aux entreprises de CTI qui détiendraient et fourniraient des outils techniques telles que des sondes pour analyser les cybermenaces sur les réseaux d'une organisation. Elle sécurise également juridiquement la CTI pratiquée pour les besoins de la recherche scientifique. Par ailleurs, rappelons que l'Arrangement de Wassenaar a fait l'objet d'une révision en 2017 afin d'assouplir le régime de contrôle des exportations des biens et technologies pouvant servir aux « logiciels d'intrusion », notamment pour les besoins de la recherche de vulnérabilités et pour les réponses aux cyber-incidents, ce qui inclus les outils mis à disposition par les entreprises de CTI[32].

Enfin, le projet de loi de la prochaine LPM 2019-2025 souhaite renforcer les moyens de détection des cyberattaques, notamment en permettant aux opérateurs de communications électroniques de recourir à des dispositifs mettant en œuvre des marqueurs techniques sur leurs réseaux pour détecter des événements

[29] Articles 113-1 et suivants du code pénal

[30] Article L. 2321-4 du code de la défense

[31] https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=48329D727E4A6325456CA5AE0351B116.tplgfr27s_2?idArticle=JORFARTI000028338933&cidTexte=JORFTEXT000028338825&dateTexte=29990101&categorieLien=id

[32] https://lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés[33]. Cette disposition intéresse donc directement les entreprises de CTI qui sont les premiers fournisseurs en matière de solutions techniques de détection des cyberattaques.

Des efforts ont donc été entrepris en France pour concilier les activités des entreprises privées de CTI avec les exigences de protection des personnes, des données et des systèmes d'information. Cependant, le cadre juridique de ces entreprises reste encore confronté à des difficultés liées à l'encadrement des moyens techniques de cyberdéfense. Certains de ces moyens qui peuvent être utilisés par les entreprises de CTI se situent juridiquement dans une zone grise[34]. En effet, ils peuvent à la fois servir à récupérer des informations sur les cybermenaces de manière passive et être utilisés à des fins plus offensives voir de « hack back » dans les cas où l'entreprise chercherait à entraver une cybermenace en s'attaquant à un serveur par exemple.

Pour répondre à ces difficultés, une proposition de loi est actuellement en cours de débats aux Etats-Unis. Elle vise à permettre aux entreprises privées de recourir légalement et seulement dans certains cas à des mesures de cyberdéfense offensive pouvant constituer des mesures de « hack back »[35]. A la différence de la loi française, la proposition de loi américaine autorise explicitement le fait de porter atteinte à un système d'information d'un attaquant et encadre plus formellement les activités privées de CTI. Si cette proposition de loi est néanmoins controversée pour les risques que le « hack back » peut présenter, elle est l'expression d'un besoin de plus de moyens pour pouvoir faire face aux cybermenaces et pour répondre de manière efficace aux objectifs de la CTI, notamment en matière d'attribution à l'heure où les cyberattaquants sont en mesure de camoufler leurs actes. Le rôle essentiel que joue le secteur privé en matière de CTI invite donc l'Europe et la France à réfléchir également sur la formalisation d'un cadre juridique adapté aux besoins de leurs entreprises privées de CTI au risque de voir ce marché en plein essor continuer à être nettement dominé par les entreprises américaines.

[33] Article 19 du projet de LPM 2019-2025 : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-projet-de-loi/loi-de-programmation-militaire-2019-2025-textes-officiels

[34] https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf

[35] https://www.congress.gov/bill/115th-congress/house-bill/4036/text

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com