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

Table des matières

ANALYSES

1. VERS UN DURCISSEMENT DU CADRE REGLEMENTAIRE DANS LA LUTTE CONTRE LES CONTENUS HAINEUX ET TERRORISTES EN LIGNE ?

15 mars 2019 : l'auteur de l'attentat dans deux mosquées de Christchurch (Nouvelle-Zélande) diffuse en direct son acte sur Facebook, relayé ensuite sur YouTube.

2016 : Larossi Abballa utilise Facebook Live lors de l'assassinat de deux policiers à Magnanville. Il y réaffirme son allégeance à Daech.

Décembre 2015 : la tuerie de San Bernardino en Californie amène les familles de trois victimes à porter plainte contre les principaux réseaux sociaux, considérant qu'ils représenteraient « des instruments de l'expansion de l'État islamique » (EI). La même année, à la suite des attentats de Paris, une famille porte elle aussi plainte contre Facebook, Google et Twitter pour « soutien matériel » à l'EI, les accusant d'avoir constitué un outil de communication.

Ces quelques exemples, loin d'être des cas isolés, démontrent bien l'utilisation des réseaux sociaux pour la préparation ou la commission d'actes criminels ou terroristes et posent de nombreuses questions : les plateformes doivent-elles porter la responsabilité des contenus haineux publiés par leurs utilisateurs ? Les gouvernements sont-ils en droit d'imposer des règles de modération des contenus ? Comment tenir compte des gros écarts de moyens entre les grandes plateformes Web et les petits acteurs de l'Internet ?

État des lieux des dispositions juridique en Europe

Si les gouvernements se sont saisis du problème il y a quelques années, ils semblent désormais chercher un « coupable » et font pression sur les plateformes. Deux principales raisons à cela :

1. L'amoncèlement d'affaires liant des actes terroristes ou contenus haineux aux réseaux sociaux, qui oblige les pouvoirs publics à réagir plus fermement. En témoigne l'Appel de Christchurch[1] du 15 mai 2019, réunissant, à l'initiative du Président de la République Emmanuel Macron et de la Première ministre de Nouvelle-Zélande, Jacinda Ardern, 10 chefs d'État et de gouvernement, dirigeants d'entreprises et organisations du numérique décidés à agir contre le terrorisme et l'extrémisme violent en ligne.

[1] https://www.elysee.fr/emmanuel-macron/2019/05/15/appel-de-christchurch-pour-agir-contre-le-terrorisme-et-lextremisme-violent-en-ligne

2. Le phénomène *fake news* / *deep fake,* amplifié par les différents scandales d'ingérence étrangère dans les élections américaines et européennes, qui a créé des conditions favorables au renforcement du cadre réglementaire permettant de contrôler les réseaux sociaux. Conscients de l'influence politique considérable que ces fausses informations peuvent avoir sur l'opinion publique, les États ne semblent avoir d'autre choix que de se saisir de la question de la modération des contenus et du chiffrement. Le 5 juin 2019, plusieurs parlementaires européens ainsi que des membres de la société civile et de la Commission transatlantique sur l'intégrité des élections[2], ont ainsi signé conjointement une lettre appelant les présidents des institutions européennes, d'une part à coopérer dans la lutte contre les abus des plateformes sur les enjeux liés à la démocratie et aux élections, et d'autre part à renforcer les règlementations existantes en matière de responsabilité et de surveillance des réseaux sociaux.

A l'échelle européenne

En 2016, Facebook, Twitter, YouTube et Microsoft ont signé avec la Commission européenne un code de conduite contre les discours de haine, s'engageant ainsi à examiner en moins de 24 heures la majorité des signalements validés demandant la suppression des contenus.

Plus récemment, la révision en avril 2018 de la directive dite « SMA » sur les services de médias audiovisuels prévoit « des règles plus strictes en matière de lutte contre les discours haineux et contre la provocation publique à commettre des infractions terroristes » dans les services de médias audiovisuels. Elle s'applique désormais aux plateformes de communication publique et de partage de vidéos qui doivent ainsi prendre des mesures pour protéger les jeunes publics de ces contenus.

A cette directive s'ajoute la proposition de règlement sur le retrait des contenus terroristes en ligne, soumise en décembre 2018 et actuellement examinée au Conseil en première lecture, qui revoit à la hausse les obligations pesant sur les hébergeurs, notamment en matière de vigilance.

A l'échelle nationale

Chaque année, la France, le Royaume-Uni et l'Allemagne sont les premiers demandeurs auprès de Google d'informations sur ses utilisateurs (après les États-Unis). Sans surprise, ces trois pays disposent déjà ou développent un arsenal juridique visant à réglementer davantage les réseaux sociaux.

En Allemagne

L'Allemagne s'est très vite positionnée en chef de file de l'encadrement des plateformes du numérique, les menaçant de sanctions à plusieurs reprises. Alors que le pays avait obtenu dès 2015 un engagement de Facebook à effectuer le travail de modération en moins de 24 heures (soit un an avant le Code de conduite),

[2] La Commission transatlantique sur l'intégrité des élections (*Transatlantic Commission on Election Integrity* en anglais) résulte de l'union outre-Atlantique d'acteurs issus de la sphère politique, de la technologie, des médias ainsi que du monde des affaires afin de stopper toute forme d'ingérence dans les élections étrangères à venir. Ce groupe, dont le mandat court jusqu'aux élections américaines de 2020, s'est donné pour ambition de sensibiliser le public, de travailler de concert avec les décideurs politiques pour encourager l'émergence de solutions politiques transatlantiques, et enfin de collaborer avec des entreprises spécialisées dans le développement d'outils de lutte contre la désinformation.

Berlin n'a formalisé ce positionnement que le 1er janvier 2018 avec la loi NetzDG, dite de « contrôle des réseaux sociaux », reprenant l'obligation d'un délai maximum de 24 heures pour la suppression des contenus « manifestement illégaux », mais en l'élargissant à toutes les plateformes comptant au moins deux millions d'utilisateurs. En cas de manquement, une amende pouvant monter jusqu'à 50 millions d'euros est prévue.

Très vite considérée comme liberticide par ses opposants, et remarquée à l'occasion de la suppression temporaire du compte Twitter de la députée d'extrême droite Beatrix von Storch après un *tweet* jugé raciste, la loi semble présenter un bilan mitigé, sinon négatif, un an après sa mise en application. Alors que le délai de 24 heures a bel et bien été respecté, il n'a été appliqué qu'à peu de demandes, 80% des cas ayant été rejetés. Ce qui conduit un chercheur du Centre d'études des politiques européennes de Bruxelles (CEPS) à conclure qu' « *il est difficile, voire illusoire, pour un législateur d'avoir une influence sur la propagation de contenus haineux en ligne* »[3].

C'est dans ce contexte pourtant que vient d'être présenté le rapport *Online Harms*[4] au Royaume-Uni et que vient d'être introduite la proposition de loi française visant à lutter contre la haine sur Internet, considérée par beaucoup comme inspirée du modèle outre-Rhin.

Au Royaume-Uni

Les autorités britanniques font pression sur les géants du Web depuis l'attentat de Londres du 22 mars 2017. Dans son rapport *Online Harms*, publié le 8 avril 2019, le gouvernement entend leur imposer un « devoir de protection », et envisage à cette fin de créer une structure dédiée indépendante en remplacement des agences de régulation existantes. Cette nouvelle structure aurait mandat pour poursuivre des cadres supérieurs de ces plateformes considérés comme responsables devant la justice, pour imposer des amendes allant jusqu'à 4% du chiffre d'affaires de la plateforme, pour décider de bloquer l'accès à cette dernière, et enfin pour commander des rapports de transparence annuels.

En France

La proposition de loi française visant à lutter contre la haine sur Internet, dite Loi Avia et adoptée par l'Assemblée nationale le 8 juillet (434 voix pour, 33 contre et 69 abstentions), vient s'ajouter à deux lois nationales, parfois considérées comme « obsolètes » dans la mesure où elles ont été promulguées avant l'avènement des réseaux sociaux :

- La loi de 1881 sur la liberté de la presse, qui réprime aux articles 24 et 29 l'injure et la provocation à la commission d'infractions graves. Si elle a été durcie à plusieurs reprises ces dernières années (dureté des peines encourues et allongement du délai de prescription), les peines qu'elle prévoit restent difficilement applicables du fait notamment de l'utilisation de pseudonyme ;
- La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004, qui impose aux opérateurs et prestataires de télécommunications, dans son article 6-I-7, de mettre en place un

[3] https://www.france24.com/fr/20190510-macron-zuckerberg-haine-internet-loi-avia-netzdg-allemagne-echec

[4] https://www.gov.uk/government/consultations/online-harms-white-paper

dispositif de signalement accessible et visible, et d'informer les opérateurs publics de toute activité illicite qui leur serait signalée.

Dans ce cadre-là, la proposition de loi, qui sera soumise au Sénat en septembre 2019, repose sur cinq piliers :

- L'obligation pour les plateformes de retirer les contenus haineux sous 24 heures maximum après avoir reçu le signalement ;
- Des sanctions financières dissuasives pour contraindre une plateforme à retirer un contenu (jusqu'à 4% du chiffre d'affaires) ;
- Une procédure de signalement des contenus haineux simplifiée et unifiée ;
- Une levée plus efficace de l'anonymat en cas de délit ;
- Un blocage définitif des sites haineux.

Outre la simplification et l'accélération de la modération des contenus (comme chez son voisin allemand), cette proposition de loi entend donc imposer un véritable « devoir d'agir » et une prise de responsabilité des plateformes, en amont de l'intervention des autorités publiques.

Pour autant, si la France, tout comme ses homologues européens, souligne régulièrement la responsabilité des géants du Web, Facebook a aussi été salué par Paris à plusieurs reprises pour ses initiatives en la matière, telles que l'envoi d'un groupe d'experts français dans les locaux de Facebook en qualité d'observateurs sur les règles de modération. C'est peut-être ce climat favorable qui a décidé le principal réseau social à accepter, le 25 juin 2019, de fournir désormais à la justice française les adresses IP des auteurs de propos haineux, à l'image de ce qu'il fait déjà pour les contenus terroristes et pédo-pornographiques.

Une progression pourtant lente et soumise à de nombreuses contraintes

Outre le débat sur les entraves à la liberté d'expression et les potentiels abus de modération liés à l'appréciation du caractère haineux ou terroriste d'un contenu, trois autres obstacles, trop souvent oubliés, ralentissent les initiatives de renforcement du cadre règlementaire :

« A chaque pays son Internet »[5] ?

Différents modèles d'Internet continuent de s'opposer. Face à « l'Internet californien », libre et autogéré, prétendument « global », et à « l'Internet chinois » [voire à « l'Internet russe » pour certains], conditionné par un État central et des libertés réduites (1,5% des publications WeChat ont été censurées par la Guobao[6] en 2016), la plupart des pays européens prônent un « Internet européen », libre mais régulé. Cette conception pose deux problèmes :

- D'une part, comment imposer une réglementation nationale aux plateformes dont les contenus sont partagés mondialement, si cette règlementation n'est pas compatible avec l'ensemble des autres régulations nationales ? Et dans quelle mesure l'Europe a-t-elle les moyens d'imposer des règles,

[5] Titre d'un article de *Courrier International* du 10/04/2019.

[6] « Police politique » chinoise.

conformes à sa vision de l'Internet, à des plateformes américaines telles que Facebook, qui portent une tout autre vision d'Internet ?

- D'autre part, un « Internet européen » est-il viable s'il cherche à faire co-exister des positions plus ou moins conservatrices en matière de responsabilité et de surveillance ? En témoigne la position britannique, jugée comme étant la plus restrictive du continent, qui a vu son texte de loi, l'Investigatory Powers Bill, être épinglé par la Cour européenne des droits de l'homme (CEDH) en septembre 2018, deux ans après sa signature, et qui continue pour autant d'aller dans ce sens, si ce n'est encore plus loin, avec son Livre blanc *Online Harms*.

A chaque principe son risque d'incompatibilité juridique ?

Le principe de responsabilité que les États tentent d'imposer aux plateformes reste à ce jour incompatible avec la directive « e-commerce » [du Parlement européen et du Conseil du 8 juin 2000] qui n'a certes pas de pouvoir contraignant mais qui prévoit, dans ses articles 13 et 14, que les prestataires de service en ligne et les hébergeurs ne peuvent en principe pas voir leur responsabilité juridique engagée lorsqu'ils stockent des contenus malveillants, faisant l'apologie du terrorisme par exemple. Idem pour la directive SMA, qui contraint les plateformes à prendre des mesures pour lutter contre les contenus haineux sans pour autant remettre en cause l'irresponsabilité de ces dernières. Par ailleurs, la directive dispose qu'en matière de régulation, chaque État membre n'est compétent qu'à l'égard des plateformes établies sur son territoire. Or, en l'occurrence, la plupart et les plus influentes parmi les plateformes concernées sont non seulement non européennes mais ont une portée mondiale.

A chaque plateforme ses moyens ?

En matière de politique de lutte contre le terrorisme et la désinformation, force est de constater que les géants du Web ont tous pris des initiatives, en développant des algorithmes spécifiques et en utilisant des technologies telles que l'Intelligence artificielle (IA) ou le *machine learning*. Facebook est ainsi passé de 10 000 à 30 000 modérateurs et continue d'investir dans son laboratoire d'IA, ce qui permet au réseau social de supprimer 99,8% des faux comptes avant même qu'ils ne soient signalés par les utilisateurs. De son côté, Google a précisé qu'il continuait son engagement via l'approche « *follow the money* », interdisant de ce fait l'accès à sa régie publicitaire à 320 000 éditeurs de publicités malveillantes. Mais qu'en est-il des petites et moyennes plateformes, qui ne disposent pas forcément des outils nécessaires, des capacités techniques ou des ressources pour développer des centres de modération ou des politiques dédiées ? Le rapport *Online Harms* s'adresse par exemple à toutes les entités du Web, sans faire de distinction entre les géants de la toile et les start-ups. De même, certains acteurs français pourraient eux aussi avoir du mal à se conformer aux exigences de la proposition de loi en cours, même si cette dernière entend différencier les plateformes sur la base de leur trafic. Reste donc à trouver le bon équilibre entre tous ces acteurs.

2. LA SECURITE DES OBJETS CONNECTES DANS LE DOMAINE DE LA SANTE

L'utilisation d'objets connectés dans le domaine de la santé est en pleine croissance. Le cabinet d'études Xerfi prédit ainsi plus de 4 milliards d'euros d'investissements pour le marché de la santé connectée d'ici 2020. D'une extrême variété, ces objets connectés regroupent aussi bien de simples capteurs collectant des données sur le bien-être de leurs utilisateurs, que de véritables dispositifs médicaux pouvant être dotés d'un actionneur et donc capables de réaliser une action concrète dans le monde physique. Ces derniers permettent, de façon instantanée, d'obtenir des informations sur l'état d'un patient, de piloter des interventions chirurgicales, d'effectuer des réanimations, des anesthésies ou encore d'administrer des dosages de médicaments en perfusion. Les objets connectés de santé, utilisés comme des dispositifs médicaux, constituent ainsi une aide précieuse pour les médecins cherchant à offrir le meilleur traitement à leurs patients, à toutes les étapes de leur intervention : du diagnostic, au contrôle ou à la prévention et au traitement d'une maladie, d'une blessure, ou d'un handicap.

Du fait de leur multiplicité et de la diversité de leur usage, la sécurité des objets connectés de santé représente un enjeu majeur, car ces derniers représentent aujourd'hui des cibles potentielles pour des personnes malveillantes/cyber-attaquants. Leur utilisation par un grand nombre d'acteurs, les potentielles vulnérabilités dans la conception des programmes, l'insuffisante sécurisation des accès à ces objets, l'utilisation de canaux de communication non chiffrés pour transmettre les données qu'ils collectent ou échangent, ou encore les bugs critiques dans les logiciels sur lesquels ils reposent, sont autant d'éléments qui constituent une porte d'entrée sur tout le système d'information.

L'utilisation croissante de ces objets en matière de santé soulève ainsi de sérieux problèmes de sécurité pour les établissements de santé mais aussi et de plus en plus, pour l'intégrité physique des patients.

Les risques cyber liés aux objets connectés de santé

Les objets connectés de santé sont soumis à plusieurs types de risques communs à l'ensemble de ces objets.

Des risques communs à l'ensemble des objets connectés

Les risques en matière de cybersécurité sont principalement liés aux atteintes à la disponibilité, à la confidentialité et à l'intégrité des données qui sont générées, collectées et transmises par les capteurs et fonctionnalités des objets connectés. Le tableau suivant précise les deux principaux types de risques :

Risque	Exemple
Dysfonctionnement de l'objet lui-même ou dans la transmission/réception des informations	Choc fragilisant un capteur de l'objet ;
	Bug du système d'information lié à une mauvaise configuration ou manipulation ;
	Perte de la connectivité dans un lieu sans réseau .
Piratage à distance ou physiquement du système d'information ou de communication	Captation des données stockées et échangées par l'objet ;
	Prise de contrôle de l'objet et manipulation des données ;
	Blocage du fonctionnement de l'objet connecté.

Des conséquences potentiellement dévastatrices dans le cas de systèmes de santé

Le dysfonctionnement ou le piratage d'un objet connecté de santé peuvent avoir des conséquences à deux niveaux :

- **Au niveau des organismes de santé** : les objets connectés de santé constituent une véritable porte d'entrée dans le système d'information d'un centre médical, dans la mesure où ces objets sont souvent interconnectés et interdépendants de celui-ci. A ce titre, ils peuvent être utilisés pour déstabiliser, l'organisation des systèmes de soins ;
- **Au niveau des patients** : directement rattachés au traitement d'un patient, les objets connectés de santé peuvent divulguer des informations relativement sensibles sur la vie privée des personnes (données de santé, géolocalisation, habitudes alimentaires par exemple) et, dans certains cas, présenter un réel risque pour leur intégrité physique, comme dans le cas du piratage ou du dysfonctionnement d'une pompe à insuline ou d'un *pacemaker* connecté par exemple).

Les risques cyber liés aux objets connectés de santé sont d'autant plus préoccupants que ces derniers sont difficiles à sécuriser.

Les difficultés liées à la sécurisation des objets connectés de santé

La sécurisation des objets connectés se heurte à des difficultés aussi bien organisationnelles que techniques.

Difficultés organisationnelles

Des milliers d'objets connectés d'utilités différentes, d'applications cliniques diverses et mises en œuvre sur des technologies et des infrastructures hétérogènes sont utilisés chaque jour dans les hôpitaux. La difficulté tient donc, pour les équipes chargées d'assurer la sécurité numérique, à assurer la supervision et la gestion de la cybersécurité d'un parc d'équipements aussi large et fourni par différents prestataires.

Dans certains cas, la sécurité de certains objets connectés de santé peut même échapper partiellement ou totalement au contrôle du responsable de la sécurité des systèmes d'information d'un établissement de santé. En effet, certains appareils sont utilisés par le patient en dehors de l'établissement santé et peuvent également être combinés avec l'usage d'un smartphone ou d'une tablette personnelle.

Difficultés techniques

La complexité des objets connectés de santé, qui dépend de la diversité des capteurs qu'ils utilisent et des données hétérogènes qu'ils traitent (images, scans, etc.) ne facilite pas leur mise à jour régulière et leur adaptation aux évolutions technologiques. Leur maintien en condition de sécurité (MCS) est donc difficile, ce qui explique les nombreuses failles qui peuvent concerner tant les logiciels que les composantes de ces objets.

De plus, les capacités de calculs des objets connectés de santé demeurent assez faibles et doivent être concentrées sur le dispositif médical, ce qui a pour conséquence de limiter voire d'exclure des dispositifs de sécurité robustes comme le chiffrement ou des anti-virus par exemple.

Enfin, la plupart des appareils médicaux utilise le Wifi pour transférer les données alors que ce dernier est en général peu sécurisé dans les établissements de santé. Il constitue d'ailleurs le principal « maillon faible » pour l'ensemble des objets connectés, car la plupart des intrusions utilisent ce vecteur. Notons également que beaucoup d'objets connectés sont utilisés sans changement de leur mot de passe d'origine.

Concilier l'innovation des objets connectés, la santé et la sécurité

L'utilisation d'objets connectés pour les soins hospitaliers constitue une innovation majeure qui ne peut se faire sans une sécurité adaptée. Cette nécessaire sécurisation nécessite l'implication de tous les acteurs concernés qui doivent tous contribuer, à leur niveau et au quotidien, à la sécurité de l'environnement dans lequel ces objets évoluent, dans l'objectif de rendre d'éventuelles attaques plus difficiles.

Enfin, au niveau de l'objet et de son utilisation, il est recommandé de se concentrer sur :

- La sensibilisation des personnels et des patients sur une bonne utilisation des objets connectés de santé ;
- Le choix de systèmes faciles à prendre en main par le patient et de composantes, notamment au niveau des capteurs, reconnus pour leur robustesse afin notamment de minimaliser les risques de dysfonctionnement dû à une mauvaise manipulation de l'objet ;
- La mise en place d'un suivi adapté du dispositif qui prévoit les risques de dysfonctionnement et de cyberattaques afin d'être capable d'assurer la continuité des soins en situation dégradée de l'objet connecté de santé.

Sources :

- https://www.ticsante.com/les-objets-connectes-a-l-hopital-sont-en-phase-d-evaluation-de-leur-interet-medical-NS_4092.html
- https://www.frstrategie.org/publications/notes/securite-numerique-des-objets-connectes-l-heure-des-choix-15-2018
- https://www.cybermdx.com/blog/new-vulnerability-disclosure-for-anesthesia-machines-tells-a-bigger-story
- https://www.us-cert.gov/ics/advisories/icsma-19-190-01
- https://www.frstrategie.org/publications/notes/securite-numerique-des-objets-connectes-l-heure-des-choix-15-2018
- https://www.kaspersky.com/blog/hacked-hospital/11296/
- https://www.nextgenges.com/security-vulnerabilities-iot-medical-devices/

FOCUS INNOVATION

WATOO : LE TATOUAGE NUMERIQUE POUR LUTTER CONTRE LES FUITES DE DONNEES

La société

Spin off de l'IMT Atlantique, la société WaToo a été créée en 2016 par deux ingénieurs, Javier Franco-Contreras, qui rédigeait alors sa thèse de doctorat sur la protection par tatouage numérique des bases de données en santé, et son directeur de thèse, Gouenou Coatrieux, du Département ITI (Image et Traitement de l'Image) et du laboratoire LATIM (Laboratoire de traitement de l'information médicale).

Partant du constat que le tatouage numérique offrait une réponse efficace contre les fuites de données, la société propose des outils d'identification et de dissuasion pour lutter contre la fuite, les détournements et les falsifications de données sensibles, qui reposent sur plusieurs brevets déposés par l'IMT.

L'innovation

Les solutions proposées par WATOO reposent sur le principe du tatouage, ou *watermarking*, qui consiste à insérer, voire dissimuler dans un support hôte (image, base de données, document…) des informations permettant à la fois d'assure la traçabilité des données de protéger ce support en matière de droits d'auteur ou d'intégrité. Il peut s'agir par exemple d'identifiants d'utilisateurs ou d'acheteurs…

La support hôte reste ainsi accessible, et la protection par *watermarking* n'a ni d'interférence dans les usages ni d'impact sur le format de stockage des données. Et ce d'autant que le marquage est réversible et permet donc de revenir au support hôte d'origine.

Si la technologie n'est pas nouvelle, son application à la lutte contre la fuite de données l'est en revanche. WATOO a ainsi développé une solution de protection des données basée sur un tatouage numérique, sous la forme d'un traceur dissimulé de manière imperceptible dans les bases de données utilisés par une organisation et qui permet, en cas de fuite ou de redistribution illégale de ces données, d'e identifier l'auteur facilement et rapidement.

Les applications

WaToo propose ainsi 2 outils :

- WaTrack, qui protège des bases de données partagées avec des collaborateurs ou vendues sous licence, et permet d'identifier le partenaire ou le client à l'origine d'une fuite ou d'une revente illégale d'information. Il utilise pour cela un TAG, ou traceur, intégré aux bases de données partagées et qui

contient des informations de traçabilité unique sur un utilisateur et sur l'usage qu'il a fait des données (ID de destinataire et l'ID d'origine, date d'envoi, etc…)

- WaTwall, qui identifie les responsables de détournements ou de fuites de données causées par utilisateurs pourtant autorisés à manipuler les données. Il s'agit cette fois d'une solution intégrée au système d'information d'une organisation et qui permet tracer les données dans les activités quotidienne de cette organisation. Dans ce cas, le TAG agit comme une mesure de dissuasion car les employés sont informés de son utilisation.

Si ces solutions s'adressent à tous les collecteurs et fournisseurs de bases de données, WATOO s'adresse de façon prioritaire aux secteurs clés que sont l'automobile, l'énergie, l'aéronautique, la biochimie et les biotechnologies. Les administrations de la santé, de l'éducation, et le secteur bancaire et financier pourraient cependant également être intéressés.

Actualité et perspectives

Présente au FIC 2019 et citée dans le « radar des start-ups cybersécurité en France » 2019 de Wavestone, Watoo fait partie, depuis novembre 2018, des sociétés du *Village by CA Finistère*, l'accélérateur de projets innovants du Finistère.

Intégrée à l'incubateur régional Emergysp pour construire et développer son offre commerciale, la société a également pu bénéficier d'un prêt d'honneur pour l'amorçage régional (PHAR) qui accompagne les projets risqués à potentiel.

CALENDRIER

05/09 : Université d'été d'HEXATRUST

Pour cette 5ème édition, l'Université d'été d'HEXATRUST et le Cloud Independence Day fusionnent pour un événement sur le thème : Vers une autonomie stratégique européenne ».

Cet événement rassemblera les acteurs de l'écosystème français dans l'objectif de construire ensemble une Europe du numérique résiliente et innovante.

L'événement aura lieu à l'Hôtel Potocki à partir de 16h et suivra le programme suivant :

Pour plus d'informations : https://www.hexatrust.com/ueht2019/

ACTUALITÉ

Création d'un grand campus de la cybersécurité

Le Premier ministre et le Secrétaire d'État chargé du Numérique, Cédric O, ont confié à Michel Van Den Berghe, DG d'Orange Cyberdéfense, la mission de réfléchir au projet de création d'un grand campus de la cybersécurité.

Annoncé lors du Cyberfestival de l'ANSSI le 4 juin 2019, ce projet a pour objectif de réunir l'ensemble des acteurs de l'écosystème français de la cybersécurité (industriels, start-ups, universitaire, agences gouvernementales) afin de renforcer et faciliter :

- La sensibilisation et la formation, dans le but de lutter contre le déficit d'experts et améliorer la prise en compte du risque dans les organisations ;
- Le partage et la mutualisation d'outils, de compétences et de données entre les acteurs du secteur, mais aussi l'échange de bonnes pratiques et les réflexions sur les enjeux et difficultés communes ;
- L'innovation publique et privée, qui doit être mieux accompagnée pour permettre le développement de la filière industrielle de cybersécurité.

Ce campus cyber qui a vocation à être « opérationnel », pourra par exemple proposer aux industriels et aux agences concernées d'accueillir leurs équipes pour partager leurs compétences dans certains domaines dans lesquels ils peuvent être complémentaires. Il devra aussi jouer le rôle de laboratoire pour imaginer les réponses à apporter aux menaces de demain, notamment via des événements et conférences rassemblant les acteurs du secteur.

Cette démarche doit ainsi permettre, en renforçant l'écosystème français, de le positionner, à l'échelle mondiale, comme un pôle d'excellence capable d'attirer et de conserver les talents et comme un acteur incontournable sur la scène internationale.

Les propositions sur la mise en place concrète de ce campus seront remises au Premier Ministre au mois de Novembre, mais plusieurs pistes sont déjà envisagées et notamment la possibilité de déployer, en plus d'un site à Paris, des sites délocalisés qui pourront couvrir des spécialités propres.

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