Lettre mensuelle – Août 2019 - disponible sur omc.ceis.eu

Table des matières

ANALYSES 2

1. LA DÉSINFORMATION : « ARME DE DISTRACTION MASSIVE » 2

2. ENJEUX ET CHALLENGES DE LA GESTION DE CRISE 8

FOCUS INNOVATION 13

NewsGuard : labéliser les sites d'information pour lutter contre les fake news 13

ACTUALITÉ 15

Souveraineté économique et numérique : les préconisations du rapport Gauvain 15

CALENDRIER 16

16/10 : Petit-déjeuner thématique trimestriel 16

ANALYSES

1. LA DÉSINFORMATION : « ARME DE DISTRACTION MASSIVE » [1]

Le terme de « *fake news* », largement utilisé, recouvre en fait plusieurs phénomènes : erreur, rumeur, mésinfomation, désinformation, etc. Mésinformation et désinformation sont parfois difficiles à distinguer, bien qu'il s'agisse de deux concepts différents : la désinformation consiste à diffuser des informations délibérément fausses ou trompeuses, alors que la mésinformation consiste en la diffusion non intentionnelle d'information fausses, à l'image de la diffusion de *La Guerre des mondes* d'Orson Welles à la radio en 1938 qui généra des réactions de de panique aux États-Unis[2].

Dans les faits, la désinformation prend souvent la forme de contenus qui ne sont pas intégralement faux, mais plus souvent volontairement exagérés, ou biaisés. Par exemple, les médias ayant relayé les quelques scènes de panique réelles générées par l'adaptation radiophonique de *La Guerre des mondes* ont pour la plupart largement exagéré les faits et ont ainsi créé un imaginaire autour de cet événement, car ils ont cherché à produire un effet sur leurs lecteurs.

Dans sa *Petite histoire de la désinformation*[3], Vladimir Volkoff précise que la désinformation repose sur trois éléments :

- « *Une **manipulation de l'opinion publique**, sinon ce serait de l'intoxication ;*
- *Des **moyens détournés** de traitement de l'information, sinon ce serait de la propagande ;*
- *Des **fins politiques**, internes ou externes, sinon ce serait de la publicité.* »[4]

[1] https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf
[2] *Idem.*
[3] Vladimir Volkoff, *Petite histoire de la désinformation*, Éditions du Rocher, 1999.
[4] *Idem.*

Information et désinformation

La perception de l'information par le lecteur, l'internaute, l'auditeur ou le téléspectateur, dépend de la façon dont il la comprend, donc de son propre schéma de pensée, et ce d'autant qu'une information, du moment qu'elle est relayée donc racontée, est empreinte de subjectivité et devient ainsi un choix délibéré de celui qui la relaie. Pour un média, c'est un **choix éditorial** qui suppose deux choix préalables : **le sujet** traité et **la façon** d'en parler.

Plusieurs biais[5] influencent la façon dont un public perçoit une nouvelle et notamment :

- **Effet de vérité illusoire** : une information qui semble familière à un lecteur déjà reçue à plusieurs reprises, même fausse ou erronée, semble plus facilement véridique.
- **Biais de corrélation illusoire** : l'auditoire construit des liens de causalité entre deux faits n'ayant pas forcément de liens directs (ex. : deux individus vaccinés tombent malades, on en conclut que le vaccin est à l'origine de la maladie).
- **Effet de renforcement**: une information, en contredisant une autre, devient la preuve de la véracité de la première (ex. : pour le lecteur convaincu que le régime de Saddam Hussein possédait des armes de destruction massive, lire un texte réfutant cette information le renforcera dans ses convictions initiales).
- ***Hostile media effect***: les informations allant à l'encontre des convictions du lecteur sont perçues comme hostiles à son égard.
- **Biais de confirmation**[6]**:** l'auditoire tend à privilégier les informations qui confirment ses positions.

Certains chercheurs rappellent aussi que la désinformation exploite avant tout « *une paresse intellectuelle naturelle* », qui consiste à relayer des informations « *sans chercher à les étayer par des preuves* »[7], et ce d'autant que les lecteurs ne possèdent souvent pas les moyens de vérifier la véracité des informations[8] et n'en font pas non plus l'effort.

Discerner la « vraie nouvelle » de la « fausse nouvelle » est aujourd'hui d'autant plus difficile du fait de :

- L'**abondance d'informations**, notamment sur Internet, accusé d'amoindrir l'esprit critique des lecteurs confrontés à une surabondance d'informations et tentés de se fier à leur intuition pour décider de la véracité d'une information sans raisonner de manière analytique[9].
- La **multiplication des vecteurs** de diffusion de l'information sur les plateformes numériques et l'**horizontalité des médias sociaux**: chacun peut diffuser l'information qu'il souhaite sans véritable contrôle.

---

[5] https://ici.radio-canada.ca/nouvelle/1173415/pourquoi-croyance-fausses-nouvelles-complots-cerveau-biais-cognitifs
[6] *Idem.*
[7] Rapport « Manipulations de l'information – Un défi pour nos démocraties » du CAPS et de l'IRSEM
[8] Vladimir Volkoff, *Petite histoire de la désinformation*, Éditions du Rocher, 1999.
[9] https://ici.radio-canada.ca/nouvelle/1173415/pourquoi-croyance-fausses-nouvelles-complots-cerveau-biais-cognitifs

- Le **micro-ciblage** (*microtargeting*) qui permet aux médias et réseaux sociaux de ne diffuser à leurs lecteurs que les informations auxquelles ils sont susceptibles d'être réceptifs.

Les outils de la désinformation : les algorithmes de personnalisation

La création de « **bulles de filtrage**[10] » est une stratégie destinée à proposer des contenus « personnalisés » aux internautes. Des algorithmes de personnalisation, aussi appelés algorithmes de recommandations, utilisent entre autres les historiques de recherches, les « j'aime », les cercles de contact et les données de géolocalisation afin de permettre aux moteurs de recherche et aux réseaux sociaux (Facebook, Instagram, Twitter, LinkedIn, etc.) de proposer des résultats de recherche et des contenus (articles de blogs, publicités, vidéos, etc.) adaptés aux préférences et aux opinions des internautes. Ces bulles enferment les lecteurs dans un « *espace cognitif clos* » et « *confortable* », qu'aucune information nouvelle ou différente ne vient concurrencer et qui renforce le biais de confirmation[11].

Les principaux **algorithmes de personnalisation**, sont les suivants[12] :

Filtrage collaboratif

Le **filtrage collaboratif** (*collaborative filtering*), ou algorithme de **recommandation sociale**, repose sur :

- L'analyse du **profil des utilisateurs** (*user-based* ou *user-centric*), en créant une corrélation entre des utilisateurs aux profils similaires (préférences, intérêts, etc.) dans leur voisinage proche (collègues, amis, etc.). Cet outil part du postulat que si ces utilisateurs ont eu un comportement similaire dans le passé, leur comportement futur devrait également l'être. Si l'historique de navigation d'un utilisateur ressemble à ceux de ses collègues, l'algorithme lui propose systématiquement des contenus consultés plus tôt par ceux-ci.
- L'analyse des **contenus** (*item-based* ou *item-centric*) mesure non pas la corrélation entre des utilisateurs mais entre des contenus. Les articles identifiés comme similaires aux articles lus ou « aimés » par un utilisateur lui seront proposé automatiquement par l'algorithme de filtrage.

---

[10] *The Filter Bubble: What The Internet Is Hiding From You*, Eli Pariser, 2012.
[11] https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf
[12] https://www.mediego.com/fr/blog/principaux-algorithmes-de-recommandation/ ; https://blog.octo.com/introduction-aux-algorithmes-de-recommandation-lexemple-des-articles-du-blog-octo/

Recommandation *content-based*

Un algorithme *content-based* ne tient pas compte de l'activité des utilisateurs mais n'analyse que la structure du contenu afin d'y détecter des similarités. L'algorithme répertorie – entre autres – le titre, le nom de l'auteur, ainsi que les mots composant une publication et les compare à d'autres articles. Plus les articles comportent de mots similaires, plus ils sont considérés comme proches et susceptibles d'être proposés à l'utilisateur. L'algorithme *content-based* propose aux internautes des publications dont les champs lexicaux sont similaires à ceux des pages stockées dans leur historique de navigation.

Algorithmes basés sur des règles

Cette méthode établie des règles générales : par exemple, l'algorithme propose aux utilisateurs les publications les plus populaires, sur la base de critères de popularité définis par le site Internet utilisant l'algorithme (ex. : nombre de fois où la publication est lue ou partagée).

Lutter contre la désinformation

Diversifier les contenus proposés aux utilisateurs

Des outils apparaissent pour tenter de percer les bulles de filtrage en proposant aux utilisateurs de réseaux sociaux d'accéder à des **contenus diversifiés**. La KIND Foundation (États-Unis) a par exemple lancé en 2017 l'outil ***Pop Your Bubble***, une application qui accède au compte Facebook des utilisateurs pour les connecter avec d'autres utilisateurs afin de les sortir de leur zone de confort cognitif. ***Pop Your Bubble*** utilise en effet un algorithme de filtrage de manière inversée, pour confronter les internautes à des schémas de pensée différents des leurs. Après avoir intégré des données telles que l'âge, la ville, le sexe et les « J'aime » de l'utilisateur, l'algorithme propose aux utilisateurs de suivre des personnes hors de sa « bulle » afin de diversifier son flux d'actualités.

Le navigateur Chrome propose quant à lui une extension, ***Escape Your Bubble***[13], créée après l'élection de Donald Trump en 2016 et destinée à sortir des utilisateurs de leur « bulle » politique. Les algorithmes utilisés par la solution insèrent dans le fil d'actualités Facebook des internautes des articles et des images relayant des opinions politiques différentes des leurs. C'est également ce que propose l'application ***Read Across The Aisle***[14], qui insère dans le fil d'actualités des réseaux sociaux des articles normalement bloqués par les algorithmes de filtrage et issus de médias jugés par l'outil comme étant à l'opposé des opinions politiques des utilisateurs.

[13] https://chrome.google.com/webstore/detail/escape-your-bubble/meplcffeedlignghmjiohclihjffopoi
https://www.businessinsider.fr/les-algorithmes-peuvent-aussi-vous-aider-a-sortir-de-votre-bulle#decouvrir-quelles-actualites-sont-discutees-en-dehors-de-votre-pays
[14] http://www.readacrosstheaisle.com

Les outils du Media Lab du MIT : laisser aux utilisateurs le choix de leurs filtres

En 2016, le Centre des médias civiques (*MIT's Center for Civic Media*) et le *Media Lab* du MIT (MIT Media Lab) ont développé un prototype de l'outil Gobo[15], proposant aux utilisateurs de Facebook et Twitter de gérer eux-mêmes leurs bulles de filtrage grâce à des curseurs leur permettant de contrôler leurs filtres de contenus. Par exemple, le filtre « politique » permet à l'utilisateur de choisir de recevoir dans son fil d'actualités des opinions politiques proches ou différentes des siennes. D'autres filtres permettent par exemple de contrôler le ton des postes (humoristique par exemple) ou leur popularité. Facebook n'a toutefois pas montré d'intérêt particulier pour cette solution, jugeant qu'elle ne serait pas réellement utilisée par les utilisateurs, peu enclins à véritablement diversifier leur fil d'actualités.

Le *Medial Lab* du MIT a également développé l'outil *Social Mirror*[16], qui utilise la visualisation de données pour montrer aux utilisateurs de Twitter comment se positionne leur réseau de *followers* dans le paysage global de Twitter. La phase expérimentale de l'outil a montré que les utilisateurs de Twitter, notamment les plus actifs politiquement, étaient la plupart du temps cantonnés à des bulles politiques correspondant à leurs opinions.

Vérification de l'information : des outils basés sur l'analyse humaine

Plusieurs outils en ligne proposent de **noter les sites web selon le niveau de fiabilité des informations** qu'ils diffusent. Souvent proposés comme extensions de navigateur, ces outils notent les sites selon un code couleur et donnent aux utilisateurs des informations détaillées sur la notation. Les sites sont notés selon des critères de transparence et de fiabilité, tels que la diffusion ou non de contenu erroné, la correction régulière des erreurs potentielles, la transparence sur les sources utilisées, les sources de financement du site ainsi que l'identité des auteurs des articles. Il est toutefois nécessaire de garder en tête que les critères sont déterminés par les équipes ayant développé la solution et reflètent ainsi une certaine conception de la transparence et de la fiabilité. L'évaluation de ces critères (déterminés pour être objectifs) est également susceptible d'être influencée par la subjectivité des évaluateurs.

Le site du Monde propose quant à lui à ses lecteurs le **Décodex**[17], un moteur de recherche qui permet de vérifier la fiabilité d'un site à partir de son URL. L'outil est disponible sous la forme d'extensions Chrome et Firefox et avertit l'internaute qui consulte un site pouvant contenir une fausse information par une fenêtre « pop-up ». Un symbole « D » ajouté à la barre d'extensions se colore selon la fiabilité du site visité (rouge pour les sites diffusant régulièrement des informations fausses, orange pour les sites dont la fiabilité est douteuse et bleu pour les sites satiriques) et permet d'accéder à des informations détaillées sur le site concerné.

La start-up américaine **NewsGuard**[18] a elle aussi développé un outil de notation de la fiabilité des sites d'informations sur la base de neuf critères de fiabilité et de transparence. La solution fonctionne aujourd'hui au Royaume-Uni, en Italie, en Allemagne et, depuis mai 2019, en France (voir Focus Inno).

---

[15] https://www.technologyreview.com/s/611826/technologists-are-trying-to-fix-the-filter-bubble-problem-that-tech-helped-create/

[16] https://www.media.mit.edu/projects/social-media-mirror/overview/

[17] https://www.lemonde.fr/les-decodeurs/article/2017/01/23/le-decodex-un-premier-premier-pas-vers-la-verification-de-masse-de-l-information_5067709_4355770.html

[18] Un Focus innovation est dédié à cette solution dans le bulletin OMC du mois d'août 2019

Les réseaux sociaux en guerre contre la désinformation

Les Etats-Unis sont particulièrement visés par l'utilisation des réseaux sociaux à des fins de désinformation, qu'elle soit volontaire, par la création de faux profils, ou qu'elle soit le résultat des bulles de filtrage. L'article *« Bulles de filtrage : il y a 58 millions d'électeurs pro-Trump et je n'en ai vu aucun*[19] *»* souligne par exemple le rôle des algorithmes de filtrage dans le résultat des élections présidentielles américaines de 2016 qui ont élues Donald Trump. De même, en 2018, Facebook a fermé des comptes et pages soupçonnés de publier volontairement des informations douteuses dans le contexte des élections législatives américaines[20]: 32 comptes Facebook et Instagram[21] accusés « *d'accentuer les rivalités idéologiques* » en juillet 2018, et 82 comptes et pages Facebook accusés de publier « *des contenus politiquement clivants* » en octobre 2018. Certaines de ces pages comptaient jusqu'à 1 million d'abonnés. Les algorithmes de personnalisation font d'ailleurs le jeu de ces faux comptes car les contenus sont créés afin d'apparaître sur les fils d'actualités des internautes consultant des publications similaires. Facebook a même mis en place une cellule de crise[22] dédiée à la surveillance de l'information diffusée sur ses réseaux, notamment en périodes électorales.

La Russie est quant à elle massivement accusée de répandre des « *fake news* » dans le cyberespace. En janvier 2019, Facebook a supprimé plus de 500 pages accusées de diffuser de fausses informations sur les opposants russes et de l'Ukraine[23]. Ces pages, imitant le style de personnalités politiques dans le but d'influencer l'opinion des lecteurs, étaient conçues pour apparaitre dans les fils d'actualités des utilisateurs russes en Europe, en Asie centrale, dans le Caucase et en Ukraine. Le réseau Instagram aurait également été largement utilisé par la Russie au cours des élections américaines de 2016, avec des comptes tels que @blackstagram, @feminismtag, @american.veterans, etc. diffusant des opinions clivantes sur les candidats Donald Trump et Hillary Clinton.

[19] https://www.numerama.com/tech/207428-bulles-de-filtrage-il-y-a-58-millions-delecteurs-pro-trump-et-je-nen-ai-vu-aucun.html

[20] https://www.la-croix.com/Sciences-et-ethique/Numerique/Facebook-supprime-32-comptes-manipulation-politique-Etats-Unis-2018-08-02-1200959376 ; https://lexpansion.lexpress.fr/actualites/1/actualite-economique/facebook-continue-sa-lutte-anti-manipulation-politique-l-iran-pointe-du-doigt_2044705.html

[21] Instagram appartient au groupe Facebook.

[22] https://siecledigital.fr/2019/01/30/facebook-va-creer-une-war-room-pour-lutter-contre-les-fake-news-au-moment-des-elections-europeennes/

[23] https://siecledigital.fr/2019/01/19/fake-news-facebook-a-supprime-plus-de-500-pages-de-propagande-gerees-par-des-russes/

La multiplication des informations et des prises de positions, associée aux biais cognitifs, a tendance à pousser les internautes, lecteurs ou téléspectateurs à prendre position et à rallier des camps. Il y a donc sans conteste une concurrence informationnelle. Qu'il s'agisse de la Russie, des États-Unis ou d'autres États, voire d'entités à plus petite échelle, l'utilisation de l'information à des fins politiques n'est pas nouvelle. Elle prend toutefois une ampleur sans précédent du fait de l'expansion permanente du cyberespace et de la multiplication des vecteurs d'information.

2. ENJEUX ET CHALLENGES DE LA GESTION DE CRISE

Cet article fait suite aux interventions sur la gestion et la communication de crise de l'événement Cyberdéfense et Stratégie du 2 juillet 2019.

On dit souvent qu'il existe aujourd'hui deux catégories d'entreprises, celles qui ont été attaquées et celles qui ne l'ont pas été. Ou plus précisément, celles qui ont été attaquées et celles qui ne le savent pas encore. De fait, la question pour une organisation n'est pas tant de savoir si elle sera attaquée, mais plutôt quand et comment, et avec quelles répercussions pour son fonctionnement, ses activités et son image, voire dans certains cas son existence même.

A titre d'exemple, on estime que l'entreprise Merck aurait à elle seule subi 310 millions de dollars de dommages[24] suite à l'attaque NotPetya de 2017 et a été contrainte dans les mois qui ont suivi l'attaque à un arrêt opérationnel de longue durée lié à des ruptures d'approvisionnement.

Dans ce contexte, et alors que le risque de cyber-attaques contre les entreprises ne cesse de croître, il est indispensable pour une organisation de se doter de capacités de gestion et de communication de crise permettant de faciliter la reprise de ses activités et d'assurer sa résilience.

Ces capacités doivent reposer sur une combinaison de mesures organisationnelles, d'outils technologiques et de méthodologies, à chaque étape de la gestion de crise.

1. Prévention

Avant même qu'une crise ne survienne, certaines mesures ou dispositifs très simples permettent de renforcer au quotidien la résilience du système d'information (SI) d'une organisation et de contenir la propagation de cette crise le cas échéant, comme par exemple :

- Appliquer les mesures basiques d'hygiène informatique : effectuer les correctifs de sécurité, cloisonner certains flux sur le SI, gérer les droits d'accès de façon rigoureuse, etc.
- Renforcer la diversité et la flexibilité des systèmes informatiques, par exemple en y intégrant des équipements fonctionnant sous Mac OS ou Linux pour limiter le risque de propagation des malwares à

[24] https://www.lemagit.fr/actualites/450429505/NotPetya-des-couts-dans-la-duree-pour-Merck

l'ensemble du parc – ces derniers étant en grande majorité conçus contre des systèmes fonctionnant sous Windows ou ne ciblant qu'un seul OS.

- Séparer les sauvegardes du reste du système pour éviter qu'elles ne soient compromises en cas d'incident, et afin qu'elle puissent donc être utilisées pour restaurer le SI le cas échéant.
- Revoir et mettre à jour régulièrement les plans d'alerte et de continuité d'activité, et étendre le système de gestion de crise à la cybersécurité.

Ces précautions et bonnes pratiques ne sont cependant pas suffisantes pour éliminer le risque d'une attaque d'ampleur. Les organisations doivent donc également se préparer à faire face à une crise et, si besoin, à mettre en œuvre les moyens nécessaires et des dispositifs dédiés.

2. Préparation et anticipation

Les récentes attaques (Wannacry, NotPetya…) ont rappelé que ni les équipes de l'entreprise touchée ni les autorités appelées pour y répondre ne sont suffisamment préparées pour faire face à des attaques de cette nature et de cette envergure.

D'autre part, la survenance d'une crise est trop souvent synonyme de panique, à la fois pour l'équipe dirigeante qui voit la crise se diffuser sans la comprendre ni pouvoir y remédier, et pour les équipes techniques qui se voient privées des outils leur permettant d'investiguer ou de reprendre la main sur les équipements affectés (outils d'administration, schémas réseaux…)

Pour réagir rapidement, efficacement et aussi sereinement que possible à une crise, les organisations peuvent se préparer en s'appuyant sur :

- **L'élaboration de process et d'une méthodologie de gestion de crise dédiés**, et notamment **d'une matrice de responsabilités RACI** (*responsible, accountable, consulted et informed*). Celle-ci permet d'attribuer les rôles et responsabilités de chacun en cas de crise et donc de déterminer à l'avance quelles sont les actions à mener et par qui. De même, planifier et séquencer en amont les grandes étapes de la gestion de crise (ex. : points quotidiens avec l'ensemble des acteurs concernés, notification des instances et organisations devant être informées, rythme des actions de communication, etc.) permet de fluidifier la réponse à incident quand il survient.
- **En amont, l'entrainement des personnels et des équipes opérationnelles –** par exemple via des simulations de crise ou des exercices de mise en situation – permet d'apprendre à mieux gérer les imprévus et à mieux appréhender les étapes à suivre en cas de crise majeure. Ce type d'exercices permet par ailleurs de **sensibiliser la chaîne décisionnelle** à la nécessité de disposer des ressources humaines, techniques, financières dédiées à la cybersécurité.
- Le déploiement, en amont, d'un **dispositif logistique adapté et activable dès que la crise survient.** Il s'agit par exemple de pouvoir :
  - Mettre à disposition une **salle ou un espace dédi**é (éventuellement isolé), à l'accès restreint.

- Adapter les r**ythmes et horaires de travail** des équipes de gestion de crise qui seront amenées à travailler de nuit, et prévoir par exemple un système de rotation des personnels pour leur permettre de travailler en continu ;
- Prévoir de pouvoir **monter un SI parallèle** au SI compromis le cas échéant.
- La création d'un **réseau de partenaires et experts externes** qui pourra être sollicité si l'organisation ne dispose pas en interne de toutes les compétences nécessaires, car la phase de remédiation suite à une attaque nécessite la mobilisation d'une multiplicité d'expertises et de compétences techniques différentes et complémentaires.

Ces dispositifs, process et méthodes préalablement définis doivent permettre aux équipes de l'organisation affectée de gérer rapidement et plus efficacement la crise et la réponse à incident.

3. Réponse et réaction

L'essentiel pour une organisation victime d'une cyberattaque est d'assurer la continuité de ses activités. Dans l'immédiat – post-crise – et avant même de lancer le processus de reconstruction, elle doit d'abord trouver de nouveaux moyens de communication et de partage des informations. Les applications de messageries grand public, moins sécurisées que leurs équivalents professionnels mais qui ont l'avantage d'être utilisées par le plus grand nombre (WhatsApp par exemple), peuvent dans ce cas s'avérer utiles.

L'organisation victime doit ensuite très rapidement envisager la reconstruction de son système d'information et limiter les atteintes à sa réputation et à son image auprès de ses employés, clients et du grand public. La réponse à la crise passe ainsi par plusieurs étapes qui peuvent être menées en parallèle :

Diagnostique et investigation

Quand un incident survient et afin de pouvoir mettre en place un processus de gestion de crise dédié, l'organisation victime doit d'abord le qualifier, c'est-à-dire en déterminer la nature, l'ampleur, et identifier quels systèmes et équipements sont affectés.

Sur le plan technique, les équipes dédiées doivent investiguer sur la cause de l'attaque (malware, chemin d'entrée de l'APT, failles dans le système d'information, etc.), ce qui doit notamment permettre de :

- Identifier le « **patient zéro**», à l'origine de la propagation au sein du système d'information de l'entreprise ;
- Définir les **éléments de remédiation** dans le but de protéger et reconstruire tous les domaines du système d'information (serveurs, postes de travail, etc.).
- Collecter des **éléments de preuve** permettant à l'entreprise de se ménager des possibilités d'action judiciaire et assurantielle.

Les équipes de l'entreprise affectée peuvent être accompagnées dans leurs efforts par des organisations spécialisées, comme les CERT (*Computer Emergency Response Team*) ou les agences nationales de protection des SI, à l'instar de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Mise en place d'une structure de gestion de crise

Dans le même temps, une structure de gestion de crise impliquant une diversité d'acteurs représentant les différents métiers et fonctions de l'organisation doit être mise en place.

Cette dernière peut par exemple comprendre :

- Un comité de crise au niveau de la direction générale, chargé de prendre les décisions stratégiques pour l'organisation ;
- Une structure « business » chargée à la fois d'identifier des moyens de continuer à produire et faire fonctionner l'organisation sans système informatique, et d'autre part de décider de l'ordre et de la chronologie du redémarrage des différents réseaux de l'organisation ;
- Une équipe de crise IT, chargée de l'investigation et de la définition d'un plan de reconstruction (des postes de travail, du réseau, de l'Active Directory, des serveurs applicatifs…) et le plan de défense du SI (dans un objectif de re-sécurisation du réseaux).

Les équipes chargées de la gestion de crise doivent, dès le début de leur intervention, documenter précisément leurs actions sous forme d'un journal présentant la chronologie des événements et des actions, si besoin en version papier si le SI est compromis. Doivent être consignés notamment : le signalement de l'incident, l'investigation, la collecte des preuves, les échanges avec les partenaires, prestataires et utilisateurs. Cette documentation permettra de centraliser les informations connues sur l'incident (avec un accès restreint si besoin), nécessaires à l'organisation *in fine* d'un retour d'expérience sur la gestion de la crise.

4. Remédiation et reconstruction

La reconstruction du système d'information et le retour à la normal est un travail de longue haleine : on estime ainsi à 3 semaines en moyenne le temps de redémarrage. Reconstruire le SI pour revenir à la normale nécessite notamment de réinstaller tous les postes de travail compromis. Plusieurs solutions permettent d'accélérer le processus comme, par exemple :

- Confier aux collaborateurs la réinstallation de leurs postes de travail, grâce à des clés USB, ce qui permet aussi de les impliquer dans la résolution de la crise ;
- Le recours à des services cloud et de virtualisation, qui permettent de cloner certains systèmes.
- Les fournisseurs et partenaires de l'entreprises affectée peuvent également représenter des relais d'accélération de reconstruction du système d'information, notamment parce qu'ils possèdent parfois des bases de données qui auraient été perdues sur le système affecté, etc.

5. Communication

La **communication de crise** de l'entreprise constitue l'un des volets essentiels de la gestion de crise.

Elle se prépare en amont, notamment sur les réseaux sociaux, de plus en plus utilisés par les entreprises car les publications sur ces réseaux atteignent instantanément un public vaste et varié et permettent de construire

et fidéliser sur le long terme un réseau de *followers*. Les réseaux sociaux permettent ensuite, en temps de crise, de communiquer aisément et rapidement pour informer le public et les employés de l'organisation touchée du déroulement et de la résolution de la crise.

Lorsqu'un incident survient, une communication de crise coordonnée et bien préparée permet d'éviter que ce dernier ne se transforme en crise médiatique s'il est mal géré et que la communication est défaillante ou inadaptée.

Pour gérer au mieux la communication de crise dans les premières heures et éviter une perte financière ou une atteinte à la réputation et à l'image de l'organisation, celle-ci peut s'inspirer d'un certain nombre de bonnes pratiques.

- **Le porte-parole** occupe une place majeure lors d'une crise. Représentant de la société aux yeux du public et des médias, ce rôle doit être attribué au préalable, à un membre du personnel entraîné à ce type d'exercice. Un guide de questions-réponses permet de définir des éléments de réponse que le porte-parole peut aisément assimiler pour faire passer rapidement les bons messages en cas de crise.
- Les **objectifs de la communication doivent ensuite être fixés très rapidement**: qui s'agit-il d'informer (le public, les employés, les investisseurs) et quel est l'objet de la communication (informer, rassurer…) ?
- En fonction de ces objectifs, il convient ensuite d'identifier les **bons canaux de communication** (les réseaux sociaux par exemple) pour positionner l'entreprise concernée comme l'interlocuteur officiel et le détenteur d'informations fiables ;
- **Il est nécessaire de doser la réactivité et la régularité** de la communication, c'est-à-dire ne pas se précipiter, ni trop attendre, ni communiquer trop peu ou trop souvent,
- Surtout, l'importance de la **communication interne** ne doit pas être sous-estimée, car elle permet de rassurer les équipes et d'éviter la panique au sein d'une société déjà déstabilisée par la crise. Et ce d'autant que les employés de l'entreprise touchée peuvent, s'ils sont correctement informés par leur hiérarchie des mesures et des actions concrètes qu'elle mène, faire office de relais fiables.

La communication fait donc partie intégrante du dispositif de gestion de crise, et doit fait l'objet d'une stratégie dédiée.

Conclusion : la sortie de crise

Le processus de gestion de crise et de retour à la normale doit s'accompagner d'efforts de long terme destinés à renforcer la cybersécurité et la résilience de la société car, même reconstruit, le SI pourra faire l'objet de nouvelles attaques. Une organisation se doit donc d'être proactive, pour identifier sans cesse de nouvelles solutions lui permettant protéger au mieux ses systèmes, ainsi que ses données et celles de ses clients.

Pour l'organisation affectée, l'organisation d'un retour d'expérience doit aussi permettre d'évaluer la façon dont la crise a été gérée et, à plus long terme, de réfléchir aux moyens d'améliorer les processus et méthodologies déployés.

FOCUS INNOVATION

NewsGuard : labéliser les sites d'information pour lutter contre les fake news

Présentation

Fondée aux États-Unis en 2018 par Steven Brill et Gordon Crovitz, journalistes et entrepreneurs des médias, NewsGuard emploie aujourd'hui environ 35 personnes sur 4 pays : Royaume-Uni, Italie, Allemagne, et, depuis le 22 mai 2019, la France. L'équipe française comprend 7 membres et est pilotée par Alice Antheaume, directrice de l'école de journalisme de Sciences Po.

Newsguard propose de noter la fiabilité et la transparence des sites d'information sur 9 critères fixés par ses experts. Les notes, formalisées par des boucliers de couleurs, sont accessibles aux utilisateurs via une extension compatible avec les principaux navigateurs (Chrome, Safari, Edge, Firefox) et moteurs de recherche (Google, Bing, Qwant, Duck Duck Go). Les notes sont également disponibles depuis Facebook et Twitter via les navigateurs partenaires.

Le business model

Le modèle économique de NewsGuard repose sur la vente de licences mensuelles aux grands acteurs du numérique, notamment Microsoft ou Google.

NewsGuard compte parmi ses investisseurs le groupe publicitaire français Publicis. En dehors des co-fondateurs, les autres investisseurs ne participent pas au processus de notation et à l'attribution des labels.

La solution

Un algorithme pour identifier les sites à noter

Les sites devant être notés sont identifiés par un algorithme qui analyse le nombre de contenus qu'ils publient et partagent en ligne. Il peut donc s'agir de médias reconnus mais aussi de blogs. En mai 2019, NewsGuard avait ainsi analysé près de 60 sites français, soit 70% de l'information partagée en ligne, et avait estimé sa progression à 90% dans les 2 mois suivants.

L'expertise humaine pour les analyser

Les sites sélectionnés sont ensuite analysés par les équipes de chaque pays, accompagnées d'un comité consultatif composé entre autres de Jimmy Wales, co-fondateur de Wikipédia, selon 9 critères évaluant leur capacité à :

- Ne pas diffuser de contenu erroné (22 points)
- Rassembler et présenter les informations de façon responsable (18 points).
- Corriger ou clarifier régulièrement leurs erreurs (12,5 points),
- Distinguer les informations des opinions (12,5 points)
- Éviter les titres trompeurs ou fallacieux (10 points).
- Mentionner le nom propriétaire du site et ses sources de financement (7,5 points),
- Signaler clairement la publicité (7,5 points),
- Fournir des informations sur les dirigeants du site et mentionner d'éventuels conflits d'intérêts (5 points)
- Préciser le nom des créateurs de contenu et indiquer leurs coordonnées (5 points).

Les sites sont notés sur 100 points qui permettent d'obtenir les labels suivants :

- A partir de 60/100 et au-dessus : "bouclier vert", gage de qualité
- Moins de 60/100 : "bouclier rouge" accompagné d'un message d'avertissement à l'attention du lecteur.
- Site satirique : « bouclier jaune »
- Site hébergeant du contenu généré par ses utilisateurs eux même et non vérifiable « bouclier gris »

Les sites ont ensuite la possibilité d'améliorer leur note en modifiant leurs pratiques journalistiques sur les critères déficients. NewsGuard estime que c'est aujourd'hui le cas de 25% des sites analysés dont Al-Jazeera English, qui a rendu public le fait que son site était détenu par le gouvernement du Qatar après l'analyse de NewsGuard.

Perspectives

La startup a levé 6 millions de dollard depuis sa création en 2018 et comptait en 2019 sur un chiffre d'affaires de 2 millions de dollars, avec l'objectif de devenir rentable d'ici fin 2020 ou début 2021.

En janvier, NewsGuard et Microsoft ont signé un partenariat permettant à la start-up d'installer son service par défaut sur la version mobile du navigateur Edge.

ACTUALITÉ

Souveraineté économique et numérique : les préconisations du rapport Gauvain

Dans le cadre d'une mission confiée par le Premier ministre, le député Raphaël Gauvain a rendu public son rapport « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » le 26 juin 2019[25]. Le rapport dresse un état des lieux de l'application extraterritoriale de la législation américaine et de l'extension de cette pratique à la Chine, à l'Inde ou encore à la Russie, et en souligne les risques pour la souveraineté économique et numérique de la France et de l'Europe.

Le rapport rappelle que le *Cloud Act* du 26 mars 2018 donne de fait aux autorités américaines la possibilité de s'affranchir des dispositifs de l'entraide judiciaire, et comporte donc un risque d'espionnage économique et d'atteinte à la confidentialité d'informations sensibles pouvant mettre en cause les intérêts économiques essentiels de la France. Le *Cloud Act* permet en effet aux autorités américaines, dont le FBI, d'obtenir directement des données stockées en Europe par des hébergeurs américains, dans le cadre de la lutte contre les « crimes graves » et de la protection de la sécurité des États-Unis.

Le risque que fait peser le *Cloud Act* sur les données sensibles françaises et européennes doit toutefois être sensiblement relativisé, notamment car cette législation ne concerne que des hébergeurs américains et qu'il existe désormais un dispositif européen de protection des données personnelles avec le RGPD. Il n'en demeure pas moins que de nombreuses entreprises européennes et française ont recours aux services des GAFAM et peuvent donc être affectés indirectement. C'est pourquoi le rapport Gauvain préconise de légiférer pour protéger ces entreprises contre la transmission par les hébergeurs, de leurs données autres que personnelles aux autorités étrangères. Le rapport envisage les mesures suivantes:

- Une procédure de contrôle préalable sur la communication des données sollicitées par les autorités étrangères, avec obligation de signalement pour les opérateurs de services numériques auprès du Service à l'information stratégique et à la sécurité économiques (SISSE), placé sous l'autorité de la Direction générale des entreprises (DGE) au sein du ministère de l'Économie. Cette autorité serait mandatée pour juger de la recevabilité des requêtes des autorités étrangères ;
- La possibilité pour l'ARCEP de sanctionner par une amende pouvant aller jusqu'à 4% du chiffre d'affaire les opérateurs de services numériques transmettant aux autorités étrangères des données sans passer par les canaux d'entraide judiciaire.

Notons que la sanction prévue par le rapport Gauvain, qui rappelle le régime mis en place par le RGPD, semble dissuasive mais pourrait avoir pour conséquence de complexifier la coopération des entreprises françaises avec les autorités étrangères en cas d'enquête internationale. Elle pourrait notamment rendre difficile la conclusion d'un DPA avec les autorités américaines, un accord permettant de se soumettre à

[25] https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/194000532.pdf

certaines obligations pour éviter des poursuites pénales[26]. L'esprit du rapport s'inscrirait ainsi dans la volonté de « faire coïncider les frontières étatiques, régaliennes, avec les frontières technologiques »[27].

Enfin, le rapport Gauvain préconise de « favoriser par tous les moyens possibles l'émergence d'acteurs français ou européens de taille pertinente dans ce domaine »[28].

CALENDRIER

16/10 : Petit-déjeuner thématique trimestriel

Deep Fakes : armes de guerre de la désinformation

Les *deep fake, ou « hypertruquages »*, sont des techniques de synthèse d'image reposant sur les technologies de l'intelligence artificielle (IA) et permettant de reproduire ou de créer de toutes pièces des contenus vidéo et audio. Outre leur utilisation dans le cadre de campagnes de dénigrement de candidats politiques et de manipulation des résultats, les *deep fake* peuvent aussi être employées à différents usages malveillants : opérations de déstabilisation, escroqueries, manipulation de preuves… A mesure que les technologies qui les sous-tendent se développent, les outils et solutions permettant de s'en protéger se multiplient également : algorithmes de détection, solutions d'authentification,…Au-delà du potentiel d'innovation qui résulte de cette surenchère technologique, *les deep-fakes* constituent un véritable enjeu commercial, politique et sécuritaire.

Comment se construit une *deep-fake* et quels sont ses fondements techniques et technologiques ? Quels risques représente l'utilisation malveillante d'une *deep fake* et avec quel potentiel de nuisance, voire quels dangers ? Enfin, existe-t-il des moyens efficace de s'en prémunir ?

[26] N. Lenoir, *Le rapport Gauvain et la protection des « intérêts économiques essentiels » de la France*, La Semaine Juridique, édition générale n° 29, 22 juillet 2019.
[27] O. de Maison Rouge*, Le rapport Gauvain : de la sécurité à la souveraineté économique*, Revue internationale de la compliance et de l'éthique des affaires n° 4, aout 2019.
[28] https://www.challenges.fr/entreprise/face-au-cloud-act-americain-le-grand-retour-du-cloud-souverain-franais_664976

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