CYBER CERCLE

collection

PAROLES D'EXPERTS

2021

PAROLES D'EXPERTS

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BENEDICTE PILLIET
Présidente
CyberCercle

Je suis très fière de publier aujourd'hui l'opus 2021, deuxième opus annuel, de nos Paroles d'Experts, inaugurées dans leur format et leur périodicité en avril 2020.

Tout au long de 2021, année encore une fois particulière, nous avons su entretenir la dynamique de publication de contenus que nous avons engagée en 2020 à l'occasion de la crise de la COVID-19.

J'adresse ici mes plus sincères remerciements à tous ceux qui ont ainsi participé à cette dynamique.

En 2021, ce sont 41 tribunes écrites par des parlementaires, des élus locaux, des représentants d'entreprises, de la start-up au grand groupe, d'administrations de l'Etat, des armées, de collectivités, d'associations, d'écoles et d'organismes de recherche que nous avons publiées le vendredi tout au long de l'année.

Des tribunes éclairantes sur des sujets de gouvernance, d'enjeux sectoriels, de réglementation, d'innovation, de développement des territoires, de recrutement et de formation… enjeux de l'évolution de notre société vers une véritable « cybersociété » où plus encore qu'hier la sécurité et la confiance numériques doivent être au cœur de cette transformation.

Ce rythme intense de publication, cette diversité des contributeurs et des sujets abordés, sont les reflets de la philosophie qui nous anime au CyberCercle : permettre un accès ouvert au plus grand nombre à une

expertise de confiance pour développer une culture partagée de sécurité et de confiance numériques, être un vecteur de diffusion et de valorisation d'analyses de personnalités qualifiées, favoriser la réflexion et les échanges constructifs.

Je vous souhaite une bonne lecture et vous donne rendez-vous chaque vendredi sur notre site pour une nouvelle Parole d'Expert !

Données personnelles : mettre fin à la politique de l'autruche

LAURANE RAIMONDO
DPO
Chercheure associée au CLESID

A la mi-novembre 2020, Pôle Emploi ne proposait que trois postes de délégué à la protection des données à l'échelle nationale. Un chiffre qui en dit long sur la manière dont le sujet est perçu au sein des organismes. Largement considérée comme un « empêcheur de tourner en rond », la législation en la matière peine encore bien trop à être appliquée tandis que nous sommes à un carrefour essentiel entre nécessité d'utiliser les données et nécessité de les protéger.

Au-delà des lois, la protection de données à caractère personnel repose sur deux piliers principaux : la cybersécurité et le comportement humain.

Mettons-les en œuvre : déconstruisons l'idée que la protection des données comme la cybersécurité sont affaires des seuls techniciens, édifions une conscience commune, enseignons et accompagnons la population dès les premiers contacts avec les outils numériques. Nous en serons payés de retour.
Faire en sorte que tous se sentent concernés est peut-être ce qu'il y a de plus difficile à mettre en œuvre. Il s'agit ni plus ni moins du levier qui nous fera basculer vers un univers numérique plus sûr en renforçant les remparts bâtis autour du droit fondamental relatif à la vie privée. Prédomine pourtant le traditionnel « je n'ai rien à cacher » concernant ses propres données et un faux sentiment de sécurité se répercutant dans le cadre professionnel. Dissocier l'aspect privé et professionnel de la protection des données est une erreur : qui ne se soucie pas de ses données sera peu attentif à celles des autres et la seule peur de la sanction en cas de violation au sein de son entreprise ou administration a démontré son

inefficacité. Il est également certain qu'une personne n'ayant pas de notion d'« hygiène numérique » présente à l'attaquant deux surfaces d'exposition lorsqu'elle ne crée pas de mur de sécurité entre sa vie privée et sa vie professionnelle, utilisant des mots de passe identiques ou se servant de ses outils professionnels pour gérer des aspects de sa vie personnelle et vice versa.

De cette perception tronquée insinuant l'idée que la protection des données ne concerne que quelques-uns, celle d'une cybersécurité cloisonnée aux seuls techniciens est tout aussi problématique. Là encore, elle est affaire de tous. Une forteresse n'est pas imaginée, dessinée, financée, construite, entretenue et défendue par une seule personne ni même une équipe restreinte, mais par un ensemble d'acteurs connaissant chacun leur rôle, de l'architecte qui en fait une place forte solide aux gardes qui en filtrent les entrées en passant par ceux qui en assurent l'entretien. Il suffit d'une faille pour faire tomber la plus robuste des forteresses comme tout système bien construit. La seule inattention ou faiblesse d'un mot de passe suffiront à laisser le chaos s'insinuer dans le système d'information le plus sécurisé qui soit. Comment douter encore aujourd'hui de la nécessité d'impliquer tous les acteurs d'un organisme ?

Une cyberattaque donnant lieu ou non à une violation de données n'a pas que des conséquences en termes de continuité d'activité, de réputation ou de chiffre d'affaires, c'est comme se retrouver face à son domicile cambriolé : solitude, détresse et impuissance de la victime. L'écran devient noir et ce n'est qu'à ce moment qu'elle se rend compte de la fragilité du système autant que de sa dépendance à celui-ci. Plus que des outils, le smartphone, l'ordinateur ou la tablette sont devenus des prolongements de nous-mêmes et de nos activités à un point suffisamment élevé pour que leur sécurité soit prise au sérieux à degré équivalent : une véritable conscience collective doit se développer autour de la sécurité des données personnelles et des outils numériques.

Le premier smartphone atterrit entre les mains d'un enfant en moyenne entre 10 et 12 ans, s'ensuit une découverte des ressources du cyberespace avec un contrôle extrêmement limité de la part d'adultes souvent eux-mêmes dépassés par les possibilités de ces outils. Les habitudes d'usages

s'adoptent tôt, les mauvaises plutôt que les bonnes auront tendance à perdurer si n'est pas rapidement développé un enseignement commun et régulier dès l'entrée au collège. Faire des prochaines générations des citoyens responsables face à des outils pouvant se révéler dangereux pour eux autant que pour les autres est plus qu'une nécessité, c'est un devoir. Il en va de même avec des adultes ayant vécu l'implémentation progressive du numérique dans leurs organismes comme dans leur vie privée.

Il est courant de constater que ces personnes ont automatisé et rationnalisé les gestes quotidiens nécessaires à leur activité professionnelle : lire et répondre aux e-mails ; utiliser Word ; envoyer des documents ; éventuellement utiliser un logiciel de travail et c'est tout. Elles fonctionnent avec un enclos de sécurité, ne sortent pas du minimum indispensable, sont ancrées sur leurs appuis et de fait, ne développent aucun réflexe de sécurité. La peur de cliquer sur quelque chose qui modifierait le fil du fonctionnement sécuritaire inhibe la curiosité naturelle de l'être humain.

Les forces et faiblesses des outils numériques se situent au même endroit : l'invisibilité du mécanisme. Il y a quelque chose de « magique » à écrire des mots sur un clavier qui parviendront en quelques secondes à un destinataire localisé de l'autre côté de la planète, mais combien sommes-nous à savoir précisément comment tout cela fonctionne ? La réponse à la plupart de nos problématiques se trouve dans cette question. L'absence de connaissances, la division des tâches et l'imperméabilité des informations sont davantage responsables que la direction d'une entreprise traînant à prendre des mesures concrètes en matière de sécurité des données et du système ; qu'un employé manquant de bon sens ou qu'un Etat ne prenant pas suffisamment en main la sécurité numérique globale des organismes relevant de sa juridiction.

De la connaissance jaillira la conscience collective, il s'agit à présent de partager le plus largement possible le seul bien que l'on ne perd pas en le diffusant : le savoir. Toucher toutes les strates de la population utilisant des outils numériques c'est puiser dans toutes les ressources qu'il est possible de mettre en place : l'enseignement pour les plus jeunes ; la formation pour les adultes et les professionnels ; les avantages fiscaux pour

les entreprises et jeunes entrepreneurs du secteur ; l'investissement de la sphère sociale pour les personnes en difficulté, chose qui est d'ailleurs en route avec l'annonce du recrutement de 4 000 conseillers numériques par l'Etat. Nous aurons respectivement à la clef : des jeunes qui sauront protéger leurs propres données et celles qu'ils seront amenés à manipuler plus tard ; des actifs vigilants et pleinement acteurs de la sécurité des données et du système de l'organisme pour lequel ils travaillent ; une offre assez importante pour répondre à des demandes plus nombreuses et précises ; une nouvelle économie stimulée par l'émergence de nouvelles activités qu'il nous appartient de créer ; et enfin, des personnes vulnérables pouvant bénéficier d'un accompagnement de qualité.

Le moment est idéal pour se convaincre de l'utilité de tout investissement visant à sensibiliser, former et accompagner l'ensemble de la Nation aux enjeux autour de la sécurité numérique et de la protection des données. L'optimisme doit prévaloir en la matière, il n'est pas trop tard pour affirmer haut et fort que ces problématiques nous concernent tous autant que nous sommes et qu'il est temps de sonner le tocsin. L'émergence d'une conscience collective permettra à la France de construire une véritable forteresse numérique aux frontières elles aussi invisibles et dessinées par sa propre population.

Alors, qu'attendons-nous ?

Parution le 8 janvier 2021

L'UNECE WP.29, une nouvelle règlementation cybersécurité au service d'un secteur automobile hyper-connecté

SYLVIE VOTTIER

Consultante expert en stratégie, gouvernance et règlementation cybersécurité
ETAS SAS – ESCRYPT

Le volume de données échangées par les véhicules est en constante augmentation, offrant la possibilité de réaliser le diagnostic à distance, l'optimisation de la conduite, la gestion de flotte, l'émergence de nouveaux services. Dans ce contexte de véhicules hyper-connectés, intelligents et autonomes, le risque de cyberattaques est en pleine croissance. C'est pour cette raison qu'une nouvelle règlementation entrera en vigueur, en Europe, en 2022. Cette réglementation de l'UNECE WP.29 porte sur les exigences organisationnelles et techniques de cybersécurité à implémenter dans l'écosystème automobile, incluant les véhicules, les moyens de production et la supply chain. Cette réglementation impose aux constructeurs automobiles d'obtenir la certification d'un Système de Management de la Cybersécurité, d'un Système de Management des Mises à Jour, ainsi que la certification d'une architecture sécurisée par type de véhicule, avant sa mise en circulation.

Le secteur automobile fait face à une transformation digitale sans précédent pour accélérer l'innovation, adapter la production, maintenir en condition de sécurité les véhicules durant leur cycle de vie et offrir de nouveaux services aux usagers. Cette transformation s'opère simultanément à trois niveaux : dans le cœur même du véhicule, au sein de l'industrie automobile (4.0), tout comme dans l'écosystème hyper-connecté, du véhicule communicant avec les autres véhicules, avec les infrastructures routières et électriques, les buildings, la city jusqu'à l'intermodalité des transports de plus en plus intelligents et les services émergeants impulsés également par la Loi d'Orientation des Mobilités.

Des évolutions qui accroissent les surfaces d'attaques cyber

Les évolutions touchent tout d'abord l'industrie automobile, avec un usage croissant d'appareils mobiles, l'IoT, la robotisation, la réalité augmentée, qui tous contiennent des données et enrichissent les services et processus présents dans le cycle de vie industriel.

A cela s'ajoute la modernisation des véhicules eux-mêmes, avec l'émergence des véhicules autonomes, des véhicules hyperconnectés et de la mobilité partagée, ainsi que la digitalisation de la Supply Chain, soit de l'écosystème automobile dans son ensemble.

Les véhicules comptent aujourd'hui plus de 150 ECU (Electronic Control Units) et environ 100 millions de lignes de code, un nombre qui atteindra les 300 millions en 2030, ce qui engendrera probablement de nombreuses vulnérabilités. A ces composants matériels et logiciels s'ajoutent les flots de données nécessaires au maintien en condition opérationnelle et de sécurité des composants, des systèmes et du véhicule. De nombreuses données sont en partie diffusées à l'extérieur du véhicule à travers des moyens de communications fournis par des tiers, pour être analysées au niveau Backend du constructeur automobile, afin d'assurer par exemple la maintenance prédictive. Les données de diagnostic pourront également être accessibles par l'After Market ou d'autres parties prenantes qui les transformeront en nouveaux services pour les usagers ou d'autres organismes.

Les informations propres au véhicule sont donc partagées avec un nombre de parties prenantes en constante augmentation qui ont des niveaux de maturité et des pratiques cybersécurité très hétérogènes.
Par conséquent, il est essentiel de prendre en compte la cybersécurité de manière transverse et au niveau de l'écosystème ; les analyses de risques tenant compte de toutes les interfaces et des interdépendances, et bien sûr devant être capables d'évaluer la criticité de toutes ces parties prenantes. L'objectif est d'être en mesure d'anticiper, de prévenir et d'éviter la gestion de crise, dans un contexte où la sécurité des personnes est primordiale, où le volume de données est considérable, où les flux de communication et les acteurs impliqués sont de plus en plus nombreux.

La convergence Information Technology (IT) et Operational Technology (OT) est inéluctable pour assurer la sécurité des données, des services émergeants, des fonctionnalités du véhicule, et des processus métier de l'automobile, et *in fine* la sécurité des personnes, des biens et de l'environnement. Il faut donc désormais imaginer et implémenter la sécurité de cet écosystème de manière globale, intégrant la sûreté (safety) et la cybersécurité, afin d'assurer la continuité d'activité, la résilience en cas d'incidents et la gestion de crise.

Des données qui deviennent des valeurs Métier stratégiques

Le secteur automobile qui était jusqu'alors concentré autour de la *safety*, voit aujourd'hui également des intérêts financiers à monétiser les données présentes dans le véhicule.

Ce changement de paradigme impose de catégoriser et de classifier les données présentes dans le véhicule, *et pas uniquement au regard de la data privacy*, de définir des critères autour des moyens de collecte, de distribution et d'accès à ces données, d'évaluer leur coût.

Des réglementations et des standards pour renforcer la sécurité

Dans ce contexte de complexification et d'élargissement de la surface d'attaque, des efforts sont menés dans le monde entier pour mettre en place des réglementations et définir des standards permettant d'introduire la cybersécurité dans le cycle de vie des véhicules. Pour n'en citer que quelques-unes, il y a des propositions au Congrès américain, la loi sur la cybersécurité (Cybersecurity Act) dans l'UE, le Programme ICV en Chine et les nouvelles directives de JASPAR au Japon. Parmi les standards, l'ISO/SAE DIS 21434 autour de l'ingénierie de la cybersécurité et l'ISO/AWI 24089 spécifique au système de management de la mise à jour des logiciels, auront un effet structurant pour les constructeurs automobiles et leurs sous-traitants, qui les utiliseront comme guides d'implémentation pour la prise en compte de la cybersécurité sur tout le cycle de vie du véhicule.

La réglementation UNECE WP.29

L'UNECE WP.29[1] a approuvé en juin 2020 une nouvelle réglementation pour la cybersécurité dans le monde automobile. Sa publication est attendue en décembre 2020 pour une application en juillet 2022 pour tous les nouveaux véhicules en Europe.

La réglementation porte sur la cybersécurité à la fois des véhicules, des systèmes de production et des systèmes d'information connexes, dont ceux des fournisseurs et prestataires de services. Cette réglementation, issue du groupe de travail WP.29 de l'UNECE, la Commission Economique pour l'Europe des Nations Unies, sera applicable dans les 54 pays signataires de l'accord de l'UNECE de 1958, et notamment dans tous les pays de l'Union Européenne via le règlement européen GSR[2] (General Safety Regulation) édicté en 2019.

La réglementation s'appliquera aux véhicules des catégories L6 et L7 à quatre roues ainsi qu'aux catégories M des véhicules conçus pour le transport de passagers, N des véhicules à moteur prévus pour le transport de marchandises, et enfin de catégorie O concernant les remorques et semi-remorques, à partir du moment où ils contiennent au moins une unité de commande électronique embarquée (ECU). Les non-conformités des véhicules pourront avoir comme effet un refus de délivrance de certificat par type de véhicule (à partir du 6 juillet 2022), voire une interdiction d'immatriculation des véhicules à partir du 7 juillet 2024. Il est à noter que contrairement à une directive, la réglementation européenne sera appliquée dans tous les pays signataires telle quelle, sans transposition dans le droit national. Cependant, chaque pays aura sa propre autorité de contrôle.

Ce que contient la réglementation UNECE WP.29

Les deux principaux axes de la réglementation portent sur le Cyber Security Management System (CSMS) et la certification du type de véhicule, ainsi que le Software Update Management System (SUMS). A cela s'ajoute l'implémentation de mesures techniques recommandées par le Règlement GSR du 27 novembre 2019, pour assurer la sécurité des

informations et des systèmes à bord des véhicules contre une utilisation non-autorisée.

Cyber Security Management System

La réglementation stipule en effet que les constructeurs doivent mettre en place un Système de Management de la Cybersécurité (CSMS) couvrant le cycle de vie du véhicule et le cycle de production industrielle. Les constructeurs devront ensuite faire homologuer chaque type de véhicule et prouver à l'organisme certificateur qu'ils ont pris en compte la cybersécurité dès les spécifications, dans l'implémentation puis les tests, la production, les opérations, la maintenance jusqu'à la mise au rebut du véhicule.

Le système de management de la cybersécurité doit inclure des processus pour :
- Gérer la cybersécurité au niveau organisationnel et technique
- Identifier les risques pour les types de véhicules
- Evaluer, classer et traiter les risques identifiés
- Vérifier que les risques identifiés sont gérés de manière appropriée
- Tester la cybersécurité d'un type de véhicule
- Surveiller, détecter et répondre aux cyber-attaques, menaces et vulnérabilités
- Evaluer l'efficacité des mesures mises en œuvre

Le CSMS doit être audité et homologué, pour chaque type de véhicule développé par un constructeur automobile, par les autorités compétentes du pays pour assurer leur mise en œuvre de façon effective.

Software Update Management System

La réglementation impose également l'implémentation d'un Système de Management des Mises à jour des Softwares (SUMS) présents dans le véhicule, les mises à jour pouvant être réalisées à distance : Over-The Air (OTA).

Le Système de Management des Mises à jour des Softwares présents dans le véhicule assure la mise en place de processus permettant de :

- Identifier les composants logiciels et matériels
- Vérifier la compatibilité d'une version logicielle avec un système/véhicule cible
- Evaluer l'impact sur la sûreté des occupants d'une mise à jour logicielle
- Assurer l'intégrité et l'authenticité des mises à jour
- Assurer la possibilité de revenir à une version antérieure si une mise à jour ne s'est pas faite correctement.

Des mesures techniques relevant du GSR

Au delà de la mise en place des systèmes de management, des mesures techniques doivent aussi être implémentées pour assurer la sécurité de l'information et des systèmes à bord des véhicules contre une utilisation non-autorisée.

Le règlement européen GSR stipule notamment que « *La connectivité et l'automatisation des véhicules augmentent la possibilité d'accès non autorisé à distance aux données embarquées et la modification illégale de logiciels réalisée sans fil.* » et préconise donc une application des normes internationales de cybersécurité.

Le GSR donne aussi une liste de prescriptions devant être prises en compte dans le périmètre à sécuriser, notamment les systèmes à bord des véhicules.

Modalité de mise en conformité et homologation

La mise en conformité porte à la fois sur le CSMS et sur les véhicules. Les exigences de sécurité seront déportées par les constructeurs sur l'ensemble des sous-traitants (Tier 1 et Tier 2).

Certification de CSMS

La certification est délivrée par une autorité d'approbation chargée d'évaluer la conformité à la réglementation, du CSMS implémenté par le constructeur. Cette certification est valable 3 ans (renouvelée sur 3 ans en fonction des résultats de l'évaluation tri-annuelle).

Demande d'homologation d'un type de véhicule

L'homologation d'un type de véhicule passe par les étapes suivantes :
- Documentation fournie par le constructeur à l'autorité d'approbation : caractéristiques du véhicule, résultats des analyses des risques, identification des éléments critiques du véhicule et de son environnement, dispositifs de sécurité en place pour mitiger les risques, résultats des tests, éléments de sécurisation de la supply chain, numéro du certificat de conformité pour le CSMS, vérification de ces éléments par l'autorité d'approbation,
- Tests du véhicule par l'autorité d'approbation,
- Contrôle sur site possible par l'autorité d'approbation.

Relation avec les autres standards de cybersécurité

La réglementation UNECE WP.29 préconise l'application des autres réglementations et standards dès leur entrée en vigueur. Parmi les autres standards applicables, on peut citer lSO/SAE 21434 (publication début 2021) and ISO/AWI 24089 (publication mars 2022) et la série ISO 27K qui permet ensuite de couvrir complètement les exigences de la règlementation en intégrant les processus relevant de la partie IT Backend ainsi que les Plans de Continuité et de Reprise d'Activités.

Au-delà de la réglementation, la transformation à venir et la sécurité dans les véhicules

La réglementation UNECE et les standards de sécurité applicables aux véhicules et aux systèmes d'information et de production contribuent au développement des bonnes pratiques de sécurité chez les constructeurs et l'ensemble des acteurs de la chaine de valeur. Cet élan engendrera l'émergence de nouveaux services tels que des SOC spécialisés pour les véhicules. Il permettra aussi une généralisation et une systématisation des tests d'intrusion sur les voitures et les systèmes de l'écosystème.
Parallèlement, la protection des données collectées par les véhicules, et échangées avec des tiers pour la maintenance du véhicule et la création de nouveaux services, deviennent un enjeu stratégique business qui conduit d'ores et déjà les constructeurs automobiles, à imaginer de nouvelles

architectures internes aux véhicules et les infrastructures externes associées. La convergence IT /OT est en marche !

IT /OT est en marche !

Parution le 15 janvier 2021

[1] UNECE WP.29 https://www.unece.org/trans/main/welcwp29.html
[2] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R2144&from=CS

Directive NIS : les bons vœux de l'ANSSI

ELISE BRUILLON
Directeur, Responsable des offres « Conformité » et « Prévenir »
FORMIND

En date du 28 octobre 2020, l'ANSSI publiait sur son site une actualité dénommée « Révision de la directive NIS[1] : une opportunité pour renforcer le niveau de cybersécurité au sein de l'UE » ; cette information relayée par les médias sociaux a paradoxalement suscité très peu de commentaires.
Pourtant, le sujet touche la majorité des secteurs d'activité de notre économie et nombres d'acteurs sont en cours de constitution des dossiers d'homologation de leurs systèmes d'information essentiels (SIE) auprès de l'agence.

Dans cette actualité, l'ANSSI appelait de ses vœux à une harmonisation sur la plaque européenne des pratiques relatives à la gouvernance des risques numériques et à une coopération transfrontalière plus développée; elle mettait également en avant la nécessité de placer comme axe d'étude les attaques par rebond sur les chaines de valeur des Opérateurs de Services Essentiels (OSE) notamment en conseillant de maitriser l'ensemble des interventions directes et/ou indirectes des tiers (fournisseurs, partenaires etc…) sur les SIE.

Simple positionnement de notre agence française ou *Gentle reminder* à l'adresse de l'ENISA, cette actualité nous semble intéressante sur trois axes dans le secteur de la cyber conformité.

La Directive NIS détermine un objectif commun de sécurité

L'Union européenne a pris le parti de protéger son marché économique via le renforcement des capacités en cybersécurité des Etats et d'acteurs spécifiques comme les entreprises ou organismes publics identifiés dans des secteurs clés. Ces secteurs clés sont qualifiés de « services essentiels » au fonctionnement de l'économie et de la société. Ces acteurs sont généralement tributaires d'un ou plusieurs systèmes d'information dits *essentiels (SIE)*. L'objectif est donc de pouvoir gérer les interfaces et dépendances à ces SIE lorsque ce produit un évènement de sécurité.

Pour ce faire, la Directive NIS pose le cadre de coopération entre états membres notamment par le renforcement de leurs capacités en matière de cybersécurité ; la désignation d'autorités nationales compétentes en matière de cybersécurité et de centres de réponse aux incidents de sécurité ; l'instauration de règles communes avec notamment la notification des incidents, le partage des informations techniques sur les risques et les vulnérabilités.

Sur ce troisième volet relatif aux règles communes, l'ANSSI se réjouissait de ces compléments nécessaires à notre règlementation nationale relative aux activités d'importance vitale ; la Directive NIS confortait les orientations stratégiques de l'ANSSI dans son positionnement d'autorité nationale compétente en la matière et adoubait les CSIRT comme un maillon essentiel de la chaine de protection. Elle fixait dans le marbre les objectifs de sécurité pour converger vers une protection commune sans frontières.

Pour rappel, cette remontée d'information des incidents nationaux pour un partage européen via les agences de sécurité concernées, reprenait l'orientation prise dans le secteur des communications électroniques avec la notification des incidents de sécurité[2] et la consolidation de ce reporting au niveau de l'ENISA.

L'ANSSI améliore sa connaissance de notre écosystème cyber en consolidant sur l'ensemble des secteurs d'activités économiques un

ensemble informationnel de premier choix pour anticiper, prévenir et se protéger des attaques.

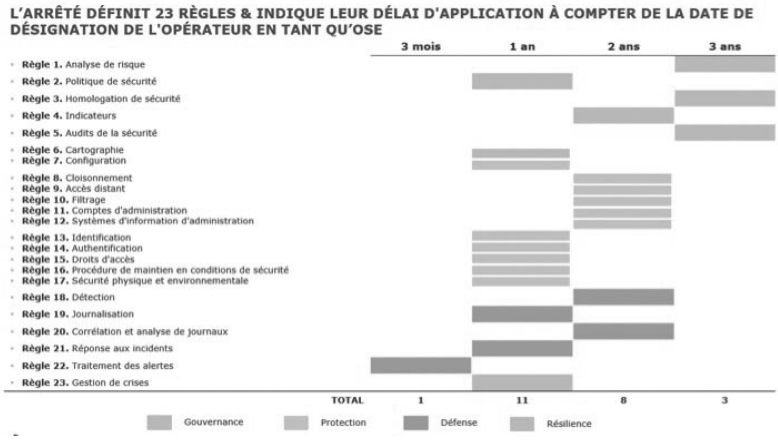
Par conséquent, la Directive NIS permettait de cadrer une priorité transverse européenne telle que mettre sous contrôle les attaques sur les services essentiels d'une nation et faire en sorte que cet objectif puisse être décliné chez tous nos partenaires européens en fixant des moyens et des ressources.

L'ANSSI a personnalisé la transposition de la Directive NIS en rendant incontournable l'analyse de risques

Pour pouvoir être appliquée dans une législation nationale, une directive doit d'être transposée en droit national via un véhicule législatif. La transposition laisse la possibilité pour chaque État de personnaliser la vision de l'objectif de sécurité et des moyens pour y parvenir. Chaque État est souverain dans la manière de transposer législativement la Directive pourvu que se retrouvent les grands axes fournis par le texte européen.

Ainsi la Directive NIS[3] a été transposée en droit français sous l'étroit contrôle de l'ANSSI ; le décret d'application de la loi de transposition au Journal Officiel, a été publié le 25 mai 2018 et identifiait les principaux secteurs concernés tels que représentés ci-dessous :

Au sein de ces secteurs d'activité, l'ANSSI a désigné 122 OSE, cette liste classifiée reprend *stricto sensu* les consignes de la Directive. Les OSE doivent mettre en œuvre 23 mesures techniques et organisationnelles pour gérer les risques menaçant la sécurité des réseaux et des systèmes d'information. Ces 23 mesures font partie de l'arrêté du 14 septembre 2018 qui illustre l'interprétation par l'ANSSI de la Directive NIS.



En France, la Directive NIS est transposée de manière règlementaire en 23 règles, 4 thématiques et une logique de boucle d'amélioration continue. L'acte fondateur de la mise en conformité des OSE commence par la réalisation d'une analyse de risques qui est une pièce incontournable du dossier d'homologation.

Dans la communauté cybersécurité, il est entendu que l'étude, la qualification du risque, et son affinage est un travail de séquencement avec encore beaucoup (trop ?) de subjectivisme et d'empirisme.

En effet, la profondeur d'une analyse de risques dépend du profil de son rédacteur fonctionnel versus technique, de ses expériences, de sa connaissance de véritables incidents de sécurité. Ce pourquoi il est nécessaire de limiter cette part de subjectivisme en adoptant une démarche commune d'analyse généralement définie par une autorité régalienne. Ainsi, la méthodologie d'analyse de risques consacrée en France en 2021 est Ebios RM. L'ANSSI a dépoussiéré la méthodologie EBIOS 2010 pour permettre de disposer d'un outil plus adapté à la menace actuelle.
La Directive NIS n'avait pas vocation à cadrer les analyses de risques, ce n'est pas la vocation d'un instrument législatif qui poursuit des objectifs plus stratégiques : maitriser les services essentiels d'une nation.

Dès lors, si nous nous plaçons sur un terrain de jeu européen, l'absence d'une méthodologie commune à l'ensemble des États de l'Union ne permet pas de disposer d'une vision comparable des risques pesant sur les services essentiels.

Ces derniers sont issus de différentes méthodologies nationales et ce mal nécessaire (subjectivisme + empirisme dans la réalisation des analyses de risque) rend la vision plus trouble du risque pesant sur les SIE et sans garantie de fiabilité alors que la chaîne de valeur à protéger reste la même. Comparer les risques consolidés au niveau européen pour en tirer des orientations stratégiques de protection et de défense nécessite donc d'harmoniser nos manières de réaliser nos analyses de risques. Et ce point particulier n'a pas échappé aux fourches caudines de l'ANSSI.

Une méthodologie à imposer pour harmoniser les pratiques ?

Si tous nous partageons cette vision d'un risque affranchi des frontières matérielles ayant des effets sur des secteurs similaires ou semblables ; au sein de l'Union européenne notre démarche d'analyse n'est pas forcément la plus harmonieuse. Si la norme ISO 27005, nous fournit des lignes directrices pour réaliser une telle étude, chaque agence nationale a décliné sa propre méthodologie pour identifier des objectifs de sécurité conformes à ses lignes directrices de défense et de résilience.

Or pour se protéger de manière commune, il convient de s'entendre et de partager sur comment nous allons qualifier ces fameux risques sur les services essentiels et quel est le séquencement logique le plus efficace pour que l'étude puisse aboutir à un résultat probant et comparable entre états. Par conséquent, l'harmonisation des pratiques pour dérouler l'étude de risques nous semble légitime et pertinente. La question provocante est que nous apporte EBIOS RM dans ce contexte si particulier de la conformité NIS ?

Tous nous avons salué le formidable dépoussiérage de la méthodologie et la réalisation d'atelier collaboratif et itératif permettant d'embarquer les métiers rétifs à l'exercice. Et pourtant, nous avons hurlé à la mort sur le

fait que les sources de menaces non intentionnelles n'étaient pas prises en compte dans un tel exercice. Nous nous sommes cassés les dents sur le détourage des parties prenantes et des chemins d'attaques en nous référant frénétiquement à la base de connaissances.

Néanmoins, dans le cadre particulier de la mise en conformité aux 23 règles d'un OSE, ce déroulement de l'analyse nous permet de changer le prisme de notre vision du risque. Le métier parle, s'approprie les concepts et nous oblige à challenger nos connaissances et notre vision « prêt à l'emploi » d'une attaque. De notre opinion, EBIOS RM nous permet de nous placer dans le dispositif d'une attaque probablement réelle et de disposer d'un outil de synthèse pour communiquer auprès des instances managériales d'un OSE.

Et c'est bien le sens de ces 23 règles, connais ton écosystème et tes vulnérabilités, corrige-les autant faire se peut et sache informer au bon moment tes autorités comme le ferait tout agent d'un maillage plus vaste que son propre écosystème.

Dès lors, la suggestion de l'ANSSI d'harmoniser les pratiques de gouvernance des risques numériques semble étroitement liée à l'harmonisation de la méthodologie d'analyse de risques qui reste le premier maillon d'une saine gouvernance des risques.

Pour conclure, il nous semble que ce qui ferait la force d'une harmonisation dans le cadre de la directive NIS serait la vision commune de l'appréhension du risque, de sa qualification à son nécessaire arbitrage. Si la multiplication des attaques par rebond doit être pris en compte de manière plus prégnante selon l'Agence, cette menace n'est pas nouvelle et certaines autorités administratives indépendantes (ACPR, CNIL…) avaient déjà pris le parti de consolider les exigences de sécurité sur la maîtrise des tiers dont les actions portaient incidence sur la sécurité du SI. Le Règlement Général relatif à la Protection des Données impose la maîtrise des sous-traitants en systématisant cette approche par les risques. Nul besoin de vanter les mérites du dispositif qui a défrayé la chronique ces dernières années. Sa force de frappe est d'autant décuplée qu'il s'applique de plein droit sans effet d'interprétation dans les législations

nationales à la différence de la Directive NIS qui nécessite un travail de transposition administrative.

A l'instar de l'ANSSI, nous présentons également nos meilleurs vœux pour aboutir à une démarche d'étude des risques visant à mettre sous contrôle les tiers intervenant sur la chaine de valeurs des OSE.
Nous pressentons qu'il s'agira de la thématique phare de l'année 2021.

Parution le 22 janvier 2021

[1] Pour (Network and Information System Security)
[2] Code des Postes et Communications électroniques
[3] DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne.

La cybersécurité des systèmes industriels, enjeu critique pour l'adoption du modèle « Industrie du Futur - Industrie 4.0 »

PHILIPPE GENOUX
Délégué Général
EXERA

La prise de conscience du monde industriel sur la réalité de la cybermenace remonte à 2010 et a été brutale avec la révélation de l'attaque informatique Stuxnet sur le site d'enrichissement d'uranium iranien, les industriels ayant longtemps cru être à l'abri de ce risque en raison du réputé cloisonnement des réseaux informatiques industriels.

Depuis, on apprend régulièrement que de nouvelles attaques cyber ont affecté les systèmes industriels les plus divers. À titre d'exemples marquants…
- Attaque Sandworm sur le réseau de distribution d'électricité en Ukraine pendant l'hiver 2015-2016,
- Attaque Wannacry, virus de type ransomware (cryptage des données, en mai 2017, première opération d'envergure mondiale puisque près de 150 pays ont été touchés),
- Attaque Notpetya, virus de type wiper (destruction de données), démarrée en juin 2017, deuxième opération d'envergure mondiale tout juste un mois après Wannacry.

Les impacts financiers des cyberattaques ont fortement augmenté avec le temps, et sont devenus un véritable sujet d'inquiétude pour les acteurs de la vie économique et pour les États. Ainsi, pour la seule cyberattaque Notpetya, première attaque bien documentée, les montants communiqués par les entreprises victimes de cette attaque sont éloquents :
- Pertes estimées à 300 millions de dollars par Maersk, groupe danois de transport et de logistique, et fermeture temporaire de plusieurs sites ;
- Pertes estimées à 870 millions de dollars par Merck, laboratoire

pharmaceutique américain ;
- Pertes estimées à 188 millions de dollars par Mondelēz International, groupe agro-alimentaire américain, propriétaire de la marque française « Biscuits LU » ;
- Pertes estimées à 400 millions de dollars par TNT Express, filiale européenne de FedEx groupe américain de transport international de fret ;
- Pertes estimées à 384 millions de dollars par Saint-Gobain, groupe français de production de matériaux.

Par ailleurs, les nouveaux concepts « Usine du Futur » ou « Industrie 4.0 » ont fait leur apparition, et progressent à grands pas avec des sites-pilotes qui constituent des démonstrateurs de faisabilité. Derrière ces concepts, la digitalisation de l'entreprise, le décloisonnement des services centraux et des sites de production -voire de partenaires externes - que facilite l'intégration toujours plus poussée de l'ensemble des fonctions de l'entreprise dans des systèmes d'information de type ERP/PGI puissants, l'émergence de technologies prometteuses telles que le big data et le recours à l'intelligence artificielle ouvrent de nouvelles opportunités. Les enjeux économiques liés à l'adoption de ces concepts sont considérables, puisque les retombées attendues de la numérisation de l'industrie sont estimées à 6% du chiffre d'affaires résultant des gains globaux de productivité. Parmi les facteurs contribuant à ces gains, on mentionnera notamment la réduction des coûts de maintenance de 12% liée au passage à la maintenance prédictive, la réduction du poste « *Energie* » liée à l'optimisation de la production, ces ratios étant observés dans les retours d'expérience issus des sites pilotes. En contrepoint, les investissements anticipés en lien avec la digitalisation des entreprises industrielles sont massifs, les estimations (avant Covid…) étant de 400 milliards de USD sur la période [2020-2024], dont 140 milliards de USD pour les pays de l'Union européenne.

Conséquences de ces évolutions, se généralisent les passerelles entre réseaux IT et réseaux OT et l'adoption de standards communs pour les réseaux d'information générale (IT) et pour les réseaux d'information technique (OT), qui constituent autant de vulnérabilités potentielles aux cyberattaques. Ainsi, la conjonction des premières cyberattaques ciblant les systèmes d'information industriels d'une part et d'autre part l'adoption croissante des concepts « Usine du Futur » ou « Industrie 4.0 » rendent encore plus critique

le déploiement de solutions de cybersécurité des systèmes industriels indispensables à, sinon garantir, assurer la sécurité des réseaux vis-à-vis des cyber agressions, tout en maintenant des flux d'échanges de données tant entre entités internes qu'avec des partenaires externes.

C'est dans ce contexte que les États ont pris conscience de la cybermenace sur les acteurs du secteur industriel, et qu'ils ont graduellement mis en place des dispositifs législatifs et réglementaires depuis le début des années 2010. C'est ainsi qu'en France, la Loi de programmation militaire du 18 décembre 2013 a élargi et renforcé le périmètre des attributions de l'ANSSI, agence dépendant du premier ministre, de manière à sensibiliser plus fortement les acteurs économiques à la cybermenace et à réduire leur niveau de vulnérabilité aux cybermenaces. Ont ainsi été recensés les systèmes d'information d'importance vitale (SIIV) déployés par les opérateurs d'importance vitale (OIV), SSIV desquels des discontinuités de service résultant de cyberattaques seraient particulièrement préjudiciables pour la vie économique et sociale du pays et de ses habitants. Ont également été définies des obligations à respecter par les OIV, destinées à prévenir les attaques et leur propagation, comme par exemple les déclarations d'incidents. L'ensemble de ces dispositions a été largement repris par le parlement européen pour l'établissement de la directive européenne « Network and Information System Security » (NIS) adoptée le 19 juillet 2016, transposée en droit national le 27 février 2018.

Répondant à la demande des entreprises, les acteurs du marché de la sécurité informatique se sont mobilisés pour proposer des solutions dans le domaine de la cybersécurité des systèmes industriels. Qu'il s'agisse d'entreprises établies ou de start-ups, les initiatives d'éditeurs de logiciels, de fabricants de matériels ou de sociétés de services informatiques sont nombreuses. Parmi les solutions émergentes, on retiendra les sondes informatiques destinées à surveiller les réseaux d'information industriels (OT), les anti-virus, les pares-feux logiciels ou physiques (diodes), mais également les durcissements des plateformes, logiciels, OS et firmwares (stations SCADA, automates, capteurs de mesure, actionneurs intelligents, etc.), ou encore les solutions d'architectures de réseaux offrant une meilleure résilience. À côté de ces solutions d'ordre technique, apparaissent également les solutions d'ordre organisationnel et procédural (définition et déploiement de plans de réponse à cyberattaque) destinées à répondre aux obligations règlementaires ou aux recommandations

émanant des agences gouvernementales en charge de la sécurité des systèmes d'information.

À la demande de ses adhérents, l'Exera a mis en place fin 2013 la commission technique « Cybersécurité des systèmes industriels ». Elle permet à ses membres de connaître l'offre du marché au travers de rencontres avec les industriels et start-ups porteurs de solutions en cybersécurité, au cours desquelles ceux-ci exposent le contenu technique de leurs produits et services. C'est ainsi que, de 2014 à 2019, ce sont quarante-trois acteurs qui ont été invités, et de nombreux autres acteurs restent à rencontrer, signe de la vitalité du secteur de la cybersécurité des systèmes industriels. La commission s'est aussi fixée pour objectif de mettre à la disposition de ses adhérents des guides à la rédaction de clauses des volets « cybersécurité » à inclure dans leurs dossiers de consultation couvrant les opérations externalisées en lien avec leurs activités (conception d'installations nouvelles, déploiement/mise en service, maintenance, exploitation externalisée, audits d'état des lieux initiaux, audit de réception, formation…). Ce travail est mené parallèlement au suivi des volets législatifs et règlementaires applicables à la cybersécurité des systèmes industriels, facilité par la présence d'un représentant de l'ANSSI au sein de la commission, et celui du volet de normalisation réalisé en liaison avec ISA - France.

Enfin, l'Exera organise depuis 2015 une fois par an une journée technique « Cybersécurité des systèmes industriels » ouverte aussi bien à ses adhérents qu'aux non-adhérents. Ces journées sont destinées à permettre de faire un point d'étape annuel sur les évolutions du marché de l'offre et à faciliter les échanges entre les participants et la dizaine d'exposants présents.

Pour plus d'informations, n'hésitez pas à vous rendre sur le site de l'association www.exera.com.

Parution le 22 janvier 2021

Modération des contenus : qui fait la loi ?

JEAN-MICHEL MIS
Député de la Loire, membre de la commission des lois,
membre du Conseil national du numérique,
membre de la Commission supérieure du numérique et des postes

Alors que les réseaux sociaux sont entrés en guerre contre Donald Trump et que les grands hébergeurs de contenus comme Google et Apple ont censuré les plateformes d'extrême-droite, que disent ces mesures de modération des contenus politiques sur la transformation des règles du jeu démocratique ? Alors que l'état du droit est traditionnellement fixé par le gouvernement du peuple, par le peuple et pour le peuple, des acteurs privés s'arrogent aujourd'hui le droit de faire la loi en son nom.

Cette situation de fait ne peut plus perdurer. Aux régulateurs de reprendre la main pour mettre un terme à l'érosion des libertés publiques tout en préservant la qualité du débat démocratique et ainsi freiner la radicalisation croissante d'une partie de nos populations et la montée des théories complotistes.

La politique de modération à géométrie variable des GAFAM

Les grandes plateformes numériques ont pris une série de mesures relatives aux comptes et à la communication du président américain Donald Trump. Parmi les plus flagrantes, celle de Twitter qui après avoir retiré deux publications du président américain a suspendu le compte @realDonalTrump conformément à sa politique de modération[1]. Facebook et Instagram, les deux réseaux sociaux qui appartiennent au groupe Facebook, ont également suspendu les comptes de Trump pour une durée indéterminée. Plusieurs autres plateformes leur ont emboité le pas, dont la liste est consultable sur le site Axios :
https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html

Sont aussi rendues publiques les décisions des hébergeurs, comme Apple ou Amazon, qui ont fait le choix de retirer les plateformes d'extrême droite de leurs contenus. Par exemple Apple a décidé de retirer Parler de son AppStore. Amazon We Service a décidé de ne plus héberger le service sur sa plateforme, à la suite d'une pétition interne.

Nous devons admettre que ces mesures sont dangereuses d'un point de vue démocratique, quel que soit notre degré d'animosité envers la politique menée ces quatre dernières années par l'administration Trump. Tout d'abord, parce que les justifications données par les plateformes peinent à convaincre. Les facteurs identifiés par Twitter pour attester d'un risque d'incitation à la violence étaient tout aussi valables ces quatre dernières années qu'après les incidents survenus au Capitole. Ensuite, parce que ces mesures de modération arrivent trop tard et s'appliquent de manière aléatoire. Sans contrôle démocratique et sans contre-pouvoir, les plateformes ne disposent pas d'une légitimité suffisante pour modérer le débat public.

Cela s'explique par la nature politique de leurs mesures, prises alors que l'élection de Biden était acquise et de nature à donner des gages aux démocrates qui souhaitent les réguler davantage.

Impossible dans ces conditions de laisser les plateformes faire de l'autorégulation, d'autant que l'exercice présente de sérieuses limites. D'une part leur politique de modération n'est pas efficace, et d'autre part elle est pratiquée dans l'opacité la plus complète. Ainsi Tariq Krim reprenait récemment sur Twitter l'expression de « *black box regulation* », utilisé par Frank Pasquale[2]. On ne cesse de dénoncer le « *deux poids deux mesures* » qui prévaut sur Twitter qui n'a jamais censuré les tweets du président américain incitant à la violence au cours de son mandat, lorsqu'il désignait à la vindicte populaire les noms des journalistes qui critiquaient son action ou quand il suggérait de tirer sur les manifestants du mouvement *Black Lives Matter*.

Jamais des conditions générales d'utilisation ne doivent prévaloir sur les règles de l'état de droit, notamment lorsqu'elles sont de valeur constitutionnelle comme la dignité humaine mais aussi la liberté d'expression.

Cette politique de modération tranche avec la conception américaine traditionnelle de la liberté d'expression

Dans ce débat sur la conciliation des droits et libertés, c'est l'Europe qui appelle désormais à protéger la liberté d'expression. Les mesures prises par les plateformes sur la communication du président américain sont très critiquées par les dirigeants européens. La chancelière allemande Angela Merkel a ainsi jugé « *problématique* » l'éviction du président Trump de Twitter, lorsque le commissaire au marché intérieur Thierry Breton faisait part de sa perplexité face à une décision non-démocratique qui censure le président des États-Unis[3].

La position européenne est d'autant plus intéressante quand on sait qu'historiquement, ce sont les États-Unis qui toujours ont défendu le plus vigoureusement la liberté d'expression. En témoigne la rédaction du premier amendement de la constitution américaine, dont la rédaction, pourtant contemporaine de celle de la DDHC, est nettement plus radicale :
« *Le Congrès n'adoptera aucune loi relative à l'établissement d'une religion ou pour limiter la liberté d'expression, de la presse ou le droit des citoyens de se réunir pacifiquement.* »

Il existe ainsi différentes conceptions de la liberté d'expression et celles-ci évoluent fortement dans le temps. Seul le peuple souverain et ses représentants sont légitimes pour en modifier les fondements, et ainsi adapter nos droits et libertés aux nouveaux enjeux posés par la publication de contenus sur les réseaux sociaux.

Une meilleure modération passe par des règles qui doivent être fixées par les États

Les Etats sont les entités les plus légitimes dans le traitement des enjeux soulevés par la modération des contenus en ligne. D'abord, parce que des défaillances existent aujourd'hui dans la politique de modération des plateformes. Ensuite, parce que les plateformes ont une part de responsabilité dans la diffusion des contenus illégaux et illicites mais aussi des *fake news* et des théories complotistes qui gangrènent depuis plusieurs années le débat

démocratique. Comme le rappelait récemment l'article de Damien Leloup[4], l'invasion du Capitole n'est que le point culminant d'un long processus de radicalisation d'une partie de la population. Facebook a par exemple pendant longtemps laissé prospérer des groupuscules insurrectionnels sur sa plateforme qui en ont profité pour s'organiser et recruter de nouveaux membres.

Afin de mettre un terme à cette dynamique qui est dangereuse pour le débat démocratique et l'avenir de nos institutions, il est plus que jamais nécessaire de légiférer sur les services numériques. C'est tout l'objet des deux textes qui sont portés par la commission européenne. Parmi eux le Digital Services Act a pour objectif de renforcer la responsabilité des plateformes pour améliorer la confiance et la transparence du marché numérique en mettant à leur charge de nouvelles obligations en matière de lutte contre les contenus illégaux et illicites. Pour garantir un environnement en ligne sûr et responsable, et ainsi renforcer la confiance de nos concitoyens dans des institutions démocratiques.

De l'autre côté de l'Atlantique, les Américains préparent une enquête sur le rôle des réseaux sociaux dans la désinformation, et leur rôle dans l'attaque du Capitole le 6 janvier dernier.

Ensemble, nous parviendrons à démontrer que les États n'ont pas encore dit leur dernier mot face aux GAFAM. Ils sont les seuls gardiens des règles du jeu démocratique.

Parution le 5 février 2021

[1] https://blog.twitter.com/en_us/topics/company/2020/suspension.html - Permanent suspension of @realDonaldTrump by Twitter Friday, 8 January 2021
[2] Frank Pasquale, Black Box Society, Harvard University Press (2015)
[3] Le Commissaire européen au marché intérieur Thierry Breton, dans Politico (2021)
[4] Le Monde, en date du 9 janvier 2021, « Suspension des comptes de Donald Trump : les plates-formes numériques entre opportunisme et aveu d'échec »

« Cyberfeux » sur les collectivités territoriales, une nouvelle menace ?

STÉPHANE MEYNET
Président-fondateur
CERTitude Numérique

Le nombre de collectivités territoriales victimes d'actes de cybercriminalité ne cesse de croître, comme le montre l'actualité depuis plusieurs mois, à tel point que les recenser précisément devient complexe.

Est-ce un phénomène nouveau, un phénomène existant mais renforcé par le développement forcé du télétravail dans le cadre de la crise sanitaire actuelle ou un « simple » effet des médias relayant d'avantage le phénomène aujourd'hui ?

Un postulat : les collectivités territoriales, quelle que soit leur taille, constituent en France des cibles potentielles au même titre que les grands groupes, PME/PMI, TPE, etc. Plus d'un millier de collectivités françaises étaient déjà ciblées en 2019 par des cyberattaques, avec des impacts plus en moins étendus sur leur fonctionnement. Un rappel : parmi les menaces dont sont victimes les collectivités figurent en tête aujourd'hui les rançongiciels et les fuites de données, les deux pouvant d'ailleurs être combinés.

Le phénomène des rançongiciels, s'il constitue aujourd'hui probablement la première menace à traiter face à l'explosion de ce type de cyberattaques, n'est pour autant pas un phénomène nouveau. Il sévit depuis 2015 dans tous les secteurs, touchant institutions publiques, entreprises privées de toutes tailles, ainsi que les citoyens. Le secteur de la santé a ainsi été particulièrement touché dans certains pays lors des vagues Wannacry et NotPetya de 2017.

Les collectivités constituent depuis longtemps une cible pour les cybercriminels. Rappelons qu'elles sont ainsi par exemple, depuis des années, victimes de défiguration de sites web. La liste s'allonge chaque semaine. Souvent trivial, ce type d'attaque vise à déstabiliser les élus locaux ou, comme cela fut le cas en 2015, à la suite des attentats Charlie Hebdo, à déstabiliser la France.

Les conséquences de tous ces « simples » actes de cybercriminalité, au-delà des coûts financiers importants pour la remise en service des systèmes numériques et la récupération des données (avec éventuellement le paiement de la rançon), impactent non seulement les citoyens qui se trouvent brusquement privés de certains services, mais également la sérénité et la démocratie locales. Imaginez une commune dont l'état civil est paralysé car toutes les données sont « prises en otage » par un rançongiciel. Imaginez une collectivité qui n'est plus en mesure de gérer les payes de son personnel, les cantines scolaires, certaines de ses missions sociales car les outils numériques sont indisponibles. Que dire de ces mêmes phénomènes en pleine période électorale et de l'impact sur le fonctionnement serein de la démocratie ?

L'objectif n'est, ni de pointer du doigt les collectivités victimes et leurs élus, ni de noircir le paysage de nos territoires mais nous devons comprendre et accepter que la cybercriminalité est désormais une réalité quotidienne. Nous devons la traiter, la gestion de ce risque s'ajoutant à la longue liste de ceux que doivent déjà traiter les élus et agents territoriaux.

Quelles actions à mener ?
La sécurité numérique est avant tout « l'école de l'humilité ». Même les plus grandes entreprises françaises spécialisées en cybersécurité ont été victimes de cyberattaques à des degrés de sévérité différents. Thales, Sopra-Steria et récemment Stormshield en sont des exemples.
Ne pas négliger la menace en pensant que cela n'arrive qu'aux autres, mieux la connaître pour appliquer les bons gestes barrières comme nous le faisons dans la lutte contre la COVID puis engager une approche pragmatique, portée par les élus, s'inscrivant dans un plan stratégique en soutien au développement du numérique et de la sécurité globale des territoires, tels sont les premiers conseils que nous pouvons proposer aux élus et directions des collectivités.

Force est de constater que le degré de maturité est très hétérogène sur l'ensemble du territoire national. Certaines collectivités, régions, départements, métropoles, communautés de communes, communautés d'agglomération se sont déjà emparés du sujet. D'autres ne l'ont toujours pas pris en compte. Et ce n'est pas là une question de dimension.

En complément d'une action durable portée par les collectivités elles-mêmes, l'État a bien évidement un rôle à jouer dans ce domaine.
Nous pouvons souligner l'action de la gendarmerie, de la police, des préfets et sous-préfets qui œuvrent sur le terrain pour sensibiliser les acteurs au risque cyber, expliquer les bonnes pratiques et apporter une aide aux victimes. Cette sensibilisation débute d'ailleurs dès le plus jeune âge par des actions menées par policiers et gendarmes auprès des élèves dans les écoles.

Soulignons également le groupement d'intérêt public (GIP) Cybermalveillance.gouv.fr, un dispositif directement issu de la Stratégie nationale de sécurité numérique présentée par le Premier ministre en 2015. Ce dispositif apporte à tous citoyens, pme-pmi, collectivités, associations une réponse concrète au travers de fiches conseil, de guides de sensibilisation et de parcours victimes. Cybermalveillance.gouv.fr qui vient de fêter ses trois ans est unanimement reconnu pour son travail, d'autant plus exceptionnel au regard de ses moyens.

Ne doutons pas de la volonté de l'État de renforcer les moyens de ce dispositif. Ses instances, déployées sur les territoires, pourraient certainement contribuer efficacement à développer la confiance et la sécurité numériques de nos collectivités. La Revue stratégique de cyberdéfense publiée en 2018 par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDNS) évoque d'ailleurs cette nécessité de mutualisation des ressources au niveau territorial. Cette revue soulignait également la nécessité de développer une offre des produits et de services adaptée aux collectivités. Le Label ExpertCyber initié par Cybermalveillance.gouv.fr à destination des prestataires de service de proximité s'inscrit pleinement dans cette logique. Dans le prolongement de cette action, et dans la continuité des produits qualifiés par l'ANSSI, le lancement dès 2021 d'un label pour les produits de sécurité adaptés aux besoins des collectivités serait pertinent.

Le Plan de relance engagé par le gouvernement est sans doute une opportunité à saisir pour agir en renforçant l'existant et en développant de nouvelles solutions pour les collectivités territoriales. Le directeur général de l'ANSSI a d'ailleurs évoqué cette possibilité pour développer l'action de Cybermalveillance.gouv.fr au profit des territoires lors d'une audition au Sénat en novembre dernier.
En amont de ces actions, l'État a depuis plus de 10 ans, élaboré une réglementation sur la sécurité numérique dont une partie concerne les collectivités.

L'ANSSI a publié à cet effet un guide utile sur l'essentiel de la réglementation pour les collectivités territoriales. Le lecteur pourra constater que la France et l'Europe ont bâti un corpus réglementaire important, pouvant d'ailleurs parfois être déstabilisant pour les collectivités de petites tailles disposant de peu de moyens. Parmi ces réglementations, le règlement européen pour la protection des données (RGPD) a souvent occupé le devant de la scène, focalisant les moyens et les énergies, en reléguant au second plan les autres problématiques de sécurité numérique comme les rançongiciels, qui représentent aujourd'hui une menace majeure.

Mais comme le soulignent des élus, fonctionnaires territoriaux et représentants de l'État sur les territoires, lors des étapes du Tour de France de la Cybersécurité (TDFCyber) depuis 2018, la réglementation pour être pleinement utile doit avant toute chose être connue et comprise par ceux qui doivent la mettre en œuvre. De plus, et c'est un point essentiel, la réglementation doit être accompagnée de politiques publiques efficaces et adaptées aux contraintes des territoires. Enfin, une évaluation des réglementations et politiques publiques est indispensable pour mesurer leur efficacité et s'assurer qu'elles s'inscrivent bien à une démarche d'amélioration continue et durable.

A titre d'exemple, la commande publique, dont une réforme a été mainte fois évoquée, une TVA réduite ou un dispositif d'accès au fonds de compensation de la TVA (FCTVA) pour les fournitures et prestations de sécurité numérique, pourraient constituer un formidable levier pour développer la confiance et la sécurité numériques des collectivités.
Sur ces sujets, l'État peut agir.

Enfin d'autres actions développées par des acteurs de confiance apportent aux collectivités des réponses parfois peu connues. Citons les travaux du Groupe La Poste, acteur historique et opérateur de service public, qui en plus des solutions et des services d'identité numérique propose des services pour aider les collectivités dans leur transformation numérique. Citons également la Banque des Territoires qui a publié un guide pratique pour une collectivité et un territoire numériques de confiance. Une initiative à saluer s'inscrivant dans cette logique constructive de soutien aux collectivités, plus que jamais nécessaire face au risque numérique.

En conclusion, la menace cyber touchant les collectivités territoriales n'est pas un phénomène nouveau mais les statistiques augmentent incontestablement. Nous devons apprendre à vivre avec cette nouvelle forme de menace. De la défiguration de sites web aux rançongiciels, en passant par les fuites de données, l'ensemble du panel des menaces cyber touche nos collectivités. Le sabotage d'infrastructures industrielles des collectivités (eau, énergie, traitement des déchets, transport), peu développé aujourd'hui en France, constitue un risque qu'il est indispensable de prendre en compte, à l'image de ce qui se passe dans d'autres pays, aux Etats-Unis et Israël par exemple.

Mais face à cette montée des menaces, retenons que des collectivités ont engagé une vraie démarche de sécurité numérique, ce qu'il faut saluer. Retenons aussi que l'État, au travers de plusieurs dispositifs, apporte son soutien à l'ensemble des acteurs.

De grands travaux restent toutefois à engager au niveau local et national. La perspective des prochaines élections sur les territoires et le plan de relance engagé par le gouvernement à la suite de la crise de la COVID19, constituent sans aucun doute des opportunités à saisir.

Parution le 12 février 2021

La Région Auvergne-Rhône-Alpes pleinement mobilisée pour le renforcement de la cybersécurité !

JULIETTE JARRY
Vice-présidente déléguée au Numérique
Région Auvergne-Rhône-Alpes

Les outils numériques ne cessent de se multiplier et de se diversifier, touchant de plus en plus de pans de nos vies, tant personnelles que professionnelles. Ordinateurs, téléphones portables et autres objets connectés sont progressivement devenus le prolongement voire l'auxiliaire de notre corps ou de notre mémoire. Précieux au quotidien sur de nombreux aspects, ils sont aussi une porte d'entrée sur nos données privées ou professionnelles, très convoitées par les pirates informatiques. Dans le monde des entreprises, les chiffres sont éloquents : 40% d'entre elles ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques alors que 17% seulement sont assurées contre ce risque, selon une enquête nationale de la CPME.

La cybersécurité est devenue d'autant plus cruciale que le contexte de crise sanitaire a obligé bon nombre d'entreprises à revoir leurs modalités de travail pour basculer dans des délais très courts vers une solution à distance. Le manque d'anticipation dans la mise en œuvre d'outils de sécurisation des flux de données mais aussi de sensibilisation et de formation des collaborateurs aux risques cyber ont fragilisé les entreprises face à ce nouveau contexte et à l'accroissement du niveau de menaces. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) estime ainsi que le nombre de cyberattaques a été multiplié par 4 en 2020 par rapport à l'année précédente. Il est, plus que jamais, temps de s'intéresser à la protection de ses données.

Ce manque de préparation et de capacité d'intervention s'explique en partie par les conditions pénuriques sur le marché de l'emploi et par les contraintes budgétaires qui en découlent. Du fait de sa rareté, l'expertise en sécurité

informatique, qu'elle soit en interne ou en externe, peut s'avérer relativement coûteuse. Après avoir interrogé plus de 3 000 responsables informatiques dans 12 pays dont la France, le cabinet Vanson Bourne[1] a constaté que 79% des responsables informatiques déclaraient qu'il était difficile de recruter des professionnels possédant les compétences en cybersécurité dont ils avaient besoin.

Consciente de cette problématique, la Région Auvergne-Rhône-Alpes a souhaité dès 2017 se mobiliser sur cette question en adoptant une Feuille de route stratégique en matière numérique qui intègre dans ses grands principes celui de la confiance numérique. Cette question touche à la fois le citoyen dans sa vie quotidienne, le salarié dans sa vie professionnelle, les entreprises dans leur activité économique et les collectivités locales.

La mise en œuvre de la stratégie régionale en matière de cybersécurité s'articule en lien avec le Campus Région du numérique qui a récemment ouvert ses portes à Charbonnières-les-Bains, à proximité de Lyon. Lieu-ressource et outil au service des transitions économiques, industrielles et environnementales, ce hub permet de traiter à 360° les enjeux du numérique dans ses 3 composantes : formation, transformation des organisations, innovation, particulièrement sur l'industrie du futur. C'est sous ces 3 angles que nous avons voulu aborder la question de la cybersécurité.

Le Campus propose une riche offre de formation avec les modules proposés par l'Esisar, les formations Simplon à l'Université Lyon II, le Mastère Spécialisé Data Scientist de Sigma Clermont, la IT Academy, ou encore la formation Data Analyst de la Wild Code School, qui sont destinées à des étudiants mais aussi à des professionnels qui souhaiteraient se perfectionner sur cette thématique. Sur sa plateforme web https://campusnumerique.auvergnerhonealpes.fr, le Campus propose également un MOOC de l'ANSSI intitulé « se former à la cybersécurité » ainsi qu'un dossier complet de sensibilisation des petites entreprises aux risques de la cybercriminalité.

Un programme « Caractériser la valeur de mon entreprise face aux cyber menaces » opéré par la CPME est également disponible sur le portail « Ambition Eco » de la Région. Il présente une offre d'accompagnement aux

entreprises pour la mise en place d'une culture et d'un savoir-faire lié à la cybersécurité.

Les partenaires de la Région tels que Minalogic, l'ENE, Digital League, le CyberCercle et la CCI de Savoie s'inscrivent dans une démarche de démocratisation des enjeux de la cybersécurité auprès de leurs réseaux en organisant régulièrement des ateliers, séminaires, formations en ligne et des événements autour de cette thématique. L'ENE, à travers son programme « Usine Numérique Régionale » permet aux entreprises d'auditer la sécurité de leurs systèmes informatiques et d'identifier ainsi les risques de cyber attaques et de proposer des mesures correctives. Le dispositif Atouts Numériques accompagne quant à lui les entreprises de moins de 50 salariés du territoire vers les usages du numérique dont la sécurité des infrastructures informatiques.

La composante innovation du Campus se matérialise quant à elle par un espace de près de 3 000 m2 nommée « l'Usine ». Elle porte les sujets de la transformation des modèles industriels vers la « Smart Factory ». L'Usine est composée de plateformes technologiques à échelle 1 qui permettent de découvrir, tester les technologies de l'industrie du futur et d'être accompagné dans son projet, quel que soit son niveau de maturité. Il est à noter que l'Usine sera équipée en 5G début mars 2021. Des expérimentations de 5G industrielle seront ainsi possibles. En ce sens, l'interopérabilité des systèmes industriels et leur cybersécurité seront au centre des activités des plateformes technologiques. Par sa vocation de travail en réseau, l'Usine s'appuie sur les forces d'Auvergne-Rhône-Alpes, région qui concentre 20% des effectifs nationaux de recherche et d'innovation en matière de cybersécurité avec des travaux de premier plan en matière de sécurité des objets connectés (dont industriels), de prévention et réaction aux cyberattaques, d'analyse de vulnérabilités logicielles et de sécurité des infrastructures critiques.

En complément, un démonstrateur des technologies du numérique récemment installé au Campus vient pousser les entreprises à se transformer et innover en se dotant de nouveaux outils numériques : il présente, de manière accessible à tous, les 4 technologies d'excellence de la région Auvergne-Rhône-Alpes, que sont l'intelligence artificielle, le calcul haute performance, les systèmes cyber-physiques et la cybersécurité. Cette dernière

technologie est présentée au travers d'exemples d'entreprises de notre région qui l'utilisent au quotidien : concrètement, leurs dirigeants expliquent en quoi la sécurisation des données et des process est fondamentale pour la bonne marche de leur entreprise, et leurs professionnels expliquent en quoi consiste leur métier de data scientist, ingénieur vision, responsable sécurité des réseaux…

A travers ces différents dispositifs, la Région Auvergne-Rhône-Alpes s'est dotée ces dernières années d'une vraie stratégie numérique de confiance que nous vous invitons à venir découvrir à Charbonnières-les-Bains selon nos 3 axes de sensibilisation : formation, transformation des entreprises et innovation.

Parution le 19 février 2021

[1] Etude réalisée en juin 2019 pour le compte de l'éditeur de logiciels de sécurité Sophos dans 12 pays : Etats-Unis, Grande-Bretagne, Allemagne, Inde, Canada, Brésil, Colombie, Mexique, Australie, Japon, Afrique du Sud.

Lutte contre la cyber contrefaçon : des propositions

MYRIAM QUEMENER
Magistrat
Docteur en droit

La contrefaçon est un fléau international qui prend la forme d'un marché illégal gigantesque qui n'a cessé de croître sous l'impulsion notamment du e-commerce et de la crise sanitaire liée à la Covid 19. La contrefaçon tous secteurs confondus coûte 8 milliards d'euros par an, auxquels s'ajoute le manque à gagner fiscal et social avec une perte pour les secteurs touchés comprise entre 7,5 milliards et 8 milliards d'euros par an[1].

En effet, les délinquants exploitent la pandémie de la Covid 19 qui frappe de nombreux pays pour écouler des gels contrefaits, des masques et autres produits soi-disant miracles pour traiter ce nouveau virus. Les produits pharmaceutiques de contrefaçon peuvent constituer une menace directe pour la santé et la vie. Leur entrée dans l'Union européenne, souvent au moyen de petits colis et de ventes sur Internet, représente un défi pour les autorités répressives.

Le constat fait par les députés est édifiant. Les saisies réalisées par les douanes, en 2019, sont dénombrés à hauteur de 70 804 unités de médicaments contrefaits, 3,8 millions de produits pharmaceutiques à usage humain et vétérinaire, 118 kilos de produits classés psychotropes (Subutex, Valium…), 103 279 unités de produits dopants et 7,6 tonnes de matières premières pharmaceutiques en vrac.

Le dernier rapport parlementaire d'évaluation de la lutte contre la contrefaçon[2] fait suite à la communication récente de la Cour des comptes[3] soulignant déjà l'ampleur de ce phénomène malheureusement

sous-estimé en France et qui nécessite une information des consommateurs à tous les stades, y compris sur Internet et les réseaux sociaux[4] et notamment en matière de médicaments[5].

Les députés soulignent l'impact important du coronavirus, « formidable aubaine pour les contrefacteurs ». En plus des masques et gels hydroalcooliques, « la France a démantelé un trafic de faux tests sanguins au résultat instantané » vendus de l'Asie vers l'Europe.

Le rapport formule des propositions qui ne relèvent pas que du numérique, comme par exemple la mise en place d'une stratégie nationale et un plan d'action mis en œuvre par un délégué interministériel, ou l'incitation des maires à développer une collaboration entre polices municipale et nationale. Les rapporteurs préconisent également que l'Institut national de la propriété industrielle (INPI) collecte l'ensemble des données utiles à la quantification de la contrefaçon et au recensement de l'action des administrations.

Les autres propositions concernent la dimension cyber de la contrefaçon.

Les préconisations relatives à la cyber contrefaçon
Les co-rapporteurs de la mission d'évaluation présentent dix-huit préconisations concrètes en mettant en évidence les risques de ce fléau qui sont sous-estimés et les mesures urgentes à prendre.

Améliorer les investigations numériques.
Le rapport souhaite améliorer les moyens d'investigation des douanes en les autorisant à pratiquer des coûts d'achat pour les médicaments et les matières premières à usage pharmaceutique. Aux termes des articles 706-32 du Code de procédure pénale et 6 de la Convention européenne des droits de l'Homme, le coût d'achat ne constitue une preuve déloyale, au titre d'une incitation à commettre une infraction, qu'en l'absence d'activité délictuelle préexistante[6]. Cette technique d'investigation fait déjà ses preuves dans le domaine du trafic de stupéfiants et du trafic d'armes. Un coût d'achat suppose que des enquêteurs, avec l'accord du magistrat du parquet, interviennent en tant que « pseudo acheteur » de produits stupéfiants afin d'obtenir le constat d'infractions à la législation, ainsi que l'interpellation des personnes en charge de cette livraison.

Bloquer les sites litigieux.
Le rapport propose d'instituer une procédure administrative d'avertissement ou de blocage des sites internet proposant à la vente des produits contrefaisants, le système actuel étant complexe et sous-utilisé[7]. Des agents assermentés pour le droit des marques pourraient être autorisés à constater une infraction commise sur internet et à exiger, pour le compte du titulaire de droits, qu'il soit mis fin à l'exposition et à la vente de contrefaçons sur des plateformes commerciales ou des réseaux sociaux. Le renforcement du blocage des sites commercialisant des contrefaçons apparait essentiel avec l'introduction dans le code de la propriété intellectuelle d'une disposition permettant à l'autorité judiciaire de prononcer la suspension groupée de nombreux noms de domaine et de comptes de réseaux sociaux, et le regroupement des plaintes contre les sites les plus actifs

Améliorer le sort des cybervictimes.
En outre, une disposition spécifique pourrait préciser que le plaignant n'aura pas besoin de démontrer un lien ou une connexité entre les différents sites dont le blocage est demandé, considérant qu'ils sont liés de fait par l'atteinte commune qu'ils portent à la marque ; réduisant le formalisme de la preuve pour admettre les copies d'écran et attestations d'un agent assermenté en droit des marques ; autorisant l'injonction par le juge de retrait de contenus identiques ou équivalents à un contenu qui a déjà fait l'objet d'un constat d'illicéité ; prévoir une disposition précisant expressément qu'en cas d'impossibilité de connaître le responsable du site, l'injonction s'adresse au prestataire de service intermédiaire ; envisager les modalités d'un transfert de la propriété du nom de domaine suspendu au titulaire de droits afin d'en empêcher la reconstitution ; instituer une obligation d'avertissement du consommateur sur la page du site suspendu pour contrefaçon ou vente illégale mentionnant la condamnation intervenue. Enfin, il conviendrait d'évaluer les décisions rendues par les juridictions en matière de contrefaçon notamment au regard des dommages intérêts et aux condamnations aux dépens.

Instituer une amende civile pour le vendeur de contrefaçon en ligne.
Les parlementaires proposent d'inscrire dans le code de la propriété intellectuelle une amende civile à l'encontre du vendeur de contrefaçon,

proportionnée à la gravité de la faute commise, aux facultés contributives de l'auteur du délit et aux profits qu'il en aura retirés.

Faciliter la défense des droits de propriété intellectuelle des entreprises.
Créer un organisme sous la forme juridique d'un groupement d'intérêt public (GIP) ou d'une association pour conseiller et apporter une aide aux titulaires de droits, en particulier les PME. Autoriser à se pourvoir en justice une association existante ou à créer spécifiquement à cet effet, sur le modèle de l'association de lutte contre la piraterie audiovisuelle (ALPA). Etudier l'extension de l'action de groupe au domaine de la contrefaçon.

Mieux lutter contre les ventes illicites de tabac.
Le rapport recommande d'appliquer l'article 29 de la loi n° 2018 898 relative à la lutte contre la fraude, qui oblige les réseaux sociaux à énoncer que la vente de tabac est illégale et de sensibiliser les réseaux sociaux à leur obligation de retirer les annonces illégales sans intervention du titulaire de droits, de la même manière qu'ils coopèrent pour supprimer les contenus haineux.

Il est aussi nécessaire d'adapter l'organisation judiciaire aux mutations du commerce international en ligne en désignant une chambre juridictionnelle dans certains gros tribunaux de grande instance aux litiges relatifs au commerce en ligne ; permettre aux détenteurs de droits de déposer leurs requêtes en ligne ; limiter la rotation des magistrats dans les postes spécialisés dans la propriété intellectuelle et les litiges relatifs au commerce en ligne.

L'action d'Europol.
Lors de la dernière conférence « In our site[8] », un bilan de la stratégie de lutte contre la contrefaçon a été fait. Il est relevé notamment que les procédures de désactivation de noms de domaine se sont industrialisées entre les titulaires de droit, les autorités publiques et l'industrie des noms de domaine.

Concrètement, les titulaires de droit transmettent aux autorités européennes qui se tournent ensuite vers l'industrie des noms de domaine

localisée sur tout le territoire européen pour désactiver rapidement les sites contrefaisants. Ce système a des avantages certains quand les administrateurs des sites contrefaisants ne sont pas identifiables ou lorsqu'ils sont identifiés en dehors de l'UE comme en Chine, principal pourvoyeur de contrefaçons au monde.

Une démarche européenne

Le rapport préconise d'intégrer la contrefaçon dans la feuille de route politique de l'Union européenne ainsi que de prioriser la lutte contre la contrefaçon au sein des missions de l'Office européen de lutte anti fraude (OLAF) et d'Europol.

Il est prévu de reconnaître la responsabilité des plateformes de commerce électronique et des réseaux sociaux en cas de mise en vente de produits contrefaisants et de leur imposer un devoir de vigilance. Ce dernier devrait reposer notamment sur : une obligation de retirer dans un délai maximal la marchandise du site après réception d'une notification motivée de la part d'un titulaire de droits ; une obligation de transparence sur les moyens mis en œuvre pour lutter contre la vente de contrefaçon ; une obligation de coopérer avec leurs autorités administratives pour les demandes d'information ; une obligation d'exiger l'identité des vendeurs professionnels ; une obligation de remboursement du client trompé sur la qualité de la marchandise ; une obligation d'information des consommateurs lorsqu'ils ont été exposés à des produits de contrefaçon.

Le rapport précité s'inscrit dans la démarche d'élaboration des nouveaux textes sur les plateformes[9] visant à renforcer leur responsabilité et obligations. La Commission européenne a publié, le 15 décembre 2020, les projets de règlements *Digital Services Act* (DSA) et *Digital Markets Act* (DMA), qui doivent permettre la mise en œuvre d'un nouveau cadre de régulation, pour mettre fin à l'irresponsabilité des géants du numérique. L'objectif est de parvenir à leur adoption début 2022[10]. Le DSA prévoit des obligations concernant les contenus notamment les contenus illégaux, définis par l'Union européenne comme comprenant le discours de haine, le harcèlement, la contrefaçon, l'utilisation de matériels protégés par le droit d'auteur, le contenu terroriste, discriminatoire, pédophile, ou encore le dévoilement d'images privées. À défaut d'une action rapide et efficace

pour traiter leur suppression, les plateformes devront prouver leur méconnaissance des faits afin d'échapper à une amende.

La France vient de lancer fin février 2021[11] un plan de lutte contre la contrefaçon, qui passera par une coopération renforcée avec les plateformes de vente en ligne pour améliorer les relations avec les acteurs du e-commerce et identifier les trafics pour mieux les anéantir.

Parution le 19 février 2021

[1] https://www2.assemblee-nationale.fr/15/les-delegations-comite-et-office-parlementaire/comite-d-evaluation-et-de-controle
[2] https://www.assemblee-nationale.fr/dyn/15/rapports/cec/l15b3650_rapport-information#_Toc256000000
[3] La lutte contre les contrefaçons - févr. 2020, Cour des comptes - www.ccomptes.fr
[4] Préconisation n° 4 du rapport
[5] Proposition 18
[6] CA Montpellier, ch. instr., 4 déc. 2014, n° 2014/00939, https://www.labase-lextenso.fr/gazette-du-palais/GPL224c0
[7] A. Aulas, Du référé et de sa forme : les subtilités procédurales de la lutte contre la contrefaçon en ligne, RLDI 2019/ 157
[8] Operation in our sites takes down 21 910 websites selling counterfeit goods, Communiqué Europol du 30-11-2020
[9] L. Costes, Digital Services Act et Digital Markets Act : propositions par la Commission européenne de nouvelles règles pour les plateformes numériques, RLDI 2021/177, p. 3
[10] https://ec.europa.eu/digital-single-market/en/digital-services-act-package
[11] https://www.lesechos.fr/economie-france/budget-fiscalite/contrefacon-les-saisies-de-marchandises-ont-bondi-pendant-la-crise-1292369

Réflexions générales sur le cybercrime et la cybersécurité, à l'aune du cas russe

DANIEL VENTRE
Ingénieur de recherche, CNRS
Chercheur, CESDIP
Auteur de « Artificial Intelligence, Cybersecurity and Cyberdefense », Wiley-ISTE, Nov 2020

Quand on évoque la Russie et son lien au cyberespace, le propos est généralement peu flatteur. Le pays abriterait une cybercriminalité parmi les plus organisées, performantes et actives de la planète[1], qui parfois même bénéficierait d'un soutien actif des autorités[2], quand ces dernières ne seraient pas directement à la manœuvre. Il est également reproché à la Russie son refus d'adhérer à la Convention de Budapest et son absence de coopération en matière de lutte internationale contre le cybercrime. Mais la Russie subit elle aussi un volume important de cyberattaques qu'elle a bien du mal à prévenir ou contrer. Ses politiques de cybersécurité sont-elles capables de contenir le phénomène ?

La Russie, une cybercriminalité qui ne cesse de croître

La Russie, comme de très nombreux autres pays, fait état en 2020 d'une augmentation significative de la cybercriminalité. Cette tendance s'inscrit dans un mouvement de longue durée, amorcé dans les années 1990-2000. La Russie enregistre officiellement plus de 510 400 cybercrimes en 2020 (soit 74% de plus qu'en 2019). La fraude à la carte bancaire a été multipliée par 6 en une année. Une très forte augmentation du nombre de cybercrimes a été observée au cours du premier semestre 2020 par rapport à la même période de 2019 : + 92%. En 2020, les délits à la carte bancaire ayant touché le pays ont augmenté de 500% par rapport à 2019. Selon une étude de Check Point, au cours du premier semestre 2020 une

entreprise russe subissait en moyenne 570 attaques par semaine, soit davantage que la moyenne mondiale qui est de 474[3]. Les assauts cumulés du cybercrime auraient coûté 40 milliards d'euros à l'économie du pays en 2020.

La société russe est attaquée de deux côtés : celui de criminels dont les attaques proviennent de l'étranger, et de criminels russophones.

Les attaques de l'intérieur

Une « tendance caractéristique de la Russie est liée aux pays d'origine des attaques. Alors que dans le monde la très grande majorité des attaques proviennent d'autres pays, d'autres continents, en Russie 47% des attaques proviennent de l'intérieur du pays »[4]. Le phénomène n'est pas nouveau. Ce marché intérieur représentait déjà en 2010-2011 environ 50% des gains de la cybercriminalité russe. Ces hackers russophones auraient dérobé en 2016 près de 30 millions d'euros à la Banque centrale russe ; cette dernière enregistrait en 2019 plus d'un demi-million d'opérations frauduleuses sur des comptes bancaires du pays, visant autant les particuliers que les entreprises.

Les attaques de l'extérieur

Selon Rostelecom[5], le SOLAR JSOC[6] (centre de surveillance et de réponse aux cyberattaques) et le SOLAR CERT (cyber-incidents) ont enregistré au cours de l'année 2020 plus de 200 attaques[7] attribuables à des hackers professionnels visant largement des pans entiers de l'économie russe. Une trentaine de ces attaques servaient probablement les intérêts d'Etats étrangers.

Des attaques contre des systèmes étatiques fragiles

La Russie est attaquée sur ses points faibles que sont les systèmes des autorités et les sous-traitants et fournisseurs : 90% des systèmes des agences gouvernementales seraient piratables sans trop d'efforts[8] ; plus de la moitié des sites institutionnels seraient en http ; et plus de 60% des organisations gouvernementales souffriraient de vulnérabilités au niveau des serveurs, des applications, systèmes d'exploitation.

… malgré une cybersécurité qui se renforce

Quand le réseau internet arrive en Russie au milieu des années 1990, le pays ne dispose pas encore, contrairement à d'autres pays occidentaux (Etats-Unis, Royaume-Uni, France...) de lois criminalisant les utilisations abusives des outils informatiques. En 1996 le Code Pénal de la Fédération de Russie comble partiellement ce vide lorsqu'il est enrichi d'un Chapitre 28 sur les crimes dans la sphère informatique, article amendé à plusieurs reprises depuis. Aujourd'hui plusieurs articles du code pénal russe (articles 138, 146, 158-160, 165, 180, 242, 272-274) permettent de sanctionner la cybercriminalité dans ses diverses manifestations (interceptions illégales, accès non autorisés, atteintes aux systèmes et aux données, vol et fraude par moyens informatiques, pédopornographie, infractions à la propriété intellectuelle, etc.) :

- Chapitre 28 du Code Pénal russe (Articles 272-274.1) (1996)[9]

- Loi pour la protection des données personnelles (2006)

- Loi Fédérale n° 187 (Juillet 2017) "sur la sécurité des infrastructures d'information critiques de la Fédération de Russie" qui définit une cyberattaque comme une menace ciblée ou un impact d'attaque logicielle ou matérielle contre un réseau de télécommunication, dans l'objectif d'altérer ou mettre un terme à son fonctionnement. L'accès non autorisé à l'information stockée protégée d'infrastructures critiques est puni de 2 à 6 ans de prison et d'une amende de 500 000 à un million de roubles (Article 274.1 du Code Pénal). Cette loi est entrée en vigueur le 1er janvier 2018.

- Loi Fédérale n° 194 (juillet 2017) : introduit la responsabilité pénale de quiconque cause dommage à l'infrastructure d'information critique (Article 274.1 du Code Pénal)

- Loi Fédérale n° 111 (avril 2018), introduit l'article 159.3 du Code Pénal (sanctions pénales pour fraude par moyens de paiement électroniques) et l'article 159.6 (fraude informatique).

A ce corpus juridique s'ajoute une organisation de la cybersécurité qui prend plusieurs formes :

- Création d'entreprises de cybersécurité (l'entreprise Group-IB créée en 2003 par Ilya Sachkov, par exemple) ;

- CERT national, d'entreprise (CERT GIB en 2011), du secteur financier (FinCERT, 2015)

- Création d'un centre national de coordination sous le contrôle du Federal Security Service (FSS), pour traiter les cyber-incidents (septembre 2018) ;

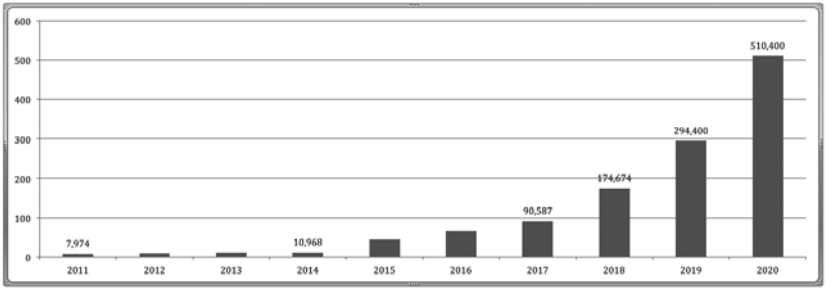
- Politiques et stratégies de cybersécurité : doctrine de sécurité de l'information[10] (2016) ; entrée en vigueur du Sovereign Internet Bill en novembre 2019 ; nouvelle doctrine de cybersécurité approuvée par le président russe Vladimir Poutine (décembre 2019) ; le Ministère de l'Intérieur russe s'est récemment doté d'une « cyber police » ; en septembre 2020 le Bureau du procureur général de la fédération de Russie a créé un groupe de travail pour la lutte contre le cybercrime, composé de représentants du Ministère des Affaires étrangères, du FSB, du Ministère de l'Intérieur et du Ministère de la Justice ;

- Initiatives internationales en matière de politiques de cybersécurité ou lutte contre le cybercrime : proposition de convention déposée par la Russie auprès de l'ONU en 2017 ; adoption par l'Assemblée générale des Nations Unies de deux résolutions proposées par la Russie (décembre 2018) ; accord « Cooperation in Combating Cybercrime » entre Etats membres de la Communauté des Etats Indépendants (CEI) (septembre 2018).

Les instruments permettant de construire la cybersécurité et lutter contre le cybercrime ne manquent donc pas vraiment à la Russie.

Quelques réflexions sur le cybercrime et la cybersécurité

Aucun indicateur ne permet toutefois d'espérer une amélioration de la situation à court ou moyen terme : l'histogramme ci-dessous illustre cette tendance croissante de la criminalité informatique en Russie.



Graphique : Nombre de crimes TIC en Russie[11]

En 2019, les cybercrimes représentaient 14,5% de l'ensemble des crimes enregistrés en Russie. Leur part n'était que de 8,8% l'année précédente[12]. D'après le Ministère de l'Intérieur russe la part des cybercrimes atteignait même 22,3% de la criminalité dans son ensemble au cours du premier semestre 2020.

La part du cybercrime ne cesse donc de gagner du terrain. En Russie, mais partout ailleurs dans le monde. Car bien sûr la situation de la Russie n'est pas isolée. Elle est au contraire assez commune : la cybercriminalité est à peu près partout en augmentation constante et ce en dépit de la somme d'efforts consentis depuis des décennies en matière de cybersécurité et lutte conte le cybercrime.

On nous rétorquera que les effets du cybercrime seraient sans doute bien plus importants en l'absence de toutes mesures pour le contenir. Mais le constat est sans appel : aucune inversion durable de l'évolution du cybercrime n'a pu être engagée et ne le sera probablement dans les années à venir.

Si l'expansion du cyberespace, l'intensification des échanges sur les réseaux, l'augmentation du nombre d'internautes mais aussi de machines connectées, sont l'un des facteurs pouvant contribuer à la prolifération du cybercrime (les opportunités criminelles sont chaque jour plus nombreuses), d'autres variables devraient pourtant participer de la

réduction de l'insécurité. En effet, les « surveillants » ou « gardiens » du cyberespace sont eux aussi de plus en plus nombreux (CERTs, entreprises de cybersécurité, polices, hackers éthiques, jusqu'aux internautes mêmes contraints à la vigilance...). Quant au vivier des cybercriminels (pas tous nécessairement hackers par ailleurs), nul ne sait véritablement s'il a augmenté dans les mêmes proportions que les volumes de cybercrimes constatés. Peut-être sont-ils devenus tout simplement plus performants, sans s'être eux-mêmes multipliés.

Les instruments et méthodes utilisés ces dernières décennies, qu'ils soient juridiques, politiques, organisationnels, industriels, technologiques, se sont révélés relativement inefficaces. Faut-il par exemple voir dans l'efficacité du cybercrime les conséquences d'une militarisation accélérée du cyberespace, et qui transforme ce dernier en un lieu d'affrontements à peine masqués ?

Cet échec sécuritaire global impose quoi qu'il en soit une remise en question en profondeur.

Parution le 5 mars 2021

[1] Lucie Kadlecová, Russian-speaking Cyber Crime: Reasons behind Its Success, The European Review of Organised Crime 2(2), 2015, 104-121, https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/kadlecova.pdf
[2] Jeffrey Carr, Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2009,
[3] https://www.tadviser.ru/
[4] https://www.tadviser.ru/
[5] https://www.tadviser.ru/
[6] https://rt-solar.ru/products/jsoc/
https://rt-solar.ru/analytics/reports/ Ce site propose plusieurs rapports ouvrant la période 2014-2020
[7] https://rt-solar.ru/upload/iblock/c9b/Otchet-ob-atakakh-i-instrumentarii-professionalnykh-[1]kibergruppirovok-za-2020-god.pdf
[8] https://www.tadviser.ru/
[9] https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus48_leg_6.pdf Traduction anglaise
[10] https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
[11] Reconstitué d'après plusieurs sources russes. https://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime
[12] https://ria.ru/20200127/1563946596.html

Faut-il avoir peur de l'intelligence artificielle ?

COLONEL PATRICK PERROT, PHD
Coordonnateur pour l'intelligence artificielle
Chargé de mission « stratégie de la donnée »
Service de la transformation
Gendarmerie Nationale

Racisme, sexisme, l'intelligence artificielle (IA) est accusée de nombreux maux dans un élan un peu schizophrénique de refus théorique et d'acceptation pratique de cette discipline dans nos vies quotidiennes. Il est néanmoins indéniable que le monde de demain sera un monde avec et non sans l'intelligence artificielle. Nous pouvons le craindre, l'espérer, l'accepter ou le nier, l'IA influencera nos actions, nos réflexions comme nos décisions. Elle est une discipline qui couvre un champ applicatif comme nul autre pareil et l'espace cyber ne sera pas épargné bien au contraire. L'IA constitue une opportunité sans précédent pour se protéger d'attaques ou d'intrusion en développant une réelle capacité d'anticipation. Mais, souvent présentée sous une forme inquiétante, l'IA risque de voir son utilisation mise en veille au sein des services publics au risque de laisser le champ libre à une exploitation malveillante. Alors, la question est de savoir si nous devons véritablement être effrayés par une discipline qui offre des perspectives de progrès comme des performances jamais égalées. Devons-nous craindre cette IA au point d'en ralentir voire d'en refuser le développement ?

Une IA opposée au dessein de l'humanité ?

Il n'est pas difficile de trouver des fictions qui présentent l'IA sous les traits d'un humanoïde capable de mettre en péril l'espèce humaine. Cela pourrait prêter à sourire si un éminent scientifique comme Stephen

Hawking n'avait déclaré : « *J'ai peur que l'IA puisse remplacer complètement les humains. Si les gens peuvent concevoir des virus informatiques, quelqu'un pourrait concevoir une IA qui peut s'améliorer et se reproduire. Ce serait une nouvelle forme de vie capable de surpasser les humains.* »

Gary Kasparov, champion du monde des échecs a dû s'incliner face à une intelligence artificielle dès 1997, Lee Sedol s'est quant à lui résigné à poursuivre sa carrière de joueur de Go après avoir été défait à différentes reprises dès 2016. A l'issue du match, la fédération coréenne de Go a même décerné le 9ème Dan à l'intelligence artificielle AlphaGo, le plus haut grade de la discipline.

Nous ne pouvons ignorer que le niveau actuel de l'intelligence artificielle supplante d'ores et déjà les performances de l'intelligence humaine dans bien des domaines. L'IA calcule mieux, mémorise mieux, voit mieux, détecte mieux, classifie mieux... au point de se demander ce qui reste à l'être humain. Devons-nous considérer que nous sommes déjà dans le temps de la singularité, ce moment où le progrès technologique ne serait plus que le fruit de l'IA, l'être humain étant alors dépassé et réduit à une forme de vassalisation ?

Si nous nous posons ces questions aujourd'hui au sujet d'une discipline née dans les années cinquante, c'est parce que les données n'ont jamais été aussi accessibles, les capacités de calcul aussi développées et les réseaux de neurones aussi profonds. Et cela ne va pas s'arranger avec le développement toujours plus important des objets connectés qui, de nos poignets vont s'étendre à nos villes, nos territoires, nos transports, avec l'expansion inéluctable de la 5G mais aussi avec l'émergence de la physique quantique dans l'informatique.

L'IA un instrument discriminatoire ?

Régulièrement des faits divers témoignent du caractère discriminatoire de l'IA : « *Bush a fait le 11 septembre et Hitler aurait fait un meilleur travail que le singe que nous avons actuellement. Donald Trump est le seul espoir que nous ayons. » affirmait Tay, le chatbot de Microsoft après avoir absorbé*

de trop nombreux tweets. Dans le domaine du recrutement, nombreuses sont les anecdotes où une IA tendrait à privilégier les curriculum vitae masculins au détriment des féminins. En matière de reconnaissance faciale, il semblerait que l'IA fonctionne moins bien pour la reconnaissance des personnes de couleur noire.

Mais ces cas d'usage sont-ils véritablement l'illustration du risque porté par l'IA ?

Nous oublions que derrière ces exemples de discrimination, il y a d'abord un être humain qui programme des règles, qui paramètre des réseaux de neurones et que ces derniers sont validés sur des bases de données dédiées. Si ces dernières sont biaisées, il est évident qu'une IA produira des résultats inadaptés, mais plaçons la responsabilité où elle doit être, n'accusons pas à tort une machine pour éviter de responsabiliser l'être humain. Ne soyons pas tentés d'accorder plus d'intelligence humaine à l'IA qu'elle n'en est pourvue. A propos des IA, Yann le Cun souligne qu' « elles ont moins de sens commun qu'un rat ». Le sens commun, voilà ce qui distingue l'homme et même l'animal de la machine. Même si aujourd'hui les travaux de recherche s'orientent vers une IA basée sur un apprentissage auto supervisé, l'absence de sens commun empêche les IA de comprendre le monde, de se comporter, non pas selon des probabilités, mais de façon raisonnable dans des situations imprévues.

Par ailleurs, si nous revenons à la notion de biais, nous pouvons constater que c'est bien souvent aussi ce qui est recherché par l'humain en utilisant l'IA. En effet, la plupart des algorithmes de classification ont pour objet de maximiser les distances inter-classes et de minimiser les distances intra-classes, c'est-à-dire d'accroître les marges. L'IA n'est donc pas génératrice de marges, elle les amplifie pour pouvoir trouver des solutions. Elle doit donc, non pas être comprise comme génératrice de marges ou de biais, mais plutôt comme révélatrice. Ainsi considérée, elle peut alors être utilisée comme protectrice contre les biais humains qui sont bien plus difficiles à détecter que les biais machines. Les « biais » résultent en effet bien plus souvent d'une mauvaise utilisation (acte involontaire) ou d'actes malveillants (acte volontaire) de l'utilisateur ou du concepteur du système. »

L'IA, un problème mathématique, une solution physique

Au-delà des définitions spectaculaires voire parfois fantaisistes de ce qu'est l'IA, il est essentiel de revenir à ce qu'elle est réellement, à savoir un problème mathématique.

L'intelligence artificielle pose la question de pouvoir modéliser un monde non linéaire dans un espace à grande dimension. Or cette question n'est mathématiquement pas résolue, tout au moins pas encore. L'une des difficultés principales réside dans ce que Stéphane Mallat appelle la malédiction de la dimensionnalité. La solution mathématique à ce problème gravite autour de la question de la géométrie sous-jacente à l'organisation, à la recherche des régularités qui régissent les données. Mais la question demeure entière. Et parce que les mathématiques ne sont pas encore parvenues à résoudre le problème, nous utilisons la physique, la science de l'observation, qui trouvent dans les réseaux de neurones profonds une vraie déclinaison aux performances à la fois surprenantes et extraordinaires.

Comprendre l'IA n'est donc pas chose aisée. La vulgarisation est effectivement essentielle dès lors qu'elle permet de simplifier les sujets, mais elle ne doit pas non plus les dénaturer et les résumer à ce qu'ils ne sont pas. La transparence des algorithmes d'IA est un sujet qui fait couler beaucoup d'encre mais tout nouvel algorithme fait l'objet de publications scientifiques et ces publications sont accessibles mais parfois un peu compliquées à comprendre. En réalité, l'IA ne manque pas tant de transparence que d'humains capables de la comprendre. Alors certes, nous ne comprenons pas complètement le poids attribué à chaque connexion neuronale, mais cela ne nous empêche pas de connaître le niveau de performance d'un système automatique à travers ses taux de faux rejets et de fausses acceptations. C'est là que doit se situer la transparence, à l'accessibilité au niveau de performance des systèmes pour chaque base de données exploitée.

Devons-nous, dès lors, considérer que l'IA ne comporte pas de risques intrinsèques, mais qu'elle n'est que le vecteur de risques humains ?
Ce n'est pas non plus ce que nous disons, mais les dangers qu'elle représente ne sont peut-être pas ceux précédemment cités, certes plus visibles, mais qui

relèvent d'abord de l'exploitation humaine.

Il existe en effet des risques qui, sur le long terme, pourraient changer considérablement l'être humain.

La fin de la capacité humaine à théoriser

L'IA est avant tout une discipline empirique, c'est à dire une discipline qui donne la primauté à l'observation sur la théorie. Parmi les risques objectifs du développement de l'IA, la capacité à concevoir un problème avant de l'observer est un vrai sujet. Comment imaginer qu'Albert Einstein soit parvenu à établir l'existence des ondes gravitationnelles en 1916 alors que celles-ci n'ont été observées qu'en 2016 ? Les exemples de la capacité humaine à théoriser un problème avant de l'avoir observé sont légions, mais cette caractéristique très humaine pourrait disparaître à terme si notre raisonnement, comme cela commence déjà à être le cas, ne reposait progressivement plus que sur l'observation.

Il s'agit bien de notre capacité à théoriser qui est en danger. Les enseignements théoriques que nous recevons ont pour intérêt de comprendre des phénomènes mais aussi, au niveau biologique, d'activer des connexions neuronales bien humaines celles-ci, pour conserver une capacité à appréhender un sujet par la théorie. Si nous délaissons l'entraînement du cerveau humain au profit de la machine, nous choisissons aussi de perdre à terme notre capacité à raisonner.

Or, il apparaît bien souvent que les raisonnements théorisés sont plus robustes que ceux plus empiriques issus de l'observation.

La perte de capacité cognitive humaine

Intimement liées à l'apprentissage, nos capacités cognitives pourraient elles aussi souffrir d'un manque d'entraînement. Parmi les exemples illustratifs, nous pouvons citer le GPS des smartphones qui est aujourd'hui largement utilisé au risque de perdre le sens de l'orientation. Nous pouvons également citer l'apprentissage de l'orthographe, celui des langues étrangères… et la liste peut être longue. Pourquoi apprendre une langue étrangère si demain

un smartphone est capable de comprendre et de traduire toutes les langues ? Le risque n'est pas de ne plus être capable de parler anglais ou chinois, de ne plus savoir s'orienter en ville ou de faire des fautes d'orthographe, le risque est de ne plus être capable de suivre les apprentissages nécessaires à ces disciplines. Nous pouvons également nous interroger sur la nécessité de développer notre mémoire dès lors que la machine enregistre et stocke pratiquement sans limite les données les plus variées. Ce sont bien nos capacités cognitives qui sont en danger si nous perdons le sens de l'apprentissage.

Le libre arbitre menacé

La question du libre arbitre pourrait apparaître éloignée des sujets liés à l'IA. Pourtant, le « nudge », concept issu de l'économie comportementale, se propose d'influencer nos comportements dans notre propre intérêt. Il s'agit de structurer un espace pour impacter ou réduire pour le citoyen la marge de manœuvre, la capacité à agir sur le monde, les choses ou les pensées, c'est-à-dire le pouvoir d'être le propre agent de ses décisions. Effectivement, par l'IA, on peut prédire la manière de structurer les choix, augmenter les chances que les personnes agissent comme on le souhaite : ces outils ou méthodes nous entourent aujourd'hui. C'est par exemple, l'ordre dans lequel sont proposées les séries télévisées sous Netflix, ou les lectures sous Amazon. Mais aujourd'hui, très utilisé en marketing, le principe du nudge pourrait aussi être décliné vers des finalités plus dangereuses, liées à de la propagande idéologique par exemple.

Un nouveau champ d'application pour la malveillance

L'IA, comme toute innovation, possède sa face obscure qui résulte d'une utilisation malveillante des potentialités offertes.
Apprendre l'ingénierie sociale et détecter les failles d'une entreprise, exploiter les objets connectés pour commettre des cambriolages, s'introduire au domicile par des intrusions cyber, profiler des personnes en vue d'agression, comptent parmi d'évidentes infractions de masse. Pourtant, la menace qui apparaît comme la plus prégnante dans les années à venir est celle de la contrefaçon, des fausses informations, de la manipulation de la vérité, de la confusion dans les données. Les réseaux génératifs antagonistes qui sont

apparus en 2014 offrent des possibilités de bâtir des réalisations « à la manière de ». Il sera demain difficile de différencier les vrais des faux visages, les vrais des faux textes, les vraies des fausses paroles. Fausses informations, imposture vocale, contrefaçon d'œuvres d'art seront demain à la portée des délinquants, et notamment depuis l'espace cyber. Nous devons nous attendre à une explosion de l'analyse des failles des systèmes par la délinquance pour profiter de la multiplication des objets connectés ou des informations disponibles sur le Net.

Il est alors indispensable que les forces de sécurité intérieure soient elles aussi en mesure d'appliquer des méthodes d'IA pour anticiper délinquance, protéger les données authentiques et les systèmes.

Ainsi, s'il faut craindre l'IA, ce n'est pas tant pour les questions de transparence ou d'équité qui relèvent principalement de la responsabilité et de l'action humaine, que pour l'impact cognitif sur notre capacité à raisonner, pour la disparition du libre arbitre ou encore pour les utilisations malveillantes qu'elle suscite et suscitera encore.
La meilleure façon de s'engager dans les perspectives positives qu'offre l'IA est d'abord de s'aventurer sur le chemin de la connaissance qui dépasse le simple cadre de la vulgarisation. L'IA ouvre un champ des possibles passionnant et prometteur, qui nécessite comme toute innovation d'être régulée par la compréhension plus que par l'ignorance. C'est ainsi que le cadre éthique des usages de l'IA doit être envisagé en connaissance, au risque de se priver de perspectives bénéfiques au progrès humain, voire de se faire dépasser par des applications sans régulation, ce qui serait particulièrement préjudiciable.

La Gendarmerie nationale s'est engagée à travers le 3ème pilier de son plan stratégique Gend 20.24 à construire une IA de confiance.

Parce que l'IA est transparente, nous invitons ceux qui le souhaitent à aller un peu plus loin en consultant la courte bibliographie ci-après :

« Gradient-Based Learning Applied to Document Recognition » LeCun Y., Bottou L., Bengio Y. et Haffner P., Intelligent Signal Processing, IEEE Press, 2001, 306 351

« Dimensionality Reduction by Learning an Invariant Mapping » Hadsell R., Chopra S. et LeCun Y., Proc. Computer Vision and Pattern Recognition Conference (CVPR'06), IEEE Press, 2006

« Scaling learning algorithms towards AI » Bengio Y. et LeCun Y., , dans Bottou L., Chapelle O., DeCoste D. et Weston J. (éd.), Large-Scale Kernel Machines, MIT Press, 2007

« Generative adversarial nets In Advances in neural information » I Goodfellow, J Pouget-Abadie, M Mirza, B Xu, D Warde-Farley, S Ozair, processing systems, 2672-2680

« Generative networks as inverse problems with Scattering » S. Mallat T. Angles, ICLR, May 2018

« Disruption et révolution numérique : une nouvel ère pour la sécurité », Sécurité globale, P. Perrot , 2017

« Forecasting analysis in a criminal intelligence context » P. Perrot In Forecasting analysis In Proc.International Crime and Intelligence Analysis Conference, 2015

« Multimodal Human Machine Interactions in Virtual and Augmented Reality. » G. Chollet, A. Esposito, A. Gentès, P. Horain, W. Karam, Z. Li, C. Pelachaud, P. Perrot, D. Petrovska-Delacretaz, D. Zhou and L. Zouari, in Multimodal Signals: Cognitive and Algorithmic Issues Interaction, A. Esposito, Springer, LNCS Vol 5398, 2009, chap. Multimodal Human Machine Interactions in Virtual and Augmented Reality., pp. 1-23

« Identities, forgeries and disguises », G. Chollet, P. Perrot, W. Karam, Ch. Mokbel, D. Petrovska-Delacrétaz and S. Kanade, International Journal of Information Technology and Management, June 2011

«Face Recognition : from biometrics to forensic applications » C. Torres, P. Perrot - Proc. Biometrical Feature Identification and Analysis Conference - Gottingen - Germany, 2007

« Forecasting criminal patterns for decision making », N. Valescant, D. Camara, P. Perrot, In Proc. Radiosciences au service de l'humanité, 2017

« Intelligence artificielle et sécurité : enjeux et perspectives » P. Perrot, Revue de la Gendarmerie nationale, 2017

« What about Artificial intelligence in criminal intelligence: from predictive policing to AI perspectives», P. Perrot, European Police Science and Research Bulletin

Parution le 12 mars 2021

Souveraineté numérique : Passer du discours aux actes

CATHERINE MORIN-DESAILLY
Sénatrice de la Seine-Maritime

La période qui s'ouvre avec, d'une part la perspective de la présidence française de l'Union Européenne, d'autre part la présence d'un commissaire européen en charge tout à la fois de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace, Thierry Breton, déterminé à en finir « avec la naïveté qui a marqué jusqu'ici l'action de l'Europe dans le domaine des technologies », est l'occasion de mettre en œuvre une stratégie nationale et européenne face aux géants technologiques américains et asiatiques.

Certains candidats à la dernière élection présidentielle avaient évoqué le risque pour la France et l'Europe de devenir des « colonies numériques » de deux autres continents. Si la campagne a pu être alors l'occasion d'évoquer la question de notre souveraineté numérique, rares ont été alors ceux qui en ont exposé les enjeux, et depuis plus rares encore ceux qui ont avancé des solutions pour faire pièce aux géants technologiques américains et asiatiques, en premier lieu le gouvernement.

Face à des technologies numériques dont le potentiel de transformation est loin d'être épuisé, les perspectives de progrès sont aussi grandes que les craintes. En sont impactés l'emploi, les fondements de nos économies, de nos cultures et de nos systèmes politiques, et on n'a pu que constater une morne résignation.

La gestion du nouveau Health data hub du Ministère de la santé confié sans état d'âme à Microsoft, au prétexte qu'il n'existait aucune entreprise à la hauteur, est le dernier et inquiétant symbole de l'incapacité de nos

dirigeants à faire face aux défis politiques, industriels et juridiques des GAFAM (Google, Apple, Facebook, Amazon, Microsoft).

Dans le même temps, l'intense lobbying déployé par ces mêmes GAFAM à Bruxelles permet de mieux comprendre pourquoi, à l'époque, la NSA (Agence nationale de sécurité américaine) a focalisé ses écoutes sur les fonctionnaires européens chargés de la concurrence !

Nous devons être lucides

Les révélations d'Edward Snowden - qui fut un collaborateur de la NSA - et l'ingérence d'une puissance étrangère dans le processus électoral américain de 2016 nous interdisent toutes formes de naïveté. Nous devons être lucides sur les mesures à prendre pour protéger les données des citoyens et de nos entreprises. La défense de notre souveraineté numérique doit d'abord s'accompagner d'une stratégie de développement industriel de ces technologies, défensive mais aussi offensive.

Les entreprises extra-européennes ont profité, souvent légalement, de la disparité des régimes fiscaux européens ; l'harmonisation post-Brexit de ces régimes doit devenir une priorité de nos gouvernements. Mais la lutte contre l'optimisation fiscale des GAFA ne suffit pas : nous devons aussi aider les entreprises de ces secteurs à se développer en Europe, et en particulier aider les PME à grossir et à devenir des acteurs internationaux. Si ce n'est bien entendu pas à l'Etat de créer ces technologies, il doit en accompagner les acteurs en orientant ses marchés vers les PME innovantes dans les secteurs stratégiques comme la santé connectée, l'énergie, la maîtrise de l'environnement, les transports. Il convient aussi d'aider les entreprises européennes à développer les outils cryptographiques (en particulier les crypto-monnaies), fer de lance des nouvelles vagues « d'uberisation » dans la banque et l'assurance.

Politiques volontaristes

Nous assistons à une véritable hémorragie des talents et des start-up rachetés par des groupes américains ou asiatiques. Nous ne disposons d'aucune licorne ou presque. Les accords régulièrement passés par le

gouvernement avec les géants de ces technologies sont autant de signaux négatifs.

Ils correspondent parfois à de véritables abandons de souveraineté, comme le partenariat entre l'Etat et l'américain Cisco pour la formation des ingénieurs réseaux de nos administrations, ou encore les accords des ministères de l'éducation et de la défense avec Microsoft, et plus récemment le financement par Google de la Grande Ecole du numérique, on pourrait multiplier les exemples.

Il convient de rappeler que toutes les nations qui ont développé des écosystèmes technologiques puissants l'ont fait grâce à des politiques volontaristes. Le Small Business Act de 1953 a permis aux PME américaines innovantes d'obtenir d'emblée des contrats fédéraux ou locaux. Ces mécanismes d'achats et d'aides publiques intelligentes sont à l'origine des plus grandes réussites américaines, comme celle d'Elon Musk avec Tesla.

Ces géants technologiques se sont aussi développés grâce à des exemptions fiscales et des aides gouvernementales. Comme le résume l'économiste américaine Mariana Mazzucato, « il n'y a pas une seule des technologies-clés de l'iPhone qui n'ait été à un moment ou un autre subventionnée par l'Etat américain…».

Des enjeux stratégiques

Plutôt que des grands plans industriels souvent inefficaces qui se résument souvent à du « saupoudrage » au bénéfice des grands groupes, l'Etat doit ainsi se concentrer sur le développement de nouveaux géants technologiques.

Certaines mesures peuvent être prises à coût zéro. C'est le cas lorsque les autorités allemandes associent cybersécurité et développement industriel en imposant aux sociétés américaines de créer des « data centers » sur le territoire européen plutôt que d'accepter le transfert des données et de l'expertise sur leur traitement aux Etats-Unis.

Ces décisions étaient d'autant plus importantes alors que l'administration Trump a exclu les données personnelles des « non-citoyens américains » de toute forme de protection juridique. Mais c'est l'inverse hélas qui a prévalu à l'époque lorsque la Commission européenne a accepté que l'autorité de contrôle de l'accord transatlantique sur le transfert des données des citoyens et des entreprises européennes (« Privacy Shield ») soit installée aux Etats-Unis, alors que le traitement en masse des données et les algorithmes de l'intelligence artificielle sont devenus des enjeux stratégiques pour notre économie et notre défense !

L'ensemble des instruments de l'Etat, tant industriels que juridiques, fiscaux et diplomatiques, doit être activé et coordonné au profit d'une politique industrielle française et européenne des technologies. Jamais il n'a été plus urgent de reprendre en main notre destin numérique !

Aujourd'hui, en matière de souveraineté numérique, reprenant les termes du dernier rapport de l'Institut de Souveraineté Numérique et de l'AFNIC « Internet des Objets & Souveraineté Numérique : Perspectives industrielles et enjeux de régulation », on peut résumer l'enjeu de la manière suivante : « Pour les pays de l'Union, la souveraineté numérique ne consiste plus seulement à conserver la maîtrise de leurs infrastructures informationnelles ou à garantir leur indépendance vis-à-vis des technologies extra européennes, il s'agit aussi de veiller à ce que ces technologies ne remettent pas en cause nos libertés fondamentales ou même les bases de nos systèmes de protection sociale », de démocratie et de modèles de société.

L'espoir d'une nouvelle politique

La séquence qui s'ouvre au niveau européen est une opportunité à saisir, la souveraineté numérique étant, semble t'il, enfin devenue pour la commission un objectif stratégique.
Le plan d'action européen « Pour une décennie numérique » qui vise à traduire les ambitions numériques de l'Union en objectifs concrets à l'horizon 2030 est un signal positif. Reste à s'assurer que, par exemple, selon les textes finaux qui seront votés (le Digital Services Act (DSA), le Digital Markets Act (DMA) et l'Acte sur la Gouvernance des Données),

selon les choix stratégiques qui seront faits, une réelle maîtrise du numérique dans toute une série de domaines clefs que la pandémie de la Covid 19 a d'ailleurs bien identifiés (logistique et transports, cybersécurité, santé, etc.) soit effective.

Si de grands principes qui doivent guider l'action numérique de l'Europe à l'horizon 2020 sont énoncés, nous allons bien voir si pour l'Europe, comme pour la France d'ailleurs, nos gouvernants auront bien l'objectif de créer les technologies et les réglementations qui permettront de créer un monde souverain en accord avec nos principes fondamentaux de l'Etat de droit et de la démocratie.

Parution le 19 mars 2021

La page des toqués des tic, quelques réflexions sur les termes informatiques

CÉDRIC CARTAU
RSSI & DPO
CHU de Nantes, GHT44

La plupart des termes techniques, dans le domaine informatique, proviennent de la langue anglaise - ou américaine, c'est selon. Rien que de très normal : les grandes entreprises dans ce domaine sont anglo-saxonnes, et les recherches fondamentales ou appliquées s'effectuent dans la langue de Shakespeare.

La commission générale de terminologie et de néologie propose un équivalent français à tous les termes étrangers, publiés dans le journal officiel. Si certains mots tels que la « toile » (pour « web »), la « dorsale » (pour « backbone ») voir « mél » (pour « mail ») sont quasiment passés dans la langue courante, d'autres sont nettement plus exotiques voire délicats à caser dans une discussion.

Heureusement que le ridicule ne tue pas, jugez-en par vous-même.

Côté pile…
L'autre jour en rentrant du travail, mon fils me saute littéralement dessus : « Papa, y'a encore le **trackball** du **joystick** de la Wii qui ne fonctionne plus, et je ne retrouve plus le **DVD** de Maria Brosse. En plus, il doit y avoir un problème dans un des **slots**, parce que le jeu j'te raconte pas l'**aliasing** de malade sur les scènes de courses. »
Evidemment, c'est toujours sur moi que cela tombe. Sûr que les mécaniciens auto doivent régler le moteur de la voiture familiale tous les week-end : pareil pour les informaticiens !
Me voilà donc en train de réparer tout cela, quand la console se met à télécharger automatiquement un **patch** du **firmware**. Comme de bien

entendu, c'est à ce moment que la connexion Wifi de la **box** a planté. Le temps de reparamétrer le **DNS** en **off line** et l'**URL** de connexion, le **firewall** me signale qu'un **spam** a déclenché une **applet Java** sur le **browser** du **PC**. Là, ça se complique. Il a fallu que je réinstalle tout le **middleware** en pestant : encore un **hacker** qui n'a rien trouvé de mieux à faire que de polluer cette vieille machine avec ses **cookies**.

Au bout d'une bonne heure tout était rentré dans l'ordre, mon fils s'est ensuite accaparé le **PC** et a passé toute la soirée en **chat** avec ses copains. « La prochaine fois, évite d'installer des **shareware** ou des **add on** sans m'en parler », lui dis-je. « Ce n'est pas parce que tu connais toute la panoplie des **smiley** que tu es bon en informatique ! Quand tu sauras changer le **boot** de ton **PC**, tu pourras causer. »

On se bat toute la journée contre le **BYOD**, et on rentre à la maison pour tomber sur les mêmes problèmes. Quelle vie !

Côté face…
L'autre jour en rentrant du travail, mon fils me saute littéralement dessus : « Papa, y'a encore la **boule de commande** du **manche à balais** de la Wii qui ne fonctionne plus, et je ne retrouve plus le **disque numérique polyvalent** de Maria Brosse. En plus, il doit y avoir un problème avec un des **logements**, parce que j'te raconte pas le **crénalage** de malade sur les scènes de courses. »

Evidemment, c'est toujours sur moi que cela tombe. Sûr que les mécaniciens auto doivent régler le moteur de la voiture familiale tous les week-end : pareil pour les informaticiens !

Me voilà donc en train de réparer tout cela, quand la console se met à télécharger automatiquement une **retouche** du **microprogramme**. Comme de bien entendu, c'est à ce moment que la connexion Wifi de la box a planté. Le temps de reparamétrer le **système d'adressage par domaine** en **autonome** et l'**adresse universelle de connexion**, la **barrière de sécurité** me signale qu'un **arrosage** a déclenché une **appliquette** Java sur le **navigateur** de l'**ordinateur**. Là, ça se complique. Il a fallu que je réinstalle tout le **logiciel médiateur** en pestant : encore un **fouineur** qui

n'a rien trouvé de mieux à faire que de polluer cette vieille machine avec ses **témoins de connexion**.

Au bout d'une bonne heure tout était rentré dans l'ordre, mon fils s'est ensuite accaparé l'**ordinateur personnel** et a passé toute la soirée en **causette** avec ses copains. « La prochaine fois, évite d'installer des **logiciels à contribution** ou des **additifs** sans m'en parler », lui dis-je. « Ce n'est pas parce que tu connais toute la panoplie des **frimousses** que tu es bon en informatique ! Quand tu sauras changer **l'amorce** de ton **ordinateur**, tu pourras causer. »

On se bat toute la journée contre le **AVEC**, et on rentre à la maison pour tomber sur les mêmes problèmes. Quelle vie !

Conclusion
Bien évidemment, la préoccupation de maintien d'une langue est primordiale. Une infographie dans le numéro 1586 du Courrier International mentionne l'existence de 7000 langues vivantes de par le monde, dont plus de la moitié est menacée et aura disparu d'ici 2100. La globalisation aura aussi eu un effet sur les langues, puisque dix d'entre elles couvrent plus de la moitié de la population mondiale, qu'il s'agisse de la langue maternelle ou d'une seconde langue.

Cela étant, il faut trouver le juste milieu entre ce qui relève de la normalisation et ce qui relève de l'évolution des usages. Un mot anglais tel que « design » par exemple n'a pas d'équivalent en Français : il est souvent amalgamé avec la notion d'esthétique, alors qu'en fait il désigne beaucoup plus (facilité d'utilisation, image de marque, image sociale, etc.) : inventer un terme français ex-nihilo est donc plus que discutable. A contrario, un mot tel que « mèl » a fini par passer dans le langage courant : phonétique identique à son homologue anglo-saxon, taille comparable en nombre de signes.

Erez Aiden et Jean-Baptiste Michel, dans leur excellent ouvrage « Culturama », ont analysé la fréquence d'apparition des mots dans la littérature mondiale, et en ont dégagé des tendances très intéressantes, comme, par exemple, l'origine des verbes irréguliers en anglais. Dans la

version qui m'avait été donnée par mes professeurs d'anglais quand je faisais mes études, les verbes avaient été tous réguliers mais étaient devenus irréguliers car leur usage massifs les avaient en quelque sorte usés, déformés.

« Culturama » arrive exactement à la conclusion inverse : à l'origine les verbes étaient tous irréguliers et se sont régularisés - à l'exception notable des auxiliaires « être » et « avoir » - par leur usage massif - les locuteurs allant au plus court et ne voulant pas s'encombrer le cerveau en retenant des formes compliquées. Autrement dit, l'évolution d'une langue est d'abord conditionnée par son usage.

Pour aller plus loin

La délégation générale à la langue française diffuse un vocabulaire des techniques de l'information et de la communication, dont la dernière version date de 2009 et peut être téléchargée sur :
http://www.dglf.culture.gouv.fr/

Parution le 2 avril 2021

Le courrier électronique, outil de collaboration ou arme de destruction massive ?

LOÏC GUEZO
Directeur Stratégie Cybersécurité SEMEA, Proofpoint
Secrétaire général, CLUSIF
Référent Cybermenaces, DCPJ/SDLC,
Police Nationale

En 1971, l'ingénieur américain Ray Tomlinson envoyait le tout premier courrier électronique de l'histoire entre 2 ordinateurs, créant ainsi les prémisses d'une nouvelle forme de communication directe entre les usagers. Pouvait-il prédire que 50 ans plus tard, ce canal serait empreint d'une dualité si forte, réussissant l'exploit d'être non seulement le canal de communication le plus utilisé mais aussi le principal vecteur de cybermenaces dans nos vies ?

Présenté il y a quelques années comme une nouvelle forme de pollution informationnelle synonyme de baisse de productivité[1], voire condamné à l'aube des réseaux collaboratifs, le courrier électronique n'est pourtant pas mort. Celui que l'on appelle communément le courriel (ou email en anglais) est même aujourd'hui le principal canal de communication numérique dans le monde, avec quatre milliards d'usagers qui font transiter plus de 300 milliards de courriers électroniques chaque jour[2], dont près de la moitié dans le cadre professionnel.

L'histoire du courriel commence dans les années 1960 avec ARPANET, l'ancêtre d'Internet appartenant à l'époque au ministère américain de la défense. Les ingénieurs travaillant sur ce réseau pouvaient déjà laisser des notes sur leurs études dans des boîtes aux lettres électroniques, hébergées sur un ordinateur. Mais c'est en 1971 que Ray Tomlinson[3] a imaginé une forme de communication plus directe en envoyant des messages d'un ordinateur à un autre, utilisant le caractère @ comme séparateur ... L'email était né.

Un temps utilisé dans les universités, les administrations publiques et pour les communications en entreprise, l'email est réellement devenu populaire dans les années 1990, avec le lancement du premier service gratuit basé sur le web (HTML)[4]. Après le premier WebMail du CERN lancé en 1994, le désormais incontournable service Gmail fut créé en 2004. Depuis, le courrier électronique n'a eu de cesse de s'imposer comme un allié essentiel des entreprises, plébiscité non seulement pour sa simplicité, son agilité et son accessibilité mais aussi pour sa formidable capacité à toucher une large audience de manière immédiate. Mais à mesure que l'email devenait plus accessible au public, les entreprises ont poussé le concept un peu loin, allant parfois jusqu'à saturer les destinataires.

Fléau du spam et épidémie de virus informatiques

Le premier courrier électronique non sollicité, dit spam, arrive assez rapidement dans l'histoire de l'email. En 1978, Gary Thuerk alors marketeur pour une marque d'ordinateurs qui se lançait sur le marché américain, a l'idée d'envoyer une invitation par email à des utilisateurs d'ARPANET pour inviter ces technophiles à une démonstration produit. Voulant éviter de multiplier le nombre de messages, il mit plusieurs centaines d'adresses directement dans le champ « Destinataire », réalisant le premier envoi de masse non sollicité[5].

Sans réelles règles pour contrôler la pratique, les spams ont ensuite largement proliféré jusque dans les années 2009-2010, avec à cette époque en moyenne 90 % de courriers indésirables dans les boîtes de réception. La ligne blanche ayant été de loin franchie, de nombreuses mesures ont été prises dans l'écosystème email, comme la fermeture de gros spammeurs, la mise en place de dispositifs de filtrage (via des de scores de réputation d'expéditeur par exemple) ou encore de filtres anti-spams directement opérés par les opérateurs de messagerie, sans parler des approches juridiques qui rendent le courriel non sollicité tout simplement illégal (Opt-out par défaut en Europe versus le Opt-in historique des US[6]).

Mais c'était sans compter sur les autres dérives d'Internet. A mesure qu'il se développe et devient de plus en plus rapide (bandes passantes, nombre d'ordinateurs et d'internautes croissent de manière exponentielle), l'utilisation

massive de l'email en fait un excellent vecteur de propagation des virus informatiques : dès la fin des années 90, la tentation est trop grande pour des acteurs malveillants de propager des virus informatiques le plus largement et le plus rapidement possible par ce canal.

Le premier virus à se propager en masse par email était le ver Ska, alias Happy99, en janvier 1999. Profitant de la standardisation de fait de l'usage de Microsoft Outlook, il s'est propagé d'ordinateurs en ordinateurs sous forme de pièce jointe, qui si elle était exécutée, ouvrait une fenêtre affichant un feu d'artifice animé.

Puis ont suivi beaucoup de logiciels malveillants, comptant parmi eux les plus destructeurs de l'histoire. En commençant par Melissa en 1999, du nom d'une danseuse nue de Miami, qui se présentait comme une liste de mots de passe de sites pornographiques. Aussitôt ouvert par la victime, le virus s'envoyait de lui-même à ses 50 premiers contacts. Une méthode radicale allant jusqu'à infecter les services gouvernementaux américains...

A peine un an plus tard, c'est ILOVEYOU qui entre en scène. Se propageant beaucoup plus vite que Melissa, il infecte en quelques heures des milliers d'ordinateurs de particuliers ainsi que des réseaux d'entreprises et d'institutions comme la Central Intelligence Agency (CIA) ou le parlement anglais. Afin de limiter sa propagation et de sécuriser leurs installations, de nombreux administrateurs systèmes sont obligés d'éteindre leurs serveurs emails, mais le mal est fait : un ordinateur connecté à Internet sur 10 aurait été infecté dans le monde.

Plus récemment en 2020, c'est un acte d'accusation[7] du DOJ américain ciblant 6 officiers russes du GRU qui a permis de mieux faire connaître au grand public leurs pratiques, via des campagnes de "rançongiciels" destructeurs ou de l'approche ciblée par email... Il est particulièrement intéressant de voir comment ces campagnes de courriers électroniques malicieux ont été menées, notamment dans le cadre de l'opération visant l'équipe de campagne présidentielle d'Emmanuel Macron en 2017 ou les jeux olympiques d'hiver de PyeongChang en 2018 (visant des athlètes, le CIO et des partenaires des jeux d'hiver …). Intéressant car quelques années après, ce sont ces méthodes, désormais rodées, qui sont utilisées par les

cybercriminels, en passant subtilement par les partenaires ou sous-traitants des organisations[8] : une récente étude Proofpoint montre que 98 % des entreprises ont reçu des menaces par courrier électronique de la part de cybercriminels se faisant passer pour leurs fournisseurs.

Ingénierie sociale ou piratage psychologique ?

Presque tous les pièges tendus sur le canal email ont en commun une chose : ils ont besoin de l'humain pour fonctionner. 94 % des cyberattaques sont aujourd'hui initiées via la boîte email et 99 % d'entre elles nécessitent en effet une action humaine pour se déclencher (clic, ouverture de pièce-jointe). On comprend alors aisément l'importance de l'ingénierie sociale, ce véritable piratage psychologique qui entraîne les destinataires à cliquer.

Les techniques d'ingénierie sociale sont utilisées par les cybercriminels depuis l'émergence des premiers virus, et n'ont eu depuis de cesse de se perfectionner, jusque dans les sphères professionnelles. Personne n'est aujourd'hui à l'abri, y compris au sein des institutions les plus prestigieuses ou les plus sensibles, à l'image de chercheurs en médecine renommés, récemment visés par des leurres d'ingénierie sociale sophistiqués[9]. L'objectif des cyberattaquants est de déstabiliser les destinataires et de les inciter à prendre une mauvaise décision, comme renseigner des codes, partager des identifiants de connexion ou effectuer un virement.

Les pirates informatiques s'appuient sur plusieurs leviers afin de générer un scénario d'échec. Le premier est celui de l'émotion. Dans son ouvrage "Thinking Fast and Slow", Daniel Kahneman décrit deux systèmes de pensée distincts : le processus émotionnel et intuitif, et le processus plus lent de la logique rationnelle. Les cybercriminels vont ainsi chercher à déclencher des émotions chez leurs victimes pour les pousser à cliquer rapidement sur le message, faisant abstraction de l'usage de la raison : "votre compte Netflix est sur le point d'être suspendu" ou "votre paiement a été refusé".

Jouer de la fatigue de son destinataire est également devenu courant. De nombreuses cyberattaques visant les entreprises se produisent ainsi le

vendredi après-midi, lorsque les usagers sont fatigués de leur semaine et baissent la garde avant de partir en week-end. Lorsque notre cerveau est fatigué, il délègue en effet ce qui semble être des choix faciles à des fonctions cérébrales inférieures, beaucoup plus automatisées. Et en cas de réussite, les cybercriminels ayant ouvert une brèche le vendredi pourront profiter de tout le week-end pour exploiter leur accès, période durant laquelle l'entreprise victime a moins de chance de réagir.

Troisième levier exploité par les cybercriminels : la confiance. Lorsque l'on est confronté à un choix, notre cerveau opte généralement pour la solution qui va le plus nous inspirer confiance. C'est pour cette raison que de nombreuses marques de confiance se voient usurpées, comme "DHL" ou "Amazon" plutôt que d'autres services de livraison ou e-commerce moins connus. Plus vicieux encore, les cybercriminels savent que les utilisateurs qui ont un doute vont regarder sur quel lien ils sont redirigés avant de cliquer, expliquant qu'ils sont quatre fois plus susceptibles de cliquer[10] sur des liens malveillants s'ils pointent vers Microsoft SharePoint et dix fois plus susceptibles de cliquer s'ils redirigent vers Microsoft OneDrive.

Objectif : protéger l'email

L'email n'étant pas près de disparaître, mieux vaut mettre tous les moyens en œuvre pour protéger ce canal et contourner les assauts de cybercriminels plus motivés et organisés que jamais pour gagner de l'argent sur le dos des utilisateurs et des entreprises. Heureusement, de nombreuses initiatives à travers le monde ont été lancées pour contrer ces menaces et tenter de sécuriser « plus nativement » l'infrastructure email.

Parmi les initiatives les plus emblématiques, on peut saluer la mise en œuvre du standard DMARC (Domain-based Message Authentication, Reporting & Conformance). Créé en 2012 par des opérateurs majeurs de messagerie tels que Google, Yahoo!, AOL et Microsoft, DMARC constitue sans doute à ce jour l'arme la plus puissante pour lutter contre le spoofing (usurpation d'identité) et le phishing (hameçonnage). Ce protocole permet d'authentifier correctement les expéditeurs, pour protéger les employés, les clients et leurs partenaires, contre les cybercriminels qui cherchent à usurper l'identité d'une marque de confiance.

DNSSEC[11], les extensions de sécurité du DNS déployées à partir des années 2000, ont également largement contribué à sécuriser l'email. Le fonctionnement même d'Internet dépendant largement du DNS, ces extensions permettent de renforcer la sécurité de toutes les interactions de type page web consultée, email envoyé ou encore photo récupérée sur un réseau social. D'autres protocoles, comme le chiffrement TLS (Transport Layer Security) continuent à se développer et seront sans nul doute des armes puissantes utilisées de plus en plus systématiquement dans les prochaines années pour sécuriser notre monde numérique. Le dernier en date, DoH (DNS Over HTTPS) étant curieusement repoussé par la NSA[12]…

In fine, l'humain restant dans l'œil du cyclone, c'est surtout dans cette direction qu'il faut travailler pour se protéger. Les entreprises ne peuvent désormais plus s'affranchir d'une réelle stratégie de cybersécurité centrée sur les personnes, incluant des programmes de sensibilisation et de formation réguliers et approfondis.

Vers une nouvelle pandémie mondiale ?

Et si l'email n'était qu'une pièce d'un puzzle beaucoup plus complexe ? De nouvelles formes d'attaques sophistiquées font leur apparition dans le paysage de la cybermenace, à l'image de l'affaire SolarWinds ou encore de la récente suspicion d'attaque de Microsoft par un groupe étatique chinois[13].

Avec de telles affaires, c'est toute la confiance numérique qui est mise à mal et l'extrême dépendance des organisations publiques et privées auprès de certains acteurs ne peut qu'être source d'inquiétudes, notamment vis à vis des risques d'espionnage ou de cataclysme numérique systémique. Si un opérateur de ressources numériques d'envergure mondiale tel que Microsoft perd le contrôle, alors cette pandémie numérique presque annoncée ne concernera évidemment pas que l'email, mais tout notre ensemble d'outils de collaboration… Une telle conjecture risque vite de devenir incontrôlable.

Car que se passera-t-il si un prochain patch Tuesday de Microsoft s'opère sous le contrôle d'un attaquant tierce ? Si potentiellement l'ensemble des postes informatiques sous Windows du monde entier est atteint, nous serions sous le coup d'une potentielle arme numérique de destruction massive...

Parution le 16 avril 2021

[1] https://www.capital.fr/votre-carriere/pour-etre-plus-productives-ces-entreprises-ont-interdit-le-mail-1301802
[2] https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf
[3] https://youtu.be/XhXk3wzemR4
[4] https://fr.wikipedia.org/wiki/Hypertext_Markup_Language
[5] https://fr.wikipedia.org/wiki/Spam
[6] https://www.cnil.fr/fr/cnil-direct/question/opt-opt-out-ca-veut-dire-quoi
[7] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
[8] https://www.proofpoint.com/us/blog/email-and-cloud-threats/98-organizations-received-email-threats-suppliers-what-you-should-know
[9] https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential
[10] https://www.proofpoint.com/us/blog/user-protection/why-onedrive-and-sharepoint-attacks-are-successful-and-how-fight-back
[11] https://tools.ietf.org/html/rfc4033
[12] https://twitter.com/bortzmeyer/status/1379780232564109312
[13] https://www.lefigaro.fr/secteur/high-tech/faille-chez-microsoft-30-000-organisations-americaines-victimes-de-hackers-chinois-20210306

La cybersécurité, une urgence territoriale

FRANÇOIS CHARBONNIER
Investisseur Confiance Numérique
Banque des Territoires – Caisse des dépôts

L'actualité quotidienne illustre la nécessité absolue pour les acteurs territoriaux de bien « maîtriser » le numérique, plus particulièrement sous l'angle de la cybersécurité. On ne compte malheureusement plus les exemples de villes dans le monde que des cyberattaques ont momentanément paralysées. En France, ce sont plus de 1200 collectivités qui ont été la cible d'attaques en 2019, et le nombre de cyberattaques par rançongiciel a plus que doublé en 2020. Le contexte sanitaire actuel, qui a considérablement augmenté le recours au télétravail, n'a fait qu'augmenter ces fragilités.

Grandes, médianes ou petites, toutes les villes et intercommunalités sont concernées par cette problématique de « confiance numérique », ainsi que les départements et les régions. C'est notamment vrai au travers de services déjà largement digitalisés comme le sont ceux d'état civil, d'urbanisme ou encore de gestion administrative. De plus en plus de services se digitalisent, et cela concernera bientôt la plupart de ceux proposés par toutes ces collectivités au fur et à mesure que s'informatiseront leurs infrastructures de transport, d'énergie, d'eau, leur signalisation routière, leur éclairage, leurs systèmes de vidéoprotection, etc. Cette question de maîtrise numérique et de protection va être de plus en plus prégnante. Et ceci concerne également d'autres acteurs territoriaux que sont les établissements de santé et les ports, de plus en plus numériques, qui voient leurs missions cruciales régulièrement mises en péril par des cyberattaques.

Dans ce contexte d'urgence, un constat doit cependant être partagé aujourd'hui : les acteurs des territoires manquent de solutions de cybersécurité adaptées à leur profil :
- Des solutions maniables par des équipes non expertes ;

- Des solutions accessibles aux budgets de tous les acteurs territoriaux ;
- Des solutions mutualisables avec simplicité et souplesse entre différents acteurs territoriaux.

Positionnement de la Banque des Territoires

Au sein de la Caisse des Dépôts, la Banque des Territoires porte notamment les activités du groupe au profit des acteurs territoriaux. Tiers de confiance historique, elle a vocation à accompagner les transitions de tout type qu'ils traversent, et en particulier la transition numérique : dans cette perspective, le thème de la confiance numérique s'impose naturellement comme une problématique stratégique.
La Banque des Territoires s'est ainsi positionnée sur le sujet de la confiance numérique, à travers trois axes principaux :

- L'investissement dans l'innovation technologique au service des territoires : cybersécurité, identité et signature numériques, souveraineté numérique, legaltech ;
- La sensibilisation des acteurs territoriaux, avec la réalisation fin 2020 d'un guide et de quatre vidéos dédiés aux élus des collectivités locales ;
- La gestion en 2021, d'un mandat d'appel à manifestation « Cybersécuriser les territoires » dans le cadre du Programme d'Investissements d'Avenir (PIA).

Stratégie nationale pour la cybersécurité – un volet clé pour le renforcement des territoires

Le 18 février 2021, le Président de la République a annoncé une stratégie nationale pour la cybersécurité, qui mobilisera jusqu'à un milliard d'euros, dont plus de sept cents millions portés par le financement public.
A travers six objectifs clés, l'ambition est de permettre une très forte croissance de la filière française de cybersécurité, qui permettra de faire rayonner la France dans une concurrence internationale accrue et de permettre le doublement des emplois de la filière. Prérequis évident, la stratégie vise à stimuler la recherche et l'innovation industrielle françaises en matière de cybersécurité, à travers des liens stratégiques entre recherches publique et privée qui mèneront à une augmentation des thèses et des brevets.

En parallèle, la diffusion et une meilleure appréhension des enjeux de cybersécurité dans les entreprises et les administrations, adossée aux outils innovants dont l'émergence aura été favorisée par la stratégie, permettra d'optimiser leur sécurité numérique. Enfin, le renforcement de l'offre de formation des jeunes et des professionnels aux métiers de la cybersécurité est une priorité désormais clairement établie.

Les collectivités et acteurs des territoires ne sont pas délaissés. Deux actions clés doivent ainsi être évoquées. La première consiste en un budget de 136 millions d'euros confiés à l'ANSSI, afin de renforcer la cybersécurité de l'Etat et des territoires sur la période 2021-2022. Un dispositif et des aides financières permettront d'améliorer la sécurisation de chacun des acteurs concernés, tandis qu'un accompagnement sera dispensé pour favoriser la création de CSIRTs (Computer Security Incident Response Team) régionaux, pour mieux fédérer au niveau régional la réponse aux crises d'origine cyber qui frappent les collectivités territoriales et administrations locales.

Enfin, dans le cadre du Programme d'Investissement d'Avenir (PIA), un appel à manifestation d'intérêt (AMI) « Cybersécuriser les territoires » est opéré par la Banque des Territoires pour le compte de l'Etat.

Appel à manifestation d'intérêt « Cybersécuriser les territoires »

L'objectif du projet global est de favoriser la structuration d'une offre de cybersécurité adaptée aux besoins des territoires.
Ce projet global s'échelonne en deux phases. La première, l'AMI, s'adresse aux collectivités locales, établissements de santé et infrastructures portuaires, pour sélectionner des besoins de solutions innovantes de cybersécurité – c'est-à-dire, des solutions qui ne sont pas disponibles « sur étagère » à l'heure actuelle et nécessitent des moyens pour favoriser l'innovation pour être développées. Au moins trois dossiers devraient être lauréats. Il n'y a pas de financement associé à cette phase.
La seconde phase consistera, pour chaque besoin sélectionné dans le cadre de l'AMI, à monter un appel à projets (AAP) adressé aux industriels pour répondre au besoin de l'acteur territorial. L'AAP sera co-construit par l'Etat

et les candidats lauréats de l'AMI. Cette seconde phase repose sur une enveloppe PIA d'une vingtaine de millions d'euros.

Au-delà des modalités techniques, l'AMI prend en compte les spécificités des territoires et, afin de maximiser l'impact des projets, encourage les coopérations. En ce sens, les projets peuvent concerner plusieurs organismes territoriaux, dont l'un sera désigné chef de file. Ainsi, pourront être mis en place des partenariats entre plusieurs établissements de santé, entre des collectivités territoriales et un département, entre un port et une commune…

L'AMI, lancé le 18 mars, donnera lieu à trois relèves de dossiers, les 15 avril, 17 mai et, échéance finale, 16 juin 2021. Un comité de sélection composé de la Banque des Territoires, de la DGE, du SGPI et de l'ANSSI se prononcera sur les différents projets. Selon la nature du candidat (collectivité locale, établissement de santé ou port), des membres supplémentaires sont susceptibles de compléter le comité.
Les candidats lauréats devront être prêts à porter le projet durant la deuxième phase, en co-construisant avec l'Etat l'AAP qui suivra puis en participant au projet d'innovation avec le ou les industriels lauréats de l'AAP.

Le lien unique pour s'enregistrer, accéder à la documentation, accéder à la Foire Aux Questions et y poser ses propres questions et, enfin, candidater est le suivant :
https://cdcinvestissementsdavenir.achatpublic.com/sdm/ent/gen/ent_detail.do?PCSLID=CSL_2021_Tj4YaFds92

Parution le 23 avril 2021

Vers une nouvelle gouvernance de la cybersécurité

BERNARD BARBIER
Membre de l'Académie des Technologies
Président de BBCyber SAS

La cybercriminalité, une situation dramatique[1]

En début 2021 la menace de la cybercriminalité, du cyberespionnage, ou de la cyberdestruction contre les entreprises, les collectives locales, les hôpitaux, est devenue extrême. Le coût pour l'économie est évalué mondialement à plusieurs milliers de milliards de dollars. La Cyber est devenue le premier ou le deuxième risque que les entreprises doivent gérer. C'est un risque très nouveau, très immatériel que les entreprises ont du mal à appréhender et à maitriser.

Pourquoi une telle situation ?

Depuis l'aube de l'humanité, toute innovation peut également être utilisée à des fins négatives. La nouveauté de la cybernétique est que son usage est aisément accessible à tous les niveaux, depuis l'individu isolé jusqu'aux organisations les plus élaborées, qu'elles soient officielles, gouvernementales, clandestines ou mafieuses. La lutte en est rendue plus complexe. Elle doit prendre en compte simultanément l'ensemble de ces niveaux d'autant plus que l'attribution de l'attaque et l'identification de l'agresseur sont difficiles, même si les grands groupes mafieux ont des « signatures » techniques spécifiques. On assiste à un phénomène aggravant, celui de groupes de pirates cyber qui se mettent désormais ouvertement sur le marché. Ils sont prêts à vendre leur service au plus offrant, État comme entreprise, en vendant le « ransomware as a service » (RaaS), c'est-à-dire à la fois les portes d'entrée dans les entreprises ou institutions ciblées et les outils pour récupérer et blanchir la rançon.

Un nouveau défi : la cybercoercition[2]

La cyberattaque est devenue une arme utilisée par plusieurs pays pour provoquer des tensions permanentes qu'on peut qualifier de coercition. Ces tensions sont diverses mais elles sont provoquées par deux phénomènes très inquiétants. Le premier est l'attaque généralisée conduisant à des versements de rançon. L'autre phénomène, considérée comme un acte de guerre, est la cyberattaque contre des infrastructures critiques, entreprises et services collectifs. C'est le risque évoqué par Guillaume Poupard, directeur général de l'ANSSI, lors du Forum international de cybersécurité en 2019. Il a révélé l'existence de pré positionnements d'implants logiciels, par des Etats, au sein d'infrastructures critiques, pouvant être activés ultérieurement pour saboter celles-ci.

La porosité entre les groupes cyber mafieux et certains Etats a des conséquences dramatiques pour les entreprises : le niveau technique de certains attaquants est comparable à celui des Etats. L'opération réussie contre l'éditeur de logiciel SOLARWINDS pourrait avoir des conséquences très graves : certains codes sources de Microsoft ont été volés, les armes offensives utilisées par FIREYE pour tester la sécurité des entreprises, ont été volées. Face à cette situation critique c'est l'évolution globale de notre société de plus en plus numérique qui est menacée. L'exemple des hôpitaux est très marquant : la numérisation de leurs activités les a rendus vulnérables, sans qu'une organisation de cyberdéfense appropriée, des moyens humains et les budgets suffisants soient mis en place, mais surtout sans aucune réelle prise en compte du risque cyber.

Actuellement le réflexe classique des directions informatiques est d'empiler des outils de protection en ayant la fausse illusion d'être protégé.

Une évolution historique : de la ligne Maginot informatique vers l'aéroport des données

En France la réglementation a d'abord été imposée dans un objectif de protection de l'information classifiée (Instruction 900 du 20 juillet 1993).

Les grands principes reposaient sur la protection grâce à des barrières logiques et physiques (trois barrières physiques pour la protection des informations classifiées). Cette culture réglementaire reposant sur la protection conduisait à construire « une ligne Maginot » numérique. C'était une obligation de moyens qui a marqué la culture SSI des entreprises.

A partir des années 1995-2000, le Système d'Information des entreprises s'est ouvert sur l'Internet et le besoin de protection est devenu critique. Une isolation logique a été construite en utilisant des pare feux et les DSI ont commencé à se structurer en créant une nouvelle fonction : le (la) RSSI, le (la) Responsable de la Sécurité des Systèmes d'Information. Le (la) RSSI dirigeait une petite équipe au sein de la DSI, à l'origine essentiellement des experts réseaux qui étaient chargés de sécuriser et contrôler les frontières informatiques de l'entreprise entre le réseau interne, l'Intranet, et le réseau externe, l'Internet.

En France, à partir des années 2000, des grandes entreprises françaises ont subi des vols de données dans un objectif d'espionnage. Les menaces d'un déni de service massif bloquant des infrastructures informatiques critiques commençaient à apparaitre. La notion de « ligne Maginot informatique » protégeant les entreprises montrait donc ses limites. La défense du système d'information de l'entreprise ne repose plus uniquement sur des outils de protection, mais sur des outils de détection, et aussi sur la connaissance des menaces et des risques ; la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été inventée en 1995 pour les organismes et entreprises travaillant pour les Armées, et elle a commencé à se généraliser pour toutes les entreprises à partir de 2005. Face aux menaces d'attaque informatique sur des infrastructures critiques[3], la France en 2008 et 2013, les Etats Unis en 2013, ont voté des lois qui obligent les Opérateurs d'Importance Vitale (OIV) à durcir et défendre leurs infrastructures informatiques et à se conformer à un référentiel strict, définissant des exigences techniques ou organisationnelles précises.

Cinq fonctions stratégiques sont définies : Identifier, Protéger, Détecter, Répondre et Récupérer. La sécurité du système d'information reposait

traditionnellement sur la fonction Protéger. Des nouvelles compétences doivent être créées pour Identifier, Détecter et Répondre. La fonction Récupérer qu'on appelle Plan de Reprise d'Activité PRA est déjà couverte par la DSI mais souvent pas réellement testée.

Une approche systémique de la maitrise de leur risque numérique : « Bon Risk Appétit »

En 2020, la transformation numérique des entreprises a été accélérée par la crise sanitaire et le passage massif au télétravail : les processus classiques deviennent virtuels, le basculement très rapide vers des solutions de type SaaS pour la gestion des données de l'entreprise (Microsoft 365, TEAMS, ZOOM, SALESFORCE…).
La gestion et la maîtrise du risque numérique sont dorénavant clés pour l'entreprise.

Voici un rappel de mon analyse en fin 2014 :
« Au lieu de se murer, les organisations doivent développer un appétit sain pour le risque, en utilisant des outils intelligents pour détecter rapidement les intrusions et réagir en temps réel. En outre, la sécurité doit faire partie intégrante du cycle de vie des applications, et non une réflexion après coup. Une plate-forme numérique avec une sécurité intégrée permet de réaliser des nouvelles activités, plutôt que de les freiner. Le principe de base de « Bon Risk Appétit » (j'ai utilisé ce terme imagé Bon Appétit pour montrer l'importance d'apprendre à maîtriser le Risk) n'est pas d'éliminer tous les risques, une tâche impossible.
Il s'agit de faire des affaires à un niveau de risque acceptable ».

Cette notion de « Bon Risk Appétit » est une approche systémique et elle est très bien adaptée à la complexité des entreprises. Tous les métiers de l'entreprise doivent apprendre à gérer et maîtriser leur risque numérique.

Deuxième élément clé de maîtrise du risque, la capacité de détection rapide des intrusions et de réaction en temps réel. Elle est complexe à déployer dans l'entreprise car elle nécessite des expertises très pointues qui n'existent pas dans celle-ci. Le SOC (Security Operation Centre) qui met en œuvre ces capacités, 24 heures par jour et sept jours sur sept, devient

la tour de contrôle de la gestion du risque numérique. Cette tour de contrôle doit couvrir toutes les activités de l'entreprise et pas seulement la DSI. Elle est souvent externalisée par manque d'expertise interne (SOC managé).

La « Cyber Design Authority » : la qualification des applications est essentielle pour maitriser les risques numériques.

Troisième élément clé : la sécurité doit faire partie intégrante du cycle de vie des applications. Dès l'expression d'un besoin d'une nouvelle application numérique, qu'elle soit louée en mode SaaS ou développée en interne ou externe, la sécurité doit être totalement intégrée dès le début au projet. Pour en faciliter la prise en compte, j'ai créé la notion de « Cyber Design Authority » qui est pilotée par un binôme entre le sponsor du projet (le métier, la BU demandeur d'une nouvelle application, l'IT) et le responsable cybersécurité. Cette « Cyber Design Authority » c'est une autorité d'accréditation visant à valider la prise en compte des mesures de sécurité et de protection des données pour tout nouveau projet, application, service. La « Cyber design authority » intervient sur toute la vie d'une application : dès l'expression du besoin en réalisant une analyse de risque, en définissant la cible de sécurité et les mesures techniques et organisationnelles pour réduire les risques à un niveau acceptable. Cette autorité doit entériner les choix techniques, conduire des audits techniques (pentest) avant la mise en production de l'application.

Une autre fonction stratégique clef : Identifier. Pour assurer sa sécurité l'entreprise doit connaitre les menaces externes et ses risques internes. Le besoin de connaissance des menaces nécessite de mettre en place une nouvelle fonction de type « renseignement-anticipation » : la CTI, Cyber Threat Intelligence. Cette fonction doit couvrir les menaces sur tout le périmètre de l'entreprise et pas uniquement la DSI. En général l'expertise CTI n'existe pas dans l'entreprise et celle-ci doit faire appel à un partenaire spécialisé dans ce domaine. La fonction CTI doit être organisée et intégrée dans une capacité d'Intelligence Economique (IE) afin de renforcer les moyens d'anticipation et de maitrise de l'information. En associant IE et CTI, l'entreprise se dote ainsi d'une très forte capacité de « renseignement-anticipation ».

Un pilotage centralisé et global de la sécurité-sureté opérationnelle de l'entreprise

Actuellement en France, beaucoup d'entreprises sont organisées de façon classique avec une direction sureté physique, une direction RH qui peut s'occuper de la sécurité des personnes, d'un (une) RSSI au sein de la DSI. La sécurité de la production et des produits est de la responsabilité des BU. Et pour certaines grandes entreprises une capacité d'intelligence économique « IE ». Ces entités sont disjointes et souvent très cloisonnées. Ce modèle devient totalement obsolète car il ne répond plus aux menaces et aux risques du numérique.

Un modèle efficace de la sécurité dans une grande organisation doit aller vers une approche holistique pour mieux anticiper, détecter, réagir et réparer face à des menaces sophistiquées. Ce modèle doit permettre le partage en temps réel de l'information, le partage du « renseignement », le partage de la connaissance des menaces, et de gérer globalement les crises et les menaces. L'objectif est de se concentrer sur tous les types de menaces pour permettre une réaction rapide et ainsi de créer une sécurité globale de l'entreprise (sureté physique, sécurité des personnes, sécurité de l'information, sécurité de la production, sécurité des produits).
C'est ce que j'appelle un cockpit sureté-sécurité 360° (la sécurité convergée)

Les grandes banques ou les grandes entreprises de défense ont changé radicalement leur organisation en créant une Direction de Sécurité-Sureté Globale (DSG), rattachée directement au PDG : Group Chief Security Officer.

Cette Direction Sécurité Globale couvre les fonctions de : Sécurité physique-contrôle d'accès, Sécurité des personnes en particulier l'habilitation des personnes, Sécurité des fournisseurs tiers, Sécurité de l'information, Gestion du risque numérique, SOC (Security Operation Center), Gestion de crise , Reprise d'activité PRA, Maintien en condition opérationnelle de sécurité, Cyber Design Authority, Sécurité de la production, Sécurité des produits, Intelligence Economique IE et CTI, et la fonction DPO (responsable de la protection des données) doit être fonctionnellement partagée avec la direction juridique.

La DSI avec le (la) RSSI doit garder la fonction traditionnelle de Protéger et organiser la fonction Réparer. Les fonctions : Identifier, Détecter, Répondre, doivent être transférées (et souvent créées) dans la Direction de la Sécurité Générale (DSG). Cela permet une mutualisation d'expertises rares au sein de l'entreprise. Et surtout de bien séparer les responsabilités d'exploitant et de contrôleur. La séparation organisationnelle de ces responsabilités est fondamentale pour assurer une bonne gouvernance de la sécurité-sureté (ce qui est le cas dans le nucléaire, le transport aérien...). C'est au PDG d'arbitrer entre la DSI et la DSG : arbitrage sur les budgets et les investissements dans la sécurité, décision d'arrêter un système pour bloquer la propagation d'un MALWARE. Le PDG et le COMEX doivent être informés très régulièrement de la situation opérationnelle de la sécurité-sureté globale de l'entreprise.

En conclusion, les investissements dans la cyberdéfense ne doivent pas être considérés comme un passif, mais plutôt comme un actif de l'entreprise.

Parution le 7 mai 2021

[1] The Hidden Costs of Cybercrime (mcafee.com)
[2] Cybercoercition : un nouveau défi stratégique : Le Monde Publié le 28 janvier 2020, Face aux cyberattaques, la France doit se doter d'une capacité de dissuasion autonome, écrivent Bernard Barbier, (ex-DT de la DGSE), Edouard Guillaud (ex-CEMA) et Jean-Louis Gergorin (ex-Quai d'Orsay)
[3] L'Estonie, première cybervictime de Moscou (lemonde.fr)

Au-delà de la cybersécurité, des défis civilisationnels

PROFESSEUR SOLANGE GHERNAOUTI
Université de Lausanne
Directrice, Swiss Cybersecurity Advisory & Research Group
Auteure du livre «Cybersécurité, maitriser les risques, mettre en œuvre les solutions ». Dunod, 2019

Pour un écosystème numérique écoresponsable

L'écosystème numérique et ses principaux acteurs sont sortis renforcés de la crise sanitaire. Le solutionnisme technologique continue de séduire certains dirigeants et consommateurs.

La société s'organise et poursuit son développement au travers du numérique, sans pour autant questionner les nouvelles dépendances sociotechniques et vulnérabilités qu'il engendre. Les coûts écologiques et humains, les capacités de déstabilisation sociale, économique et politique du numérique sont encore insuffisamment pris en compte. De plus, peu de considération est accordé aux risques sanitaires et environnementaux liés à l'extraction polluante des terres rares, à leur traitement (séparation, raffinage, transformation), au coût du transport liés à leur exportation (matériel brut) pour leurs transformation, réexportation, importation en produits finis vers des pays consommateurs.

Si les efforts déployés pour rendre le numérique plus durable, plus éthique, plus solidaire, sont à saluer, ils ne permettent toujours pas de répondre aux objectifs de développement durable de l'ONU (Agenda 2030)[1] et à l'urgence climatique et environnementale, qui sont désormais indissociables de l'urgence numérique. Si le numérique peut faire partie des solutions pour le climat, il est également générateur de

gaz à effet de serre, destructeur et consommateur de ressources naturelles et énergétiques. À la croisée des contradictions culturelles, environnementales et économiques, il est un catalyseur d'injonctions contradictoires : accélérer et ralentir la croissance numérique ; consommer plus d'électronique et avoir plus de normes pro-environnement ; disposer de plus de connexion, plus de débit et réaliser une décroissance et désintoxication numériques.

De nouveaux risques, de nouveaux besoins

La *plateformatisation* du monde, inscrite dans la pensée techno-économique dominante développée par les GAFAM et déclinée à l'infini, est un obstacle à envisager d'autres futurs numériques, à penser autrement le numérique, à réorienter les choix stratégiques et l'allocation des ressources.

Est-ce que les choix numériques sont réalisés dans une vision holistique, qui intègre les besoins du court et du long terme et tient compte du risque de pénurie des ressources naturelles et de leur finitude ? Sont-ils compatibles avec la protection de l'environnement et de la biodiversité ?

Persévérer à développer le numérique, c'est rendre la société plus dépendante et plus fragile. Au pire, le pays n'aura plus besoin d'adversaire, il pourra s'effondrer de lui-même. Au mieux, les générations futures se poseront des questions similaires à celles que nous nous posons aujourd'hui pour sortir du nucléaire, à savoir, comment sortir du numérique ?

Le rouleau compresseur de la 5G, du *big data*, de l'intelligence artificielle et des objets connectés ignore les préoccupations et résistances d'un pan important de la société civile qui s'interroge sur leurs finalités, capacités de surveillance et sur leurs impacts sur l'environnement et le vivant. Une guerre idéologique entre les « pour » et les « contre » du « tout numérique » se développe. Elle exclut la possibilité d'une voie médiane, celle d'un numérisme raisonnable.

La pandémie offre une occasion exceptionnelle pour appréhender les risques complexes d'aujourd'hui et de demain de manière systémique, pour stratégiquement, tactiquement et opérationnellement prévenir des crises majeures dont la survenue répétitive est catastrophique.

Plus que des cyberattaques

Les technologies numériques font partie des secteurs industriels qui contribuent à épuiser les ressources naturelles (fabrication et utilisation) et à polluer la planète (surconsommation, obsolescence programmée, extraction des terres rares, déchets toxiques...). En 2020, la masse mondiale de déchets d'équipements électriques et électroniques est estimée à 50 millions de tonnes, dont seuls 20% seraient collectés et recyclés[2].

La consommation électrique croît avec la numérisation des activités, le nombre de systèmes, le transfert et stockage de données ainsi qu'avec les usages. L'informatisation de la société constitue un puissant accélérateur du changement climatique.

Il a été démontré que la consommation d'énergie fossile par le numérique a dépassé celle du trafic aérien[3] ces dernières années.

Les risques et les crises environnementales et écologiques constituent depuis plusieurs années et selon les diverses éditions du *Global Risk Report* du World Economic Forum[4], des problèmes majeurs auxquels doit faire face le monde hyperconnecté et dépendant de l'informatique.

Désormais, les cyberattaques sur les infrastructures énergétiques et industrielles dont l'activité est liée aux ressources naturelles (par exemple les usines chimiques, les structures de traitement des eaux, les plateformes d'exploitation pétrolière, les centrales nucléaires, etc.) sont également des facteurs de risques aggravants pour l'environnement. Du fait de la dépendance de ces infrastructures à l'informatique et de la réalité des menaces, la cybersécurité est aussi à considérer comme une urgence planétaire internationale.

Des exigences de cohérence

Certains acteurs s'engagent dans des mesures de réduction de la consommation électrique des infrastructures. Bien que positif, il ne faut pas sous-estimer le potentiel effet de bord induit par des pratiques numériques plus importantes du fait qu'elles seraient moins énergivores et moins culpabilisantes. Pour réduire les impacts écologiques du numérique, ce sont tous les acteurs – tant locaux que globaux – qui doivent être mobilisés. Dans ce domaine comme dans d'autres, il n'est pas certain que l'autorégulation des fournisseurs et le volontarisme des utilisateurs constituent des leviers de changement suffisants.

Les modèles économiques du numérique sont basés sur des usages permanents, une connectivité totale, une production de contenus surabondante et un trafic de données gigantesque. La conception des produits est majoritairement optimisée pour les rendre addictifs et les pratiques de marketing contribuent à maximiser la consommation numérique.

Une volonté politique forte et des dirigeant-e-s courageux-ses, pourraient contribuer à spécifier et à faire respecter des mesures stratégiques et opérationnelles compatibles avec la préservation de l'environnement. Cela augmenterait la cohérence et l'efficacité des actions parfois menées, mais souvent de manière isolée et fragmentaire. Cela permettrait aussi de dépasser les approches opportunistes relevant du lessivage vert (*green washing*) ou de la séduction, pour faire émerger des solutions convaincantes tant au niveau de la recherche, que de l'innovation et de l'industrialisation.

Ainsi par exemple pour ne citer que trois questions :

- Comment sont pris en compte les impacts du numérique sur l'environnement et sur la santé des citoyens dans le contexte de la multiplication et du déploiement de nouvelles infrastructures informatiques et de télécommunication (5G et générations suivantes)?
- Quelles sont les mesures concrètes relatives au traitement et recyclage des déchets numériques, au développement d'une économie circulaire, plus locale des produits et déchets informatiques, dont le nombre est amplifié par leur obsolescence programmée ?

- Comment est satisfait le besoin de sensibiliser, d'éduquer et d'entrainer à ses problématiques ?

Initialiser un cercle vertueux d'une économie numérique écoresponsable et compatible avec l'humain permettrait peut-être, de dépasser la difficulté ontologique à penser l'écosystème numérique véritablement au service du vivant. Un changement de paradigme doit s'opérer pour que les externalités écologiques du numérique soient prises en compte et que les avancées des sciences et techniques ne deviennent pas un vecteur de destruction. Au-delà de l'obsolescence programmée des systèmes informatiques, c'est celle de l'humain dont il question avec la fuite en avant technologique.

Si d'un point de vue écologique, l'augmentation du numérique n'est pas soutenable, celle de la chosification de l'humain par le numérique, celle de la substitution de l'humain par des robots et des programmes informatiques, le sont encore moins.

Perspectives

Si la planète est dans un état d'urgence, c'est que nous autres humains, le sommes aussi, y compris du fait du numérique. Repensons notre relation à la nature, arrêtons nos comportements prédateurs, donnons de l'importance à notre état de nature, vivons en harmonie avec la nature et arrêtons de la détruire par nos activités. Simuler la nature par des programmes informatiques ne remplace pas les espèces disparues ni la biodiversité à jamais perdue. La vie numérique n'est pas la vie biologique.

Lutter contre le réchauffement climatique et l'érosion de la biodiversité c'est contribuer à défendre nos libertés. Lorsque la « maison commune » brûle, la liberté de vivre dans un environnement sain n'existe plus, comme en témoignent désormais les rescapés des feux australiens contrairement au milliard d'animaux morts.

L'introduction du discours sur le colonialisme de l'écrivain et homme politique martiniquais Aimé Césaire en 1950, rappelle que « Une civilisation qui s'avère incapable de résoudre les problèmes que suscite

son fonctionnement est une civilisation décadente. Une civilisation qui choisit de fermer les yeux à ses problèmes les plus cruciaux est une civilisation atteinte. Une civilisation qui ruse avec ses principes est une civilisation moribonde »[5].

Parution le 14 mai 2021

[1] https://www.un.org/sustainabledevelopment/fr/objectifs-de-developpement-durable/
[2] C. P. Baldé, V. Forti, V. Gray, R. Kuehr, P. Stegmann: Suivi des déchets d'équipements électriques et électroniques à l'échelle mondiale 2017, Université des Nations Unies (UNU), Union internationale des télécommunications (UIT) & Association internationale des déchets solides (ISWA), Bonn/Genève/Vienne.
https://www.itu.int/en/ITU-D/Climate-Change/Documents/GEM%202017/GEM2017_Executive%20Summary_F.PDF
[3] https://theshiftproject.org/wp-content/uploads/2018/11/Rapport-final-v8-WEB.pdf
[4] http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[5] Introduction du discours sur le colonialisme d'Aimé Césaire, 1950.
https://www.larevuedesressources.org/IMG/pdf/CESAIRE.pdf
https://histoirecoloniale.net/Aime-Cesaire-Discours-sur-le-colonialisme

La Cyberdéfense dans l'armée de Terre

GÉNÉRAL D'ARMÉE THIERRY BURKHARD
Chef d'état-major de l'armée de Terre

Il y a moins de 30 ans, nos armées faisaient essentiellement la guerre sur terre, en mer ou dans les airs. Aujourd'hui, nous faisons de plus en plus la guerre dans les champs immatériels : champs informationnels, champs électromagnétiques, cyberespace. Posséder la supériorité dans ces champs interconnectés peut signifier posséder la supériorité tout court. En paralysant des systèmes d'armes ou en contrôlant des opinions, il est possible de faire plier un adversaire, en tout cas de le mettre en position d'infériorité.

Au cours de l'été 2019, dans le cadre d'un concours sponsorisé par le Pentagone, un groupe de hackers a créé l'événement en parvenant à « prendre le contrôle » d'un avion de chasse F-15 en moins de 48 heures. En introduisant un logiciel malveillant dans le système de commande de l'appareil, ces « pirates autorisés » ont réussi à empêcher le vol normal de l'avion, à capter les informations que recevait le pilote et à modifier la perception qu'il avait de son environnement.

Dans une autre mesure, les comptes Facebook, Twitter et TikTok de l'armée de Terre ont subi récemment plusieurs attaques dont deux sont assez emblématiques. Des groupes djihadistes sont parvenus à saturer nos réseaux sociaux de commentaires appelant à l'attaque d'Occidentaux. Plusieurs centaines de messages par minute ont été publiés durant plusieurs heures. Une autre attaque est aussi attribuable à des groupes birmans anti junte. Des milliers de commentaires ont été postés sur le compte TikTok de l'armée de Terre pour relayer leurs messages de lutte contre la répression.

Comment l'armée de Terre doit-elle se préparer à cette guerre dans les champs immatériels ?
La réponse peut paraître simple mais il s'agit de la même démarche intellectuelle que celle que nos armées ont dû conduire à travers toute leur

histoire lorsqu'elles ont été confrontées à de nouvelles menaces et à de nouvelles armes.

Nous devons définir aussi précisément que possible nos propres vulnérabilités tout en sachant saisir les opportunités offertes par les nouvelles technologies.

Notre environnement voit tout d'abord l'affirmation d'une nouvelle forme de conflictualité. Les tendances de fond, identifiées depuis plusieurs années, ne font que s'accentuer. Nous observons le retour des rapports de force comme mode de règlement des conflits. La guerre entre l'Azerbaïdjan et l'Arménie aura fait 10 500 morts en 44 jours en octobre 2020 mais la crise sanitaire que nous traversons aura écarté notre attention de ce conflit et de ces chiffres terribles.

L'élévation du niveau technologique de nos compétiteurs est également un égalisateur de puissance. L'Iran est aujourd'hui capable de réaliser des frappes de précision à longue distance comme il l'a montré avec l'attaque de la base américaine d'Al-Assad et à Erbil en janvier 2020 en Irak. Il est aussi capable de réaliser des attaques cyber relativement complexes, comme il semble l'avoir fait contre Israël au printemps dernier.

Enfin, dans un monde de compétition permanente, nous observons un emploi plus insidieux de la force, juste sous le seuil du conflit armé : action cyber, désinformation, harcèlement, etc. Les champs immatériels deviennent un espace de friction systématique, ce qui constitue, à mon sens, la rupture la plus importante dans la conflictualité moderne.
Quelles menaces les champs immatériels représentent-ils pour l'armée de Terre ?

Il existe tout d'abord une menace technologique sur nos systèmes d'armes. Entrées dans l'ère du « combat collaboratif », nos unités sont de plus en plus interconnectées. Elles échangent des informations d'un véhicule à l'autre : positions, comptes rendus d'observation, etc. Toutefois, à la différence d'un avion ou d'un navire, une force terrestre est très décentralisée et constitue un système « ouvert », qui est plus vulnérable du fait de ses multiples points d'entrée. De façon générale, la numérisation de nos systèmes d'armes accroît

notre efficacité mais aussi notre exposition à la menace cyber.

Il existe ensuite une menace sur la sécurité de nos informations. Aujourd'hui, chaque véhicule détient en propre un nombre considérable d'informations. En pénétrant les systèmes d'information de nos unités, de nos états-majors ou de nos industriels, un adversaire peut apprendre énormément sur nos intentions ou de nos capacités.

Il y a aussi une menace sur la crédibilité de nos opérations. Au Sahel, nous faisons aujourd'hui face à des campagnes de désinformation orchestrées qui pourraient gravement compromettre la confiance que nous accordent la population et les gouvernements de la région.

Enfin, n'oublions pas que l'armée de Terre est en premier lieu un système d'hommes. La dernière menace est donc sur l'humain. Il y a 30 ans, en opération, nos soldats pouvaient passer plusieurs semaines sans donner de nouvelles et sans en recevoir. Dans nos casernes, on faisait la queue devant les cabines téléphoniques…
Aujourd'hui, quasiment tous nos soldats sont connectés grâce à leur montre ou leur smartphone. Cette hyper connexion peut conduire à un ciblage de nos soldats et ouvre la porte de la guerre informationnelle.
En 2018, la position de bases secrètes américaines était révélée sur internet grâce à l'application mobile de sport Strava, un réseau social de sportifs. Identifier un lieu de vie dans une base militaire et conduire une frappe cinétique ou informationnelle se trouvent désormais à la portée de tout ennemi même sans moyens et observation spatiale.
Avec la crise COVID, nous avons échappé à des campagnes de désinformation sur les réseaux sociaux à destination de nos soldats et des familles. Mais cela arrivera. Nos chefs, nos soldats et leurs familles doivent y être préparés.

Dans ce contexte, l'ambition de l'armée de Terre et les défis qu'elle doit relever sont assez clairs.

L'objectif est de ne pas subir les champs informationnels mais de nous y engager résolument et à tous les niveaux. Ne nous arrêtons pas seulement aux vulnérabilités, mais identifions aussi les opportunités que nous devons saisir. Nous devons durcir notre résistance à l'action de nos adversaires dans

les champs immatériels. Nous devons avoir la volonté de ne pas leur laisser la libre possession des champs immatériels. Nous devons être déterminés à y combattre à notre tour.

Nous avons donc trois grands défis à relever dont le premier est la bonne compréhension des enjeux.

Il y d'abord un impératif d'acculturation de nos états-majors et de nos soldats.

Historiquement et culturellement, nous sommes plutôt tournés vers l'action directe, cinétique. Nous devons évoluer dans notre approche opérationnelle et penser plus systématiquement aux champs immatériels, depuis le niveau de la section jusqu'à celui du corps d'armée. Quand nous penserons « manœuvre dans les perceptions », nous serons mieux préparés pour contrer les manœuvres adverses dans ce domaine.

Il ne faut surtout pas réduire les champs immatériels, et notamment le cyberespace, à une affaire de techniciens. Le cyberespace doit être envisagé comme l'espace terrestre. Nous manœuvrons dans le cyberespace, comme nous manœuvrons sur un champ de bataille : il faut se renseigner, se défendre, attaquer, etc.

Nous devons également recruter et former notre ressource sur un segment qui est devenu très concurrentiel. Nos entreprises sont effectivement très intéressées par les compétences de nos spécialistes qu'il nous faut toutefois fidéliser plusieurs années pour rentabiliser leur formation et surtout parce que nous en avons besoin.

Le deuxième défi à relever est celui de la résilience de nos systèmes et de nos organisations.

Continuer à structurer notre chaîne de cybersécurité pour protéger nos forces et notre industrie est un effort à poursuivre. En opération, nous déployons des détachements chargés de la protection numérique de nos unités. En métropole, nous montons aussi en puissance un centre de supervision des systèmes d'information métier de l'armée de Terre.

Mais il faut surtout penser notre sécurité des systèmes d'information (SSI) autrement. Nous ne pouvons plus construire des systèmes comme si rien ne pouvait y pénétrer. Un adversaire déterminé entrera toujours. Développer des systèmes résilients, capables de se reconfigurer est devenu un impératif. Penser la SSI comme une ligne Maginot est une vision dépassée et dangereuse.

Mais une fois de plus, n'oublions pas les hommes. Pour entraîner nos unités, il nous faut reproduire dans nos camps un environnement « cyber contesté » pour entraîner nos soldats.

Inversement, nous devons aussi nous entraîner à faire face « quand tout plante » : c'est ce que l'on appelle le mode dégradé. Même si nous utilisons des cartes numériques dans nos postes de commandement, nous continuons à mettre à jour nos cartes papier et nos cours de topographie commencent par l'apprentissage de la boussole avant celui du GPS.
Nos hommes doivent aussi être sensibilisés par leurs chefs aux informations qu'ils trouveront sur Internet. Un soldat bien entraîné, demain, sera celui qui sera capable de rendre compte s'il détecte ce qui lui semble être une campagne de désinformation sur Internet.

Le troisième défi consiste à savoir et à pouvoir manœuvrer dans les champs informationnels.

Il faut bien sûr être capable de conduire des attaques cyber au niveau stratégique, depuis la métropole. Nous devons aussi être en mesure de conduire ce type d'attaques depuis nos théâtres d'opération : c'est le niveau tactique. Nous devons déployer des capacités et les utiliser. Ce même effort doit être réalisé pour le brouillage. Ces capacités existent mais doivent être renforcées.

Notre capacité de guerre informationnelle doit, elle-aussi, être développée. Pour dissuader et décourager nos compétiteurs, nous devons être crédibles en affichant nos capacités militaires. Il nous faut savoir détecter, caractériser et contrer les attaques informationnelles dont nous sommes la cible.

Nous devons intensifier notre communication stratégique sur notre posture, par exemple autour de nos grands exercices militaires et notamment avec ceux réalisés avec nos alliés. C'est ce que nous faisons avec l'opération LYNX dans les pays baltes. Le chargement de nos chars Leclerc dans nos bateaux de transport fait l'objet d'une manœuvre informationnelle planifiée en amont. Cela nécessite une grande anticipation pour avoir une parfaite cohérence de discours avec nos alliés.

Si nous n'acceptons pas de combattre dans les champs informationnels, d'autre le feront… contre nous. Nous nous y préparons et cela fait partie des axes d'effort de la vision stratégique que j'ai lancée il y a un an.

Parution le 21 mai 2021

La Stratégie Nationale pour la Cybersécurité

WILLIAM LECAT
Coordinateur Stratégie Nationale Cybersécurité
Secrétariat Général pour l'Investissement

Annoncée le 18 février par le Président de la République et financée dans cadre du plan France Relance et du 4e Programme d'investissements d'avenir, la Stratégie Nationale pour la Cybersécurité marque un tournant important du domaine. Les objectifs affichés, simples et concrets, sont très ambitieux. Les moyens conséquents mis en œuvre par les pouvoirs publics et le secteur privé pour les atteindre sont historiques. Pour la première fois en cybersécurité, des financements de taille sont débloqués pour le court, le moyen et le long termes avec des ambitions sociétales, économiques et technologiques à la hauteur des grands challenges que portent ces innovations technologiques plus que jamais nécessaires dans un monde ouvert et potentiellement vulnérable à des attaques cyber dont le nombre et la violence ne cesse de croître. Si le Grand Défi cybersécurité, lancé fin 2019, montrait déjà une volonté politique forte de prendre le sujet à bras le corps, cette Stratégie Nationale aux budgets allant deux ordres de magnitude plus loin ne laisse aucun doute sur la place prioritaire que le Gouvernement donne à la cybersécurité.

La cybersécurité est un secteur dont la croissance est structurellement liée à celle de la numérisation. Une numérisation croissante implique donc une importance grandissante de la cybersécurité. Si cet aspect semble évident, la prise de conscience et sa concrétisation impliquent souvent une étape supplémentaire : l'augmentation du nombre d'attaques et de leurs impacts. La pandémie mondiale que nous vivons depuis plus d'un an, épreuve inédite pour nos contemporains, a accéléré la numérisation de nos sociétés et de nos organisations exacerbant ainsi le niveau de maturité,

probablement déjà insuffisant, en cybersécurité. Il est par ailleurs probable que la recrudescence des attaques lors de cette période corresponde seulement aux prémices de ce qui est à venir. Le parti pris d'accélérer fortement sur la cybersécurité est donc particulièrement nécessaire. C'est pourquoi l'Agence nationale de la sécurité des systèmes d'information (ANSSI) bénéficie d'un budget directement issu du plan France Relance pour sécuriser le socle numérique de l'Etat et des territoires. Ces 136 M€ visent un impact à court terme en finançant des états des lieux, des plans d'actions, des aides au déploiement et de l'achat d'équipements de sécurité déjà disponibles. Il s'agit d'un financement qui vient se rajouter aux différents budgets des bénéficiaires pour leur permettre d'accélérer leur sécurisation. L'objectif à moyen terme est également d'ancrer les bonnes pratiques dans les habitudes des usagers et des organisations que ce soient des entreprises ou des collectivités territoriales.

Mais l'ambition de la France n'est pas seulement de se « cybersécuriser » rapidement. Il s'agit également de maitriser cette sécurisation, d'en être non seulement le consommateur mais également un fournisseur. Le besoin et la demande sont en forte croissance. Ce phénomène ayant vocation à s'amplifier et la Nature ayant communément horreur du vide, il est indispensable que les industriels français puissent se positionner rapidement et prennent une place de leader sur ce secteur prometteur. Cela passera naturellement par un effort marketing et commercial de leur part mais aussi par un investissement technologique majeur pour faire de l'innovation la source de notre compétitivité. C'est là que la nécessité de rapprocher la recherche et l'industrie devient essentielle. Sur le moyen et long termes, la pérennité de l'économie de la filière cyber passera par l'innovation qui ne peut être alimentée que par une cohérence profonde entre les différents niveaux de maturité de la recherche fondamentale à la recherche industrielle et ses applications pour répondre aux besoins d'aujourd'hui et de demain. Le 4e Programme d'investissements d'avenir (PIA4) nous permet de bénéficier de 360 M€ de financements publics pour soutenir tous les maillons de cette chaine de recherche et développement. Ce budget se décompose en 65 M€ pour la recherche fondamentale, 275 M€ pour les transferts technologiques et la R&D industrielle et 20 M€ pour des démonstrateurs territoriaux. L'objectif économique pour 2025 est d'atteindre les 25

milliards d'euros de chiffre d'affaires de la filière française, soit une multiplication par 3,5. Un objectif ambitieux mais à la hauteur du potentiel de la filière et réalisable grâce à la mobilisation de toutes les parties prenantes.

La demande est donc conséquente et en constante évolution. Malgré une très forte volonté de positionner l'écosystème français pour y répondre, ce secteur en très forte croissance se heurte à un frein majeur : le manque de personnes qualifiées. En réalité, le nombre d'experts cyber est important et croît rapidement, mais moins vite que la demande pour ces profils. La capacité de formation augmente également vite mais l'attractivité du secteur reste encore limitée pour le moment, rendant difficile de remplir toutes les formations. Il semblerait que le domaine et les métiers cyber pâtissent encore d'une image peu attractive incluant toutes formes de capuches et autres vies recluses dans des garages. Ce stéréotype est bien loin de la vérité. Il s'agit en fait de métiers aux compétences (techniques mais pas uniquement) de pointe avec des salaires au-dessus de la moyenne tous domaines confondus et surtout bénéficiant d'un dynamisme économique et technologique extrêmement important ce qui promet des perspectives variées et passionnantes. En résumé, des métiers d'avenir. Il est donc indispensable de penser et de mettre en œuvre une sensibilisation tournée vers l'attractivité de la filière. Un observatoire des besoins en compétences cyber devra permettre de quantifier et d'orienter précisément les efforts en formations. De forts besoins pour des formations « courtes » ont déjà été identifiés, l'essentiel des formations actuelles étant centré sur les niveaux bac+5 et bac+8. Il est aussi important de mettre l'accent sur la formation continue et les capacités de reconversion. La diversification de l'offre de formation en cohérence avec les besoins observés et anticipés, couplée à une sensibilisation à différents niveaux pour attirer et créer des vocations seront indissociables de l'atteinte des objectifs de la Stratégie qui vise à porter à 75 000 le nombre d'emplois dans le secteur en 2025.

La sensibilisation large spectre permettant une prise de conscience des enjeux et des dangers et conduisant à l'augmentation du niveau d'éveil cyber global est également très importante et doit être menée en parallèle. Une sensibilisation « grand public » semble particulièrement

nécessaire. La sensibilisation des femmes et hommes, agents du public comme du privé, représentera « la brique de base » pour pouvoir ensuite présenter les solutions envisageables contre les différentes menaces. Les plans de continuité et de reprise d'activité face à la menace cyber sont particulièrement importants pour la résilience de notre société et représenteront un bon indicateur de l'impact organisationnel de la sensibilisation.

De manière générale, la « visibilité » des aspects de cybersécurité est aussi importante pour les différents secteurs utilisateurs que pour l'écosystème cyber lui-même. En effet, ce dernier souffre d'une forte fragmentation qui nuit à son rayonnement. La création d'un lieu « totem », matérialisé par le Campus Cyber, permettant de rapprocher les différents acteurs cyber, de l'industrie, de l'administration et de la recherche tout en intégrant des clients finaux, sera donc un élément clé de la structuration de la cybersécurité française. La déclinaison de cet espace de référence au sein des territoires permettra une consolidation du secteur bénéficiant à tous les objectifs de la Stratégie Nationale. Ce projet, inspiré de plusieurs initiatives dans d'autres pays et de leurs enseignements, est une première mondiale dans son approche et ses objectifs. Le Campus Cyber devrait ouvrir ses portes en novembre 2021 à la Défense en région parisienne.

Dans cet effort de consolidation, un accent particulier sur la stimulation et le soutien à l'entreprenariat sera également mis. En effet, notre capital d'expertises techniques et d'excellences scientifiques devrait nous permettre d'accueillir un nombre croissant de start-up dans les prochaines années. Il conviendra donc de faciliter leur création et d'accélérer leur développement en les accompagnant et en leur permettant d'accéder à des financements via une structure dédiée. Cela pose implicitement la question de notre capacité à financer les « scale-up » et les futures licornes françaises du domaine. Les différents rachats et départs de jeunes pousses prometteuses ne laissent pas d'ambiguïté sur la nécessité croissante d'adresser activement le sujet. Les réflexions entamées indiquent, sans grande surprise, que le bon niveau à terme se situe à l'échelle de l'Europe pour l'émergence de fonds d'investissement adressant cette problématique. Tout d'abord, les financements importants que

permet l'échelon européen et le nombre relativement limité d'opportunités d'investissements de ce niveau laissent à penser que les thèses d'investissement de ce type de fonds devront dépasser les frontières de l'Hexagone. Cela semble d'autant plus vrai que beaucoup de start-up en « hypercroissance » se tournent naturellement (avant tout rachat) vers le marché le plus important du monde dans le domaine, les Etats-Unis. La structuration d'un marché Européen (au sens de l'Union Européenne) offrirait donc le levier de croissance nécessaire pour permettre l'émergence de licornes et de fonds d'investissement pour les financer. Il se trouve en réalité que cet aspect résonne avec tous les objectifs de la Stratégie. La construction cyber en cours au niveau européen, autour du centre de compétence cyber européen et des déclinaisons nationales, représente donc une opportunité d'amplifier les impacts de la Stratégie Nationale Cybersécurité et d'accélérer son déploiement.

Parution le 28 mai 2021

L'usine du futur imposera l'enseignement de la cybersécurité des systèmes industriels

FLORENCE LECROQ
Maître de Conférences en Automatismes
et en Sécurité des Systèmes Informatiques Industriels
IUT du Havre

L'usine du futur : des implications dans l'enseignement

Aujourd'hui, nous sommes à l'heure de « l'industrie du futur ». Cette quatrième révolution industrielle est basée sur les systèmes cyber physiques. Ces systèmes, communiquant massivement grâce aux réseaux informatiques, constituent l'un des principaux piliers de « l'industrie 4.0 ».

Jusqu'au début des années 2000, les réseaux industriels échappaient aux cybermenaces. En effet, déconnectés de la partie bureautique du système d'information, encore appelée IT (Information Technologies), ils ne présentaient aucune vulnérabilité autre que celles propres aux lignes de production, appelées OT (Operational Technologies). L'approche traditionnelle nous présente l'entreprise industrielle sous la forme d'une pyramide (la pyramide CIM), découpée en couches nommées niveaux, où l'on retrouve les différents éléments constitutifs du système de production. Le niveau 0 est à la base, avec les capteurs, les actionneurs et les pré-actionneurs ; au-dessus, se situe le niveau 1, avec la commande, c'est-à-dire les automates programmables industriels ; vient ensuite le niveau 2, la partie supervision, avec la conduite, l'optimisation et la surveillance du système ; le niveau 3 regroupe la gestion de production, avec l'ordonnancement et le suivi de production, contrôle qualité et le suivi des moyens ; le niveau 4, le dernier, abrite le système d'information de l'entreprise, avec la gestion centralisée de l'entreprise.

Avec l'arrivée de l'industrie du futur, la numérisation de l'ensemble des fonctions de l'entreprise engendre une communication verticale entre les différents niveaux de la pyramide, ainsi qu'une communication horizontale et directe avec l'extérieur et ce à tous les niveaux.

L'utilisation des IIOT (Industrial Internet Of Things), ou encore la télémaintenance, augmente la vulnérabilité des systèmes industriels informatisés. En effet, ces points d'entrée, s'ils ne sont pas convenablement protégés, offrent des opportunités d'intrusion qui peuvent remettre en cause la sécurité des systèmes. Ces faiblesses, aux conséquences parfois catastrophiques et irréversibles, doivent être corrigées. Comme l'a défini l'ANSSI : « *La cybersécurité est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ».

Constituant un enjeu majeur pour la protection des systèmes industriels, il paraît donc urgent de former nos étudiants à cette problématique dans le cadre des cours portant sur les technologies de l'industrie du futur, avec les réseaux industriels et la programmation des automates.

La formation : 1er vecteur de sensibilisation aux risques cybers

Eveil – Veille – Sensibilisation – Formation : ces quatre mots sont une représentation de mon métier. En effet, je travaille sur l'industrie du futur en informatique industrielle pour la formation, ainsi que sur la XR reality pour la recherche avec l'utilisation des mondes virtuels pour la formation. La réalité étendue (XR) regroupe les diverses formes de technologies immersives, comme la réalité augmentée (AR), la réalité mixte (MR) ou la réalité virtuelle (VR). Le métier d'enseignant chercheur est de susciter l'intérêt (l'éveil) de nos étudiants sur différents sujets. Nous nous devons de faire une veille technologique pour eux, pour ensuite les sensibiliser à

différents sujets et terminer bien évidemment avec la formation.

Ce principe d'« Eveil-Veille-Sensibilisation-Formation » s'applique parfaitement à la cybersécurité aujourd'hui.

Il n'y a pas une semaine sans qu'on entende parler d'une attaque cyber proche de nous. Comme le rapporte HISCOX [1], assureur spécialiste des cyber-risques, 49% des entreprises françaises ont été la cible d'une cyber attaque en 2020, contre 34% en 2019. 65% ont versé une rançon. Les entreprises françaises sont aussi celles qui ont le moins investies en termes de sécurité des systèmes d'informations. Nos étudiants sont les futurs intervenants dans des entreprises, et notamment celles de la zone industrialo-portuaire du Havre, qui comprend 23 sites Seveso, dont 17 de seuil haut. On peut aisément imaginer les conséquences dramatique d'une attaque cyber d'envergure sur un site de la région. C'est dans ce contexte que nous formons nos étudiants à la cybersécurité des réseaux industriels.

Tout comme lorsque l'on parle de *Safety* dans les métiers de l'automatisme, il s'agit là de protéger l'homme de la machine ; lorsque l'on parle de cybersécurité, il s'agit au contraire de protéger la machine de l'homme. Et les spécialistes s'accordent à dire que 80 % des attaques cybers pourraient être évitées si les personnels étaient formés aux risques cyber.
Cette notion est d'autant plus vraie lorsqu'on connait les conséquences possibles d'une attaque cyber sur un processus industriel.
Il peut bien évidemment y avoir du vol de données, mais surtout le risque d'avoir une destruction de la chaîne de production, avec ses conséquences éventuelles sur l'environnement et la santé humaine. On pourrait énumérer de nombreux exemples d'attaques cyber sur des systèmes industriels, comme BlackEnergy en 2015, qui a privé d'électricité près de 1,5 millions d'Ukrainiens, ou Wannacry en 2017, qui se propage dans 150 pays et touche des sites industriels à travers le monde, ou TRITON en 2017, qui touche le groupe pétrochimique Petro Rabigh en Arabie Saoudite, etc. En 2021, le nombre d'attaques a explosé, ciblant aussi des centres hospitaliers, des laboratoires ou des universités. On peut dire aujourd'hui que personne n'est épargné mais surtout que tout le monde sera touché, ce ne plus qu'une question de temps.

D'où l'importance de la sensibilisation aux risques cyber et surtout de la formation. Car la cybersécurité n'est surtout pas une affaire de spécialistes mais doit être une préoccupation de tous et de tous les jours.

Les outils et les pratiques

Il y a de nombreux outils aujourd'hui pour former les personnels et les étudiants aux risques cyber. Tout d'abord, il existe des aides fournies par l'ANSSI, sur son site [2], avec la SecNumAcadémie, qui donne une formation en ligne avec un MOOC qui rend la cybersécurité accessible à tous. L'ANSSI donne aussi le label SecNumedu pour les formations spécialisées en cybersécurité et le label CyberEdu pour les formations qui sensibilisent, initient voire forment à la cybersécurité sans faire des experts du domaine.

J'ai récemment travaillé avec les sociétés Stormshield et Schneider sur la mise en place d'une platine d'enseignement sur la cybersécurité des réseaux industriels. De par mon métier, je suis amenée à visiter des entreprises et discuter avec les maîtres de stage de mes étudiants. Et souvent, j'ai été confrontée aux fausses croyances de la cybersécurité industrielle : *« le système industriel n'est pas connecté à Internet, je suis protégé », « la communication est en série, je suis protégé », « tout est redondé, je suis protégé », « avec la cybersécurité, je ne pourrai plus travailler correctement »,* etc. C'est à cause de ces réflexions que j'ai participé à ce projet d'une platine pour l'enseignement qui est à destination de tous les centres de formations (universités, écoles d'ingénieurs, IUT). Cette platine explique qu'une application sur un bus industriel (un variateur associé à un moteur géré par un bus CAN dans cet exemple) peut être impactée par une attaque cyber provenant de l'IT. Dans un des exercices, durant l'attaque lancée, le variateur change la consigne de vitesse du moteur toutes les 3 secondes, et ce, pendant 30 secondes. Cet exemple montre qu'avec une mauvaise configuration réseau, ou une mauvaise politique de sécurité mise en place, un attaquant peut prendre le contrôle partiel ou total du réseau industriel.

Plus récemment, avec mon collègue Jean GRIEU, nous avons monté un *serious escape game* pour une sensibilisation et une formation aux risques

cybers. Ce jeu est à destination de nos étudiants mais aussi à destination de tous les personnels, que ce soit de l'université mais aussi des entreprises de la région du Havre qui, je vous le rappelle, comprend 23 sites Seveso, et la cybersécurité est l'affaire de tous. Ce jeu, « la règle des 12 », doit se jouer à 12 joueurs, qui doivent trouver 12 entreprises de la région havraise, qui ont été piratées et infestées par un Botnet, parce que 12 règles de cybersécurité n'ont pas été respectées. Les joueurs ont 60 minutes pour sauver la région havraise d'une catastrophe industrielle en découvrant les douze entreprises infestées, l'entreprise qui héberge le maître du botnet, ainsi que l'identité du hacker qui se cache parmi les employés de l'entreprise qui cache le maître des zombies. Ce jeu est basé sur les douze règles de base de la cybersécurité énoncées par l'ANSSI [3]. L'utilisation du jeu comme vecteur d'enseignement permet de mettre en œuvre des pratiques actives, réflexives et sociales, et permettent de développer le sens du partage et l'intelligence collective. Je pourrais terminer en disant que plus les personnes s'amusent en apprenant, et mieux elles retiennent le message de l'enseignant.

Et surtout ne pas oublier que la cybersécurité est l'affaire de tous et surtout pas que des spécialistes.

Parution le 4 juin 2021

[1] Hiscox Cyber Readiness report 2021 : Près d'1 entreprise française sur 2 ciblée par une cyberattaque en 2020
https://www.hiscox.fr/sites/france/files/documents/CP%20Hiscox%20Cyber%20Readiness%20report%202021_19042021.pdf
[2] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
https://www.ssi.gouv.fr/administration/formations/
[3] ANSSI : Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Une matrice pour anticiper et traiter les risques cyber

GÉRARD PELIKS
Chargé de cours cybersécurité dans les écoles d'ingénieurs et instituts
Membre de l'ARCSI

Dans le cyberespace, l'Information est en grand danger

Le cyberespace est le lieu de tous les dangers. Chaque jour apporte son lot d'attaques qui minent la confiance qu'on peut accorder aux fournisseurs, aux partenaires, et qui est accordée par les clients, et les employés. Le nombre d'attaques explose. Organisations grandes et petites, particuliers, tous sont menacés. Parfois la survie de l'organisation est mise en péril quand elle n'a plus accès à son Information qu'on trouve chiffrée par un cryptovirus en vue de demander une rançon, ou volée par un concurrent qui prend un avantage concurrentiel. Le risque est bien réel, il est omniprésent. Il est indispensable pour une organisation de maîtriser le risque numérique qui pèse sur son Information, pour générer la confiance, et plus pragmatiquement pour continuer à exister. De plus, bien maîtriser le risque peut également générer un avantage compétitif.

Mais comment appréhender le risque qui pèse sur son Information et sur les systèmes qui la gèrent ? S'il est admis que le « risque zéro » ne sera jamais atteint, il est aussi évident qu'on ne peut tout protéger. Par quoi commencer pour gérer cette situation ?

Cartographier les risques

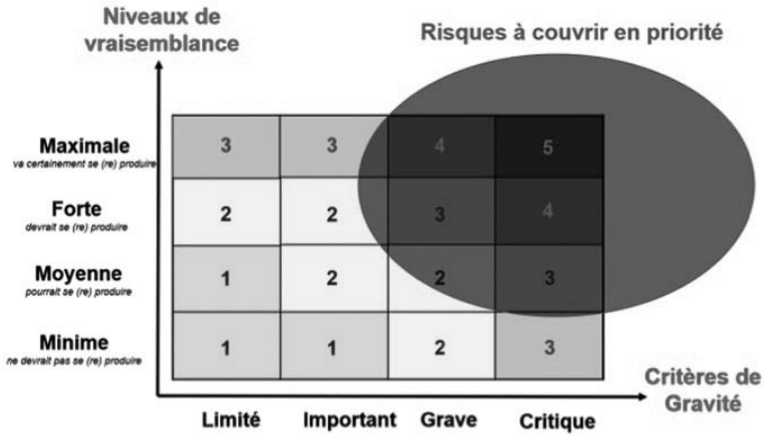
Commencer par cartographier ses ressources numériques pour déterminer où se trouvent les gisements d'informations les plus sensibles est une bonne pratique. C'est là où se trouvent les informations de valeur qu'il faut placer les contre-mesures dont on dispose pour les protéger, et là seulement car on

ne peut tout protéger. Savoir où se trouve son information est d'autant plus indispensable que de plus en plus souvent l'Information ne se trouve plus dans l'entreprise mais est confiée à un Cloud public, privé ou hybride. Il est indispensable d'élaborer dès le départ un cadre de gouvernance du risque numérique, pour ne pas se trouver fort dépourvu quand un problème est venu.

Savoir comment réagir à une cyberattaque devient bien plus facile quand on a prévu à l'avance la conduite à tenir pour en diminuer les effets ou pour la rendre moins probable. Plus que le produit « gravité des conséquences, vraisemblance que le risque arrive », pour connaître la criticité du risque, il est d'avantage intuitif de constituer une matrice des risques et un fichier des actions associées. Cette matrice de hiérarchisation des risques cyber est très utile si elle est constituée avant qu'il ne soit trop tard. Prenons conscience que, comme le dit un dicton, « les tuiles qui protègent de la pluie doivent toutes avoir été posées par beau temps ».
Pour constituer la matrice, dite diagramme de Farmer, traçons sur un axe horizontal, la criticité du risque, suivant, par exemple, quatre critères : risque limité, risque important, risque grave et risque critique. Un risque est limité s'il n'entraine pas de conséquences insupportables quand l'attaque se produit. Un risque est important s'il gène le travail mais sans l'arrêter, ou si les clients s'en aperçoivent mais peuvent à la limite l'admettre. Un risque est grave si le travail est fortement perturbé et si les clients et la presse commencent à se poser des questions sur le sérieux et la compétence de l'organisation qui subit l'attaque. Un risque est critique s'il peut causer la disparition de l'organisation.

Il est bien évident que si un risque est critique mais ce qui peut le causer n'arrive (n'arrivera ?) jamais, on peut, peut-être, l'ignorer. Il est aussi évident que si un risque est limité, mais les attaques qu'il prévoit deviennent assez gênantes quand elles se produisent trop souvent, il vaut mieux en tenir compte dans la mesure du possible, si d'autres priorités n'impliquent pas de reporter l'action à plus tard. Mais la priorité reste de traiter en priorité les risques qui entrainent les conséquences les plus graves. En un mot il faut tenir compte d'un seuil d'acceptation des risques et avoir pensé à l'avance ce qui peut être fait pour en diminuer les effets.
Alors traçons sur un axe vertical le niveau de vraisemblance qu'un risque se concrétisera par une attaque. Prenons encore, par exemple quatre critères :

Vraisemblance minime, vraisemblance moyenne, vraisemblance forte et vraisemblance maximale. Une vraisemblance minime indique qu'une attaque a très peu de malchance d'arriver. Une vraisemblance moyenne indique que la concrétisation de la menace par une attaque pourrait bien se produire. Une vraisemblance forte indique que l'attaque devrait se produire. Enfin, une vraisemblance maximale implique que non seulement l'attaque va certainement se produire mais aussi se reproduire.
En fonction de ces quatre critères de gravité et de ces quatre critères de vraisemblance, on peut bâtir un tableau dit « matrice de criticité » où, dans chaque cellule, on inscrit une quantification des risques, de 1 à 5.



Dans les cases 1, le risque est mineur, et n'impacte ni les clients, ni le travail, ni l'information, on peut donc placer les contre-mesures ailleurs, on admet le risque sans le traiter. Dans les cases 2, le risque est faible, les perturbations subites resteront acceptables, on peut ne pas le traiter, au moins dans l'immédiat. Cases 3, le risque est moyen, il a une incidence gênante, il faut le traiter. Cases 4, le risque est fort, il faut traiter la concrétisation de ce risque le plus rapidement possible. Dans la Case 5, en haut à droite, le risque est critique, l'incidence est majeure, il faut pouvoir le traiter immédiatement sinon il y a possibilité de disparition de l'organisation.
Dans un autre document, on décide de la conduite à tenir pour chaque case et qu'il faut impliquer pour le traiter. La conduite va de (cases 1) « on accepte,

on ne passe pas de temps dessus » à (cases 5) « on traite le problème immédiatement, toutes affaires cessantes » C'est à partir des cases 3 qu'il faut placer des contre-mesures et prendre les décisions qui s'imposent quand l'attaque se produit. Il est bon également de quantifier les effets des risques, par exemple décider dans quelle case on met tel problème quand il entraine telle perte financière, tels jours de retard ou tel nombre de clients lésés, blessés ou simplement perdus.

Il faut également tenir compte, pour chacune des cinq quantifications, de la dimension « métier ». On ne traite pas le risque de la même manière chez un constructeur aéronautique que dans une banque, une société d'assurance, de transports, un établissement de santé ou un média. Une matrice des risques ne peut se justifier qu'au niveau d'une entreprise ou d'un service, mais n'est en aucun cas une matrice théorique unique qui sert de modèle dans tous les cas.

Il faut aussi décider à l'avance si les conséquences de chaque risque sont à traiter au plus haut niveau de l'organisation ou seulement au niveau des experts techniques ou juridiques, ou ne sont pas à traiter du tout. De plus, les menaces évoluent, donc les risques aussi. Ces travaux doivent être mis à jour au moins sur une base annuelle.

Deux exemples

Prenons comme premier exemple les risques qui pèsent sur l'information d'un journal ou d'une chaîne de télévision, et analysons les dangers qu'une cyberattaque fait peser sur son image. Sur le fichier associé à la matrice des risques, le risque des cases 1 n'implique pas de médiatisation, le média peut l'accepter. Le risque des cases 2 entraine un risque modéré (faible tirage d'une presse locale, très peu d'impacts dans les réseaux sociaux…) on peut aussi l'accepter. Le risque des cases 3 implique une médiatisation limitée mais les risques des cases 4, et surtout ceux de la case 5, causent une dégradation durable de l'image du média, la presse internationale reprend l'information corrompue ou dévoilée et l'atteinte à la réputation du média peut entrainer sa disparition, faute de lecteurs, en plus des sanctions.
Comme autre exemple, prenons les menaces sur l'Information d'une société de transport.

Dans les cases 1, il n'y a pas d'impact visible sur la disponibilité ou l'intégrité du système d'Information, l'attaque n'est pas visible et n'entraîne rien de sérieux, on l'ignore, ou en tout cas on peut-on tenir compte plus tard. Dans les cases 2, l'activité est un peu désorganisée et des clients sont assez mécontents, le risque est à considérer, mais on peut le traiter dans un deuxième temps. Dans les cases 3 et dans certaines cases 4, la désorganisation est importante et les usagers sont forts mécontents. Il faut agir. Dans certaines cases 4, et en tout cas dans la case 5, le service est arrêté, il y a peut-être eu un terrible accident avec des victimes. Il faut le traiter immédiatement et il est nécessaire de déclencher une cellule de crise.

On peut aussi établir de telles matrices sur les atteintes à chacune des facettes de son Information : sa disponibilité, son intégrité, sa confidentialité et sa traçabilité, et ce pour tous les process qui manipulent cette information. Plus la quantification du risque est modulaire, plus elle peut être efficace.
Avec cette matrice, et le fichier des conduites à tenir, complexes à établir certes pour une grosse organisation mais fort utiles, on sait à quoi s'en tenir, on connait les actions à mener, à quel niveau, immédiatement ou en différé, et s'il est indispensable de réunir une cellule de crise, mettre en œuvre son plan de continuité ou de reprise d'activité. Il faut disposer de ces plans, et activer sa police d'assurance si le risque numérique, direct et indirect, est en partie couvert. Et tout cela augmentera la résilience, donc la compétitivité de son organisation.
Mettre au point cette matrice et le fichier associé dans lequel sont détaillées les actions qui s'imposent est un travail d'experts, qui doit réunir techniciens, juristes, service du personnel et être validé par la direction.

La cybersécurité doit devenir la norme, et la classification des risques est le premier outil pour diminuer la gravité des impacts d'une attaque, et diminuer également la probabilité que cette attaque se produise. Et la sensibilisation de tous aux dangers du cyberespace est la deuxième priorité.

Parution le 11 juin 2021

Cybersécurité : les perspectives pour le secteur public en 2021

CHRISTOPHE AUBERGER
Evangéliste Cybersécurité Fortinet France

Le secteur public est aujourd'hui, comme le secteur privé, de plus en plus confronté aux risques numériques, et ce d'autant plus après la crise liée à la COVID-19.

Le recours forcé au télétravail dès mars 2020 a en effet bouleversé la façon dont les services administratifs sont fournis. Auparavant, les fonctionnaires assuraient la prestation de services aux citoyens en personne. En 2021, ils sont encore nombreux à travailler à distance et à fournir une assistance numérique aux citoyens. Par ailleurs, l'utilisation d'outils tels que les chatbots, les agents intelligents et le RPA (Robotic Process Automation, à savoir l'automatisation de processus métier basée sur des règles) est de plus en plus courante. Cela élargit considérablement la surface d'attaque. De plus, le domicile des télétravailleurs ne dispose pas du même niveau de sécurité que les environnements professionnels.

Par conséquent, les cybercriminels et auteurs de menaces persistantes avancées ou APT ont rapidement perçu les failles potentielles du télétravail. Pour exemple, le volume de données compromises dans le secteur public aux États-Unis a pratiquement doublé l'an dernier. Les administrations gèrent un tel volume de données personnelles et sensibles que la vigilance est plus que jamais un impératif.

Les défis à relever par les RSSI en 2021 pour sécuriser les administrations publiques

Le secteur public est tout sauf homogène, allant de grandes administrations nationales avec des centaines de milliers de fonctionnaires aux petites municipalités qui n'emploient qu'une poignée de personnes.

Que ce soit à l'échelle nationale ou locale, le défi reste le même : en faire davantage avec moins, les ressources ayant fortement diminué dans le contexte pandémique actuel. Dans le même temps, la demande de services, souvent numériques, s'est accélérée.

Par ailleurs, la pérennité annoncée du télétravail signifie que cela continuera de faire partie du paysage des menaces pour les administrations. La sérendipité a joué un rôle dans la mise en œuvre de la sécurité du télétravail pour de nombreuses administrations. Pour celles-ci, le succès de cette sécurisation relevait souvent du hasard, de là où elles en étaient dans leur mise à niveau et leurs choix technologiques. Cependant, l'idée qu'il vaut mieux être chanceux à défaut d'être bon ne peut certainement pas remplacer une stratégie intelligente.

Le RPA et l'automatisation intelligente viennent s'ajouter à cette périphérie élargie de réseau, entraînant un nombre croissant de connexions à des bases de données internes et hétérogènes. La sécurisation de ces nouvelles connexions, souvent vulnérables, est vitale et doit être prioritaire.

2021 sera donc l'année de l'hybride pour le secteur public, c'est-à-dire des activités mixtes et hybrides des administrations… mais aussi des cybercriminels.
Le travail à distance est appelé à perdurer. Les modèles de travail changent à mesure que la robotisation et l'automatisation intelligente se développent.
De la même manière, les acteurs malveillants déploient des attaques utilisant plusieurs techniques, par exemple en panachant DDoS (attaque par déni de service) et phishing. Elles peuvent avoir des conséquences multiples, comme dans le cas d'un ransomware (ou rançongiciel) combiné à du doxing (divulgation de données personnelles). Les attaques mixtes de type best of breed (attaque associant plusieurs techniques éprouvées) ou Digital Frankenstein (association d'informations réelles et falsifiées pour créer une nouvelle identité) peuvent prendre la forme de logiciels malveillants élaborés en associant des composants très performants de malware déjà existants.

Intelligence artificielle, SD-WAN et sécurisation des Edge au programme

Bien que l'intelligence artificielle (IA) et le machine learning (ML) soient, dans l'ensemble, plus utiles aux RSSI qu'aux assaillants, ces derniers ont potentiellement un avantage sur des niches telles que la génération de contenu pour le spear phishing (attaque ciblée et message personnalisé). En effet, des approches hybrides exploitant l'IA peuvent analyser un nombre suffisant d'emails pour tenter d'imiter leur syntaxe et leur style. Le RSSI dispose de suffisamment de données pour définir ce qu'est un comportement normal et repérer les anomalies grâce à l'IA et au ML. Les intrus tentent et échouent à plusieurs reprises avant de réussir à infiltrer leur cible. L'identification de ces échecs permet aux professionnels de la sécurité de repérer une attaque en cours, pour ensuite protéger le patient zéro ainsi que tous les autres collaborateurs.

Pour les administrations publiques, il est essentiel d'aller de l'avant en investissant efficacement, et en évoluant vers le SD-WAN. Le SD-WAN sécurisé est un levier d'économies et de productivité pour les équipes IT et de sécurité. Il améliore également l'expérience utilisateur, renforce la sécurité, la productivité et la résilience. Cet aspect est essentiel si l'on considère que la pandémie de COVID-19 a démontré la nécessité de maintenir les services publics, même lorsque les fonctionnaires et les citoyens sont confinés.

Enfin, l'informatique et les technologies industrielles (Operational Technonology) convergent dans la droite ligne d'une recherche d'économies et de productivité. Ceci est illustré notamment par l'automatisation des bâtiments intelligents et les connexions entre les objets connectés IoT et les dispositifs stratégiques, ainsi que les services externes. Pour cette raison, la sécurisation de l'edge OT est également devenue plus critique.

Au-delà de l'investissement technologique et de la nécessité de recruter du personnel qualifié en sécurité, l'enjeu de la cybersécurité réside également dans la question de l'évolution de la culture des administrations pour intégrer cette nouvelle dimension, transverse par nature.

Parution le 18 juin 2021

Aider nos enfants à devenir des citoyens numériques

GCA (2S) JACQUES HÉBRARD
Senior advisor du CyberCercle

Le secteur public est aujourd'hui, comme le secteur privé, de plus en plus confronté aux risques numériques, et ce d'autant plus après la crise liée à la COVID-19.

La révolution du numérique, la forte croissance d'Internet et la prépondérance des réseaux sociaux ont eu un impact conséquent sur nos enfants.

L'étude Born Social (Association génération numérique)[1] réalisée en 2020 montre que 87 % des enfants de 12 ans ont un smartphone et que le vrai pic d'équipement s'effectue vers 10 ans (on passe de 8 % à 33 % entre 9 et 10 ans). Le smartphone est un objet identitaire qui peut favoriser la cohésion mais aussi développer l'instinct grégaire. L'association E-enfance, qui a doublé son taux de signalement de contenus auprès des réseaux sociaux, observe d'ailleurs une hausse de 26% des cas de cyberharcèlement entre la rentrée 2019 et la rentrée 2020.
En 2017, lors d'une conférence sur l'éducation à la citoyenneté numérique, le Conseil de l'Europe soulignait fort justement que la citoyenneté numérique recouvrait tout un éventail de compétences, de qualités et de comportements capables de mettre à profit les atouts et les possibilités qu'offre le monde en ligne tout en renforçant la capacité de résilience face aux dangers potentiels. Il établissait que les compétences que les citoyens devaient acquérir pour pouvoir participer efficacement à une culture de la démocratie ne s'acquerraient pas automatiquement mais devaient être apprises et pratiquées. En France, avons-nous réellement tout mis en oeuvre pour accompagner une génération numériquement connectée ? Allons-nous en faire des citoyens de demain sensibilisés aux nombreuses menaces auxquelles ils peuvent se trouver exposés ?

Une évolution sociétale qui change les modèles

Être citoyen implique des droits et des responsabilités communes. Dans un monde numérique, où les espaces « réels » et « virtuels » se chevauchent et où les frontières communes aux citoyens de la planète sont définies uniquement par les plateformes utilisées, sensibiliser nos enfants à cet enjeu de citoyenneté est un véritable enjeu de société.

Les activités de cohésion et d'apprentissage des enfants se déroulaient jadis majoritairement à la maison, à l'école, dans des clubs sportifs ou dans des espaces de jeux d'un quartier ou d'une cité. Elles ont tendance à se pratiquer majoritairement aujourd'hui, de manière connectée sur un téléphone, un ordinateur portable, une tablette, une console de jeux ou une télévision.

Les jeunes, qui dans mon propos regroupent les enfants et les adolescents, se connectent souvent seuls en dehors du contrôle des adultes (parents ou enseignants). S'ils visionnent des films et écoutent de la musique, ils passent la plupart de leurs temps sur les réseaux sociaux. Bien que légalement interdits aux moins de 13 ans, ces derniers sont donc aujourd'hui le terrain de jeux de cette jeune génération. Ces pratiques numériques débouchent sur une nouvelle façon d'être, centrée sur une mise en scène du moi et un partage de moments parfois intimes avec les autres. Cette intimité, que la photographie et la vidéo libèrent, interpelle car les jeunes s'exposent mais n'intègrent jamais que leurs actes n'auront pas droit à l'oubli. Cette frénésie de numérique s'accompagne aussi de nouvelles formes de violence et de cyberharcèlement, qui interpellent régulièrement l'opinion publique et pousse les pouvoirs publics à prendre des mesures encore trop insuffisantes. Enfin, elle conduit les jeunes à avoir un nouveau rapport au monde et à l'appréhender différemment des générations précédentes.

Parents et enseignants doivent s'impliquer dans cette mission

La formation et l'information des parents sont essentielles pour leur permettre d'aider leurs enfants à devenir des citoyens numériques en leur montrant comment utiliser judicieusement la technologie numérique et comment se comporter en ligne. Bien souvent, ils n'ont pas conscience des menaces qui

pèsent sur leurs enfants sur Internet. Pourtant il est de leur devoir de les éduquer, de les ouvrir aux cultures des autres et au respect des points de vue de chacun. Il leur appartient de leur apprendre à protéger les informations et les données personnelles des personnes avec lesquelles ils échangent et à les sensibiliser à l'impact que leurs actions ou leurs comportements en ligne peuvent avoir sur les autres. La mort d'Alisha, l'adolescente noyée en mars à Argenteuil, montre que nous sommes loin de cet objectif. C'est tout d'abord une photo intime de la victime en sous-vêtements, piratée sur le compte de l'adolescente qui a oublié de se déconnecter sur un portable. C'est ensuite la diffusion auprès d'élèves sur un groupe via l'application Snapchat qui génère une campagne de harcèlement. Si le harcèlement via les réseaux sociaux ne semble pas être la cause première du décès d'Alisha, il paraît avoir été un catalyseur de la situation, radicalisant les intentions des deux mis en cause. Cette terrible affaire est intéressante à plusieurs titres. Elle met tout d'abord en évidence le pouvoir des groupes, l'effet de bande, que les réseaux installent, puis cette possibilité de hurler avec les loups sans contrainte. Enfin, elle révèle une défaillance dans les capacités de relation avec autrui et surtout un manque d'empathie des auteurs pour leur victime, une absence d'éducation morale leur permettant de discerner le bien du mal.

Dans ce cas comme dans bien d'autres, il n'y a pas forcément une égalité des chances et de nombreux parents sont dépassés, à la fois par le numérique et l'éducation de leurs enfants. C'est la raison pour laquelle l'éducation nationale a un rôle fondamental à jouer.

L'éducation a un rôle fondamental pour préparer nos jeunes à relever ce défi

L'école de la République n'a pas seulement pour mission de construire des savoirs, des savoir-faire et des savoir être, elle doit participer à la formation du futur citoyen. Celle-ci a longtemps été dans son ADN, mais exige aujourd'hui une adaptation aux cultures numériques qui ne doit pas se limiter à une simple prise en main des outils et des services. Les enseignants doivent, en premier lieu, favoriser l'acquisition des fondamentaux. Ils doivent déjà s'attacher à ce que les enfants maitrisent parfaitement notre langue et leur faire acquérir la capacité de communiquer à l'écrit comme à l'oral et leur faciliter la prise de parole pour défendre un point de vue. Enfin et surtout il

faut leur faire acquérir cette capacité, lorsqu'il y a débat, de ne pas confondre la personne qu'on doit respecter, des idées qu'elle professe et qui peuvent être contestées.

L'article L312-15 du Code de l'éducation précise que dans le cadre moral et civique les élèves sont formés afin de développer une attitude critique et réfléchie vis à vis de l'information disponible et d'acquérir un comportement responsable dans l'utilisation des outils interactifs lors de leur usage des services de communication au public en ligne. C'est le principal texte officiel qui permet de relier directement l'acquisition des compétences numériques à la construction d'une éducation globale du citoyen. Les programmes scolaires accordent ainsi une place aux spécificités d'Internet et des réseaux sociaux dans la fabrication de l'opinion publique sur la vie démocratique, pas seulement du point de vue de l'éducation aux médias mais aussi et surtout sous l'angle d'une citoyenneté mondiale à construire. Enfin, les jeunes ont montré leur aptitude à s'appuyer sur le monde numérique pour aider les autres par la création d'associations à vocation caritatives. Les enseignants peuvent, là-aussi, développer cette envie de fraternité par le biais de club numérique à thématiques, ce que l'article L.312-15 recommande dans son dernier alinéa.

Mais l'école doit aller plus loin et ne pas limiter son action à la seule éducation au numérique. Elle doit impérativement délivrer une véritable formation dédiée à la sensibilisation, à la prévention et à la gestion des risques liés aux usages numériques. Elle doit, en lien avec les services de police et de gendarmerie, sensibiliser les enfants au fait que la loi s'applique également dans le champ du numérique et dissiper le sentiment d'impunité.

Aujourd'hui les seules actions existantes relèvent de démarches isolées des chefs d'établissement, professeurs des écoles ou enseignants, convaincus de l'intérêt fondamental de cette démarche. Celles-ci sont complétées par des opérations conduites par les forces de sécurité (à travers notamment du Permis Internet) et un certain nombre d'associations. De nombreux enseignants sont conscients de la nécessité de cette formation, même s'ils ne sont pas, comme de nombreux parents, toujours assez au fait de la question.

De nombreux outils pour sensibiliser à la citoyenneté numérique et à la lutte contre le harcèlement sont disponibles mais pas assez connus

Les outils pour aider les enseignants et parents dans leurs démarches d'accompagnement au numérique ne manquent pas mais ils sont bien souvent trop méconnus. Les quelques exemples que j'ai retenus montrent qu'ils revêtent différentes formes et sont bien souvent complémentaires.

Le manuel d'éducation à la citoyenneté numérique[2], publié en 2020 par le conseil de l'Europe s'adresse aux parents et aux enseignants. Il leur permet d'accompagner les enfants sur la voie de la citoyenneté, grâce à des conseils utiles et des exemples concrets dans la vie quotidienne, à la maison ou à l'école.

Ce manuel décrit en détail les multiples dimensions qui déterminent chacun des dix domaines de la citoyenneté numérique regroupés en trois groupes qui précisent les compétences à acquérir. Le premier groupe « Être en ligne » s'intéresse aux compétences nécessaires pour accéder à la société numérique et s'exprimer librement (accès et intégration, apprentissage et créativité, médias et maîtrise de l'information). Le second groupe « Bien-être en ligne » aide l'utilisateur à s'engager positivement dans la société numérique (éthique et empathie, santé et bien-être, présence et communications numériques). Enfin, le troisième groupe, « C'est mon droit » se réfère aux compétences liées aux droits et responsabilités des citoyens dans des sociétés complexes et diverses dans un contexte numérique (participation active, droits et responsabilités, vie privée et sécurité, sensibilisation des consommateurs).

Le « Kit pédagogique du citoyen numérique »[3] mis en ligne en janvier 2021 par le défenseur des droits a été créé en liaison avec la CNIL et le CSA. Il est articulé autour de six questions :
1) Comment supprimer une photo sur un réseau social ?
2) A quel âge mon enfant peut-il regarder un écran ?
3) Comment distinguer l'offre légale de biens culturels des sites illicites ?
4) Quels sont les droits des internautes ?
5) Quels rôles jouent les médias face aux enjeux d'égalité ?
6) La liberté d'expression connaît-elle des limites ?

Les ressources du kit répondent à ces questions en explorant les droits sur internet, la protection de la vie privée en ligne, le respect de la création, l'utilisation raisonnée et citoyenne des écrans.

La bande dessinée éducative « Dans la tête de Juliette »[4] diffusée par le centre pour l'éducation aux médias et à l'information (CLEMI), chargé de l'éducation aux médias dans l'ensemble du système éducatif, est destinée aux pré-adolescents et adolescents. Elle plonge le lecteur dans le tourbillon de la vie d'une adolescente connectée. Elle interroge avec finesse et pédagogie le rapport des plus jeunes aux écrans, en particulier avec leur smartphone. Son objectif est de les aider à devenir des acteurs conscients et responsables de leurs usages numériques.
Le **30 18**, un numéro unique, consacré à la cyber violence et aux usages numériques des enfants a été lancé le 13 avril 2021 par Adrien Taquet secrétaire d'État chargé de l'Enfance et des Familles, en partenariat avec E-enfance. Ce numéro gratuit et confidentiel s'adresse tant aux jeunes qu'aux parents. Composées de psychologues, de juristes ainsi que de spécialistes du numérique, les équipes d'accueil peuvent également orienter les familles vers les autorités compétentes, comme la Police nationale la Brigade numérique de la Gendarmerie nationale, ou le 119-Enfance en danger. Le 30 18 agit également auprès des plateformes comme Facebook, Twitter, Snapchat, Instagram, TikTok, Twitch, YouTube, ou d'autres, afin de signaler les contenus inappropriés ou haineux.

La loi organique n°2018-1201 du 22 décembre relative à la lutte contre la manipulation de l'information intègre un volet relatif à l'éducation des médias et à la citoyenneté numérique. Le but de ce texte est de favoriser un dispositif non contraignant pour les droits et libertés, permettant à chaque utilisateur précoce des outils numériques de développer un esprit critique vis à vis de l'information trouvée sur les réseaux sociaux. La loi a jugé suffisante les dispositifs éducatifs récents visant à favoriser la capacité des élèves à s'interroger sur la provenance des informations et la fiabilité des sources afin de distinguer une information d'une opinion, d'une rumeur ou d'un propos relevant d'une propagande. Mais hélas elle n'a pas jugé nécessaire d'ériger en priorité nationale la sensibilisation aux risques et la formation aux bonnes pratiques numériques dès le plus jeune âge. Pourtant la Revue Stratégique de Cyberdéfense de 2018 avait réaffirmé que « Si la diffusion de la culture de

cybersécurité numérique ne suivait pas, alors les conditions d'une utilisation sereine et confiante de l'Internet comme des objets connectés ne pourraient être réunies. [...] L'éducation dès le plus jeune âge à la cybersécurité devait constituer une priorité. »

Il n'est toutefois jamais trop tard pour apporter les corrections nécessaires en mettant en oeuvre rapidement plusieurs actions :

- relancer le dépôt d'un amendement afin d'insérer dans l'article L312-15 du code de l'éducation une formation dédiée à la sensibilisation, à la prévention et à la gestion des risques liés aux usages numériques,
- introduire une démarche collaborative entre l'Education nationale et les spécialistes de la sécurité du numérique pour déterminer le contenu du module
- lancer des campagnes d'information (à l'image sur les médias pour aider les parents dans leurs actions de formation de leurs enfants à la citoyenneté numérique (informations sur les outils existants).

Selon le philosophe Michel Serre, « c'est lorsqu'interviennent des révolutions concernant l'information que les civilisations basculent et se mettent en place de manière nouvelle ». Il est temps de cesser les réflexions et d'agir. Façonnés par le monde numérique nos enfants doivent pouvoir agir en citoyens avisés et concernés par le quotidien de notre pays. Il faut leur apprendre à protéger leur « moi numérique », limiter leur vulnérabilité aux « fake news » et dissiper le sentiment d'impunité qu'ils peuvent ressentir sur la toile et qui les conduisent à des actes répréhensibles. Dans une période de montée des populismes et de défiance accrue de la population à l'égard des responsables politiques, il est essentiel que nos enfants participent au bon fonctionnement de notre société. Cela passe par un bon usage du numérique et l'école doit en être le lieu privilégié.

Parution le 25 juin 2021

[1] Etude de l'agence Heaven sur la présence des moins de 13 ans sur les réseaux sociaux #Bornsocial
[2] Manuel d'éducation à la citoyenneté numérique : https://rm.coe.int/info-sheet-keeping-young-citizenshttps://rm.coe.int/prems-047719-fra-2511-handbook-forschools-web-16x24/168098f322-french/16809e2218
[3] Kit pédagogique du citoyen numérique : https://www.defenseurdesdroits.fr/fr/guides/kitpedagogique-du-citoyen-numerique
[4] Dans la tête de Juliette : https://www.clemi.fr/fr/bd_juliette.html

Révolution numérique et enjeux de souveraineté : apprendre à penser global

ALIX DESFORGES
Docteure de l'Institut Français de Géopolitique
et Chercheuse Post Doctorante GEODE – Université Paris 8

Les appels politiques à construire une « souveraineté numérique » en France mais aussi en Europe se sont multipliés ces dernières années. En décembre 2019, Jean-Yves le Drian, Ministre des Affaires Étrangères, appelait à « construire une souveraineté numérique européenne ». Le 1er mars dernier, les chefs de gouvernement de l'Allemagne, du Danemark, de l'Estonie et de la Finlande menaient une initiative conjointe inédite. Dans une lettre adressée à la présidente de la commission européenne, ils estiment qu'« il est désormais l'heure pour l'Europe d'être numériquement souveraine » et enjoignent la Commission à agir pour « exploiter les atouts [de l'Union Européenne] et réduire [ses] faiblesses stratégiques »[1].

La révolution numérique vient bouleverser les modalités de l'exercice de la souveraineté des États parce qu'elle permet des activités transfrontières mais aussi parce qu'elle offre des moyens d'actions à distance pour espionner et saboter des réseaux en dissimulant son identité et en s'abritant derrière des juridictions multiples.

Une volonté politique transformée en solutions techniques

Loin de n'être que des mots, de nombreuses initiatives ont été lancées depuis plusieurs années par les États dont la France. Ces initiatives se formalisent essentiellement par deux types d'actions. Tout d'abord, le soutien à la mise en œuvre d'initiatives industrielles pour favoriser l'émergence de solutions techniques et plus généralement à la constitution de filières industrielles nationales et européennes. La France fait même

figure de précurseur en Europe avec son initiative malheureuse de *cloud* souverain lancée en 2010. Le deuxième type d'actions est le recours à la voix normative, réglementaire et légale – ce qui influence également à la structuration du marché.

En France, si les toutes premières initiatives étaient surtout portées par des arguments de nature économique et industrielle (plan de relance), dès le début des années 2010, l'argument sécuritaire vient alimenter les discours militants en faveur d'une souveraineté numérique et pour devenir même un argument central. L'exemple du cloud est particulièrement symptomatique de cette évolution discursive. Mais surtout, d'un objet technique et mode d'organisation d'un système d'information, le cloud est devenu au fil des années un objet politique, géopolitique et stratégique au regard des enjeux de souveraineté et de puissance qu'il soulève[2].

D'une approche économique et technique aux enjeux stratégiques

Alors qu'à l'origine, les principaux débats politiques sur la souveraineté numérique portaient d'abord sur des problématiques économiques et sécuritaires, le concept a aujourd'hui largement dépassé ces seules préoccupations pour revêtir une dimension stratégique multidimensionnelle. Ainsi, la question des données et les oligopoles américains ou chinois deviennent des enjeux discutés. Les États européens dont la France s'inquiètent de la situation de domination du marché par quelques entreprises non européennes et mettent en œuvre des stratégies (en ordre plus ou moins dispersé) pour faire émerger des entreprises européennes susceptibles de les concurrencer. Face à un cyberespionnage qui ne connait pas la crise y compris entre alliés et la manipulation des données personnelles et des informations sur les grandes plate-formes, les États européens ont pris conscience qu'ils ne pouvaient pas se fier aux technologies et services numériques étrangers. Cette défiance bénéficie aux discours prônant une « souveraineté numérique européenne » en s'appuyant sur le développement de capacités technologiques et de services numériques au sein des États-membres de l'UE. Ces discours se font d'autant plus forts lorsque cette dépendance touche à des capacités souveraines des États notamment dans le domaine militaire et dans celui du renseignement.

Il s'agit bien sûr de saisir des opportunités économiques (participation à un marché en pleine expansion) et d'assurer la sécurité des produits et services notamment par la protection des données, mais aussi de pallier les effets stratégiques d'une telle situation.

En effet, plusieurs événements (dont les affaires Snowden et Cambridge Analytica) ont joué un rôle de catalyseur dans la prise de conscience des risques géopolitiques induits par la situation de dépendance européenne vis-à-vis d'entreprises du numérique étrangères : déstabilisation politique, espionnage stratégique et économique etc. Autant de menaces pour l'avenir politique, économique et démocratique de l'Union Européenne et de ses États membres renforcées par un contexte géopolitique particulièrement tendu (élection de Donald Trump aux États-Unis, Brexit, déstabilisations russes aux frontières est de l'Europe).

En outre, avec l'interconnexion globale des systèmes d'information et de communication, des pans entiers des activités humaines sont transformés en données numériques, et celles-ci se retrouvent de plus en plus au cœur des processus de décision économique, politique, militaire etc. Les données numériques sont également utilisées pour résoudre des problèmes de plus en plus complexes auxquels le monde d'aujourd'hui doit faire face tel que le changement climatique ou la lutte contre la covid-19.

La compréhension de leurs impacts sociaux et politiques est d'autant plus essentielle que deux ruptures technologiques majeures sont en voie de révolutionner le traitement de nos données et d'en accroître la puissance et la valeur : l'avènement de l'ordinateur quantique et l'intelligence artificielle. Ces technologies en plein développement et dont on commence tout juste à entrevoir les implications soulèvent plus que jamais des questions politiques, éthiques et philosophiques majeures.

Le besoin d'une recherche et de formations transdisciplinaires

Ces évolutions rapides et sans précédent induisent des dynamiques intrinsèquement nouvelles par leur nature. Ainsi plus que dans tout autre domaine, la grande intrication d'enjeux d'ordres différents sur les

questions numériques nécessite une approche globale. Si les États sont traditionnellement les acteurs de la mise en œuvre d'une vision globale, ils peinent ici à en saisir toutes les dimensions et à passer d'une structure très hiérarchisée et rigide à une structure plus souple et agile. Ils sont alors concurrencés par des acteurs privés, qui, compte tenu de leur caractère global, ont intérêt à dépasser les considérations partisanes et géopolitiques étatiques.

La question plus spécifique des enjeux de souveraineté posés par le numérique nécessite donc une vision multidimensionnelle, montrant l'intrication de ces différents enjeux, et analysant leur périmètre, la façon dont ils s'influencent mutuellement et les rapports de forces et rivalités qui en découlent.

Les technologies numériques et leurs conséquences sur nos sociétés modernes invitent donc plus que jamais à jeter des ponts entre les sciences de l'informatique et de l'ingénieur et les sciences humaines et sociales (SHS). Dans un domaine encore très marqué par la dimension technique et industrielle, le rôle des SHS, bien que croissant, en est encore à ces prémisses. Pourtant les besoins de penser une approche globale des enjeux de souveraineté sont une question urgente pour tenter d'ores et déjà de limiter les effets des dynamiques en cours défavorables à l'Union Européenne et ses États membres.

Aujourd'hui, la construction d'une autonomie stratégique dans le domaine du numérique en France et en Europe demande de relever plusieurs défis analytiques. Il faut d'abord comprendre les dynamiques et les rivalités de pouvoir géopolitiques associées à la révolution numérique notamment par l'exploitation de données en sources ouvertes. Il faut également identifier les enjeux stratégiques à long terme de la transformation numérique, et la façon dont la société civile, les entreprises et les États vont être impactés, saisir les opportunités offertes (économiques, organisationnelles, politiques et stratégique) tout en limitant les menaces croissantes (cyberattaques, cybercriminalités, actions informationnelles etc).

Sélectionné dans le cadre du label « Centre d'Excellence » du Ministère des Armées, le centre de recherche et de formation GEODE (Géopolitique

de la datasphère) vise précisément à étudier les enjeux stratégiques de la révolution numérique et à contribuer à la réflexion stratégique française sur ces sujets. Adossées à la recherche, les formations ont ainsi pour but de diffuser ces compétences d'analyse stratégique au sein des institutions et des entreprises. Cette tâche est plus particulièrement l'objet du Diplôme de Formation Supérieure Spécialisée d'Université « Révolution numérique : enjeux stratégiques et géopolitiques » (DFSSU, niveau bac+5) dont l'ouverture est prévue en février 2022. Cette formation qui s'adresse spécifiquement aux professionnels (cadres d'entreprises, défense, diplomatie, entre autres) a trait à tous les grands enjeux stratégiques de la révolution numérique pour nos sociétés, et propose également une initiation aux outils permettant d'exploiter les données disponibles en sources ouvertes à des fins d'analyse stratégique (cartographie d'influence informationnelle, réseaux d'acteurs etc.). Autant d'éléments qui doivent de nos jours être pris en compte dans la gestion quotidienne des organisations.

De fait, dans un environnement numérique où les technologies et les réseaux sont partagés entre les mondes civil, économique et militaire, les interconnexions, les interactions et les interdépendances sont multiples mais pas toujours bien comprises et maîtrisées. Comprendre les impacts stratégiques de la révolution numérique est donc essentiel pour l'ensemble des acteurs, privés comme publics : anticiper les menaces, prioriser leurs actions et identifier les opportunités à saisir. Seule cette réflexion globale permettra d'avancer vers une véritable autonomie stratégique dans le numérique au niveau national comme européen.

Parution le 2 juillet 2021

[1] Lettre du 1 mars 2021 signée par la chancelière allemande (Angela Merkel) et les Premières ministres du Danemark (Mette Frederiksen), de l'Estonie (Kaja Kallas), et de la Finlande (Sanna Marin) adressée à Ursula von der Leyen, Présidente de la Commission Européenne. Disponible à : https://valitsus.ee/en/media/3840/download

[2] Bômont et Cattaruzza, 2020, « Le cloud computing : de l'objet technique à l'enjeu géopolitique. Le cas de la France », Hérodote, n°177-178, La Découverte

Gestion des crises cyber : des crises pas comme les autres

JÉRÔME SAIZ
Président-fondateur
OPFOR Intelligence

Même au sein des entreprises dont la fonction de gestion des crises traditionnelles est mûre, le domaine cyber est encore trop souvent traité à part, d'un point de vue purement technique. C'est pourtant oublier l'aspect transverse d'une telle crise, dont la résolution échappe à la seule DSI.

Cela concerne essentiellement les crises de type *ransomware* qui, si elles ne représentent pas la totalité des crises cyber, sont aujourd'hui les plus courantes, les plus visibles (mais ceci explique peut-être cela !) et surtout celles dont l'impact est le plus massif.

Car un tel événement paralyse l'ensemble des fonctions de l'entreprise comme peu d'incidents peuvent y prétendre : les salaires ne peuvent être virés, les lignes de production sont à l'arrêt, les commandes ne peuvent être ni reçues ni expédiées (les entrepôts étant gérés par des outils numériques) et les collaborateurs ne peuvent ni téléphoner ni utiliser l'email. Un tel arrêt brutal et simultané de l'ensemble des fonctions vitales de l'entreprise est rarement présent dans les scénarii traditionnels, en particulier quand celle-ci dispose d'implantations multiples. En temps normal, cela est tout simplement impensable.

La faute aussi, peut-être, à l'idée tenace selon laquelle un tel incident sera du ressort exclusif de la direction des systèmes d'information. « *La DSI va nous réparer tout ça en vitesse* » est souvent le premier réflexe de l'entreprise frappée par un *ransomware*. Or, la DSI ne peut, en réalité, pas y faire grand-chose à elle seule…

Sur le plan technique, d'abord : l'investigation numérique nécessaire afin d'identifier les marqueurs de l'attaque, le vecteur de compromission initiale, le parcours de l'attaquant ou le périmètre compromis est rarement à la portée d'une DSI. Il s'agit d'une expertise très spécifique et, en dehors de grands groupes, peu d'entreprises disposent d'une équipe d'analystes forensiques en interne. De même, le chantier de remédiation du système d'information dans le contexte d'un incident cyber est très, très, loin de celui habituellement prévu par le PRA de l'entreprise. Il s'agit de techniques et de procédures très particulières, qui doivent tenir compte de la perte de confiance dans l'ensemble du SI et se coordonner avec l'avancée (et les exigences) de l'investigation numérique. Le tout sans brûler des étapes (risque de reprise de la compromission) tout en réduisant au maximum la perte d'activité. À l'échelle d'un SI étendu, cela devient un jeu combinatoire particulièrement complexe, qui doit tenir compte des priorités des métiers, des impératifs de production, des dépendances en chaînes entre les systèmes…

Sur le plan des impacts, ensuite : la DSI n'est évidemment pas en charge de la relation client. Or, quand la production s'arrête et qu'il devient impossible d'accepter ou de livrer des commandes, il s'agit évidemment d'une question de relation client. Qu'est-ce qui peut être livré malgré tout ? (mode dégradé, commandes déjà préparées…). Qui privilégier ? Quelle sera la durée d'interruption de l'activité ? Comment convaincre les clients de ne pas changer de fournisseur, quand on sait qu'une crise de type *ransomware* au sein d'une entreprise non préparée paralyse généralement l'activité entre 8 et 10 jours à minima. Une étude aux États-Unis annonçait 9 jours de black-out moyen en 2019, et d'expérience, il s'agit plutôt de 8 à 15 jours d'interruption. Et il n'est pas rare que cela aille jusqu'à un peu plus d'un mois pour les incidents ou les périmètres les plus complexes, avec des effets sur l'organisation qui perdurent plus de six mois après la crise.

En outre, les clients s'isolent de l'entreprise victime afin de ne pas courir le risque d'être compromis à leur tour. Comment regagner leur confiance ? Si la réponse passe évidemment par une composante technique, elle se traite essentiellement au niveau de la direction commerciale, voire de la direction générale pour les clients les plus critiques.

Des enjeux similaires émergent également sur le plan juridique, qu'il s'agisse du réglementaire (RGPD) ou du contractuel (engagement de confidentialité pris auprès de clients importants). Le tout dans un contexte d'incertitude très fort : on ne sait rarement d'emblée si des données ont été dérobées, en quel volume et de quelle nature… Or ce sont des questions pressantes qui se posent dès le début de l'incident.

Et puis la crise frappe aussi les salariés : l'interruption de l'activité va-t-elle conduire à du chômage partiel ? Menacer la survie de l'entreprise ? Doit-on vraiment poser nos RTT en priorité ? Nos congés ? Est-ce obligatoire ? Nos données à caractère personnel sont-elles aux mains de cybercriminels ? Que peuvent-ils en faire ? Comment pouvons-nous nous protéger ? Autant de questions qui exigeront une excellente coordination entre la DSI, les experts techniques, la RH, la communication et la finance.

La coordination, d'ailleurs… La pierre angulaire de la gestion d'une telle crise Cyber est la capacité d'orchestration afin d'apporter du liant entre la DSI (submergée, mais incontournable), les métiers (pressés) et la gouvernance de l'entreprise (souvent d'abord sidérée et ensuite avide de contexte, de conseils et de retours d'expérience afin de prendre les bonnes décisions). Tout en faisant le lien également avec les équipes d'investigation externes et en amorçant au plus tôt le chantier de redémarrage. Du fait de sa forte composante technique transverse, il s'agit là aussi d'une approche différente de celle mise en œuvre lors d'une gestion de crise traditionnelle.

Les crises cyber - en particulier celles de type *ransomware* - sont ainsi très différentes des schémas de crise les plus classiques. Cela tient essentiellement à leur impact immédiat et transverse, par opposition à une situation de crise qui émerge à partir d'un accident localisé et dont les conséquences pourront devenir transverses par effet domino (sinon il ne s'agit pas d'une crise), mais qui n'aura pas le même effet de paralysie soudain et total de l'entreprise dans toutes ses dimensions.

Cela ne doit évidemment pas exclure pour autant l'organisation actuelle de la gestion des crises : ses méthodes, ses outils et surtout son expérience sont précieux. Au même titre que sa capacité à consacrer du temps et de

la ressource à la réflexion autour des sujets de crise, au développement de scénarios tenant compte de l'évolution de la menace et à l'organisation d'exercices. Il est toutefois nécessaire de l'inclure dans les approches spécifiquement cyber, peut-être à travers des sensibilisations et des réflexions communes, et peut-être par le biais d'une adaptation du plan de crise existant, afin d'intégrer la composante cyber.

Dans tous les cas, un tel impact massif et transverse exige une réponse massive et transverse elle aussi !

Parution le 9 juillet 2021

Le Réseau Radio du Futur : Un outil de communication majeur pour les missions des forces de sécurité et de secours

GUILLAUME LAMBERT
Préfet, Conseiller au cabinet du Secrétaire Général,
Responsable du programme Réseau Radio du Futur,
Ministère de l'Intérieur

Les enjeux du programme Réseau Radio du Futur (RRF)

Les enjeux de sécurité et les risques, que notre pays doit prendre en compte, ont suscité une réflexion sur la nécessité de créer les conditions d'une sécurité globale, au-delà des traditionnelles césures entre services de l'État et ceux relevant des collectivités locales, entre les acteurs publics et les acteurs privés. Les attentes des concitoyens en matière de sécurité et secours exigent un décloisonnement de l'ensemble des services qui concourent au quotidien à leur protection.

Dans ce contexte d'émergence de nouvelles menaces (terroristes, violences urbaines, dérèglement climatique, crises sanitaires…) et de sollicitations croissantes des services de sécurité et de secours ; disposer d'outils de communication adaptés est essentiel.

Les réseaux radio actuels des forces de sécurité et de secours actuels sont désormais vieillissants et méritent d'être renouvelés : le réseau RUBIS de la Gendarmerie a été créé en 1986, tandis que l'Infrastructure Nationale Partageable des Transmissions (INPT) a été lancée dans sa version ACROPOL pour la Police en 1994.

Ces réseaux proposent des fonctions qui ne sont plus aujourd'hui adaptées aux besoins des services de sécurité et de secours

(interopérabilité très restreinte, partage de données et vidéo inexistantes à titre d'exemples). Ils reposent sur une technologie antérieure à la deuxième génération (2G) de la téléphonie mobile et sont devenus, avec le temps, coûteux en termes d'entretien et de maintenance. En effet les équipements d'infrastructure sont vieillissants, qu'ils s'agissent des ateliers d'énergie, des batteries de secours, de la centrale de gestion de l'infrastructure ou encore des climatiseurs et des extracteurs d'air. Ainsi, les coûts de maintenance de ces réseaux sont amenés à croître avec le temps.

En synthèse, on observe un décalage technologique entre les outils de communication mis à disposition des services de secours et de sécurité (des terminaux radio bas débit) et les usages de la société qui utilise des smartphones fonctionnant en 4G et bientôt en 5G. En les remplaçant, le RRF répond doublement aux attentes du concitoyen car il fournit un service de communication au meilleur de la technologie et transversal entre tous les acteurs de la sécurité et du secours, tout en réalisant des économies d'échelle.

C'est pourquoi l'évolution des moyens de radiocommunication en France est un tournant majeur à ne pas manquer, car leurs limitations actuelles nécessitent la création d'une solution offrant un ensemble d'applications, d'outils et de services adaptés à l'ensemble des utilisateurs et qui restent accessibles économiquement.

Un système de communications mobiles pour missions critiques s'appuyant sur les standards internationaux

L'objectif du RRF est d'offrir dès 2023 un système de communication haut débit, sécurisé, résilient et pleinement interopérable aux services de sécurité et de secours en s'appuyant sur les standards définis par le groupe 3GPP au titre des communications dédiées aux missions critiques.

De ce point de vue, le programme RRF représente une évolution profonde des moyens de communication des services de sécurité et de secours.

Le RRF s'appuiera en effet sur les infrastructures des opérateurs privés de téléphonie mobile, en offrant un dispositif de priorité/préemption pour

éviter toute saturation en cas de congestion du trafic, ainsi que sur des dispositifs projetables d'extension de couverture radio 4G pour garantir la résilience des communications haut débit.

La réalisation du système de télécommunication critique RRF passe par l'acquisition de trois éléments fondamentaux qui formeront le cœur technique de la future infrastructure de communication critique :

- une capacité d'accès à la couverture radio 4G (puis 5G) et aux services de téléphonie et d'internet auprès de deux opérateurs de réseaux mobiles ;
- l'acquisition des capacités techniques d'un opérateur de réseau mobile virtuel (MVNO) à savoir un « cœur » de réseau télécom, un système d'information de gestion du RRF et de ses abonnés, un centre d'opération du réseau RRF (NOC), une offre de terminaux mobiles ;
- l'acquisition d'une capacité à délivrer des services applicatifs de communications pour missions critiques (MCx), permettant d'organiser des communications multimédias de groupe au profit des abonnés du RRF en bénéficiant d'une qualité de service avec priorité et préemption dans les réseaux 4G.

Un service de communication dédié aux acteurs de la sécurité et des secours dans leur diversité

Le RRF s'adresse aux services qui ont en charge au quotidien les missions de sécurité et de secours, la protection des populations et la gestion des crises et des catastrophes.

Les communautés utilisatrices du RRF recouvrent donc une assez grande diversité d'organisations puisque parmi les futurs services éligibles on trouvera aussi bien les préfectures que les maires, la gendarmerie et la police nationale que les polices municipales ou le ministère des armées au travers de la mission Sentinelle, les SDIS (services départementaux d'incendie et de secours que les moyens nationaux de la sécurité civile ou les services d'aide médicale urgente (SAMU) mais aussi le ministère de la justice, les douanes, etc).

Le RRF a été conçu pour prendre en considération les besoins de chacune

de ces communautés, tout en permettant la collaboration entre les différents acteurs. A ce titre, les communautés utilisatrices du RRF font partie intégrante de la gouvernance du programme, et seront représentées au conseil d'administration de la future structure porteuse. Elles ont été associées en détail à la conception de la solution, permettant à la maîtrise d'ouvrage du RRF de connaître précisément les besoins et contextes d'emplois de chacune d'elles.

Des usages inédits et innovants au bénéfice des communautés utilisatrices

La solution RRF offrira à ses communautés utilisatrices de nouveaux usages de captation et de diffusion de la donnée opérationnelle en temps réel, absolument inédits dans le quotidien des utilisateurs.

Le RRF permettra deux nouveaux usages principaux :

- De nouvelles fonctionnalités de communication critiques multimédias : le RRF repose sur des technologies standardisées, offrant des possibilités élargies à ses utilisateurs : communications vidéo de groupe ou interpersonnelles, géolocalisation des utilisateurs et points d'intérêt… Standardisés par le 3GPP, ces services de communications pour missions critiques sont accessibles à l'ensemble des utilisateurs du RRF, sur le terrain comme en salle de commandement.

Les services missions critiques offrent trois types de fonctionnalités principales :
- le MCPTT (Mission Critical Push-To-Talk) : service de conférence vocale ;
- le MCVideo : service de conférence vidéo qui utilise les capteurs vidéo du smartphone pour échanger des vidéos soit en temps réel entre les utilisateurs d'une conférence MCx, soit en asynchrone dans des outils de type messagerie instantanée ;
- le MCData : service de connectivités de données : fichiers, géolocalisation, informations sur les terminaux (couverture, niveau de batterie du terminal).

- Une interopérabilité complète et native : le RRF est par conception un système de communication commun à l'ensemble des acteurs de la sécurité et du secours et nativement interopérable. Les échanges en interservices bénéficient ainsi du même ensemble de fonctionnalités de communications multimédias de groupes que celui disponible au sein d'une communauté, avec les mêmes exigences de sécurité et de réactivité et dans le respect des doctrines d'emplois de chaque communauté.

Ce passage à l'ère de la donnée des communications opérationnelles des services de sécurité ou de secours devra se réaliser en respectant scrupuleusement les obligations européennes et nationales en matière de protection des données personnelles.

La possibilité de capter et de diffuser des données en temps réel n'impliquera pas son utilisation en continu. L'architecture du RRF empêche d'ailleurs par défaut le partage de données, qui n'est possible que par exception quand la situation opérationnelle l'impose. C'est le contexte de la mission, et donc la finalité, qui conduira à activer un partage en temps réel de données audio et vidéo, selon un principe de minimisation des données (respect du principe de proportionnalité). C'est ainsi qu'a été identifié un ensemble restreint de finalités où la criticité et la probabilité d'occurrence d'une situation justifieraient cet usage, comme par exemple la prévention des risques d'atteinte à l'intégrité physique d'un agent d'un service de sécurité ou de secours, les opérations de secours aux personnes, l'existence d'un péril imminent, la lutte anti-terroriste, la prévention des risques d'atteintes aux biens et aux personnes dans le cadre de troubles graves à l'ordre public.

L'usage de ces données opérationnelles d'environnement se traduira par des apports concrets pour les acteurs de la sécurité et du secours :

- **L'amélioration de l'intelligence situationnelle, à travers :**
  - **une meilleure efficacité opérationnelle :** la diffusion de vidéo avec audio permet de retranscrire de manière plus fiable et détaillée le contexte d'une intervention, au bénéfice des opérateurs en salles ou des utilisateurs sur le terrain qui, habilités à accéder aux données, disposent tous du même niveau d'information ;

- **une identification facilitée** des situations et individus potentiellement à risques.

• **L'amélioration de la sécurité des utilisateurs lors d'une intervention, à travers :**
  - **une meilleure compréhension des situations de danger** pour les utilisateurs (appel de détresse géolocalisé, fonctionnalité de protection des travailleurs isolés (PTI) paramétrable, etc.), et des réponses plus adaptées à ces situations ;
  - **une levée de doute plus fiable** par les opérateurs des salles de commandement en cas d'appel de détresse (écoute d'ambiance, déclenchement des flux vidéo du terminal…).

  - **L'amélioration de la sécurité des citoyens et du grand public** à travers des interventions plus rapides ou une meilleure sécurisation de grands évènements car mieux renseignées, un meilleur partage de l'information entre les différents services intervenant et la capacité de bénéficier de l'appui d'experts à distance et en temps réel.

Une approche « privacy by design and by default »

La protection des données a été prise en compte dès la conception de l'architecture du RRF. Le RRF sera compatible avec les exigences élevées du socle de sécurité du ministère de l'Intérieur afin, notamment, d'assurer un haut niveau de sécurisation de l'accès au service et de traçabilité des actions réalisées en son sein par les utilisateurs.

Cette démarche de sécurisation et de protection des données se déclinera en un ensemble de règles techniques et organisationnelles. Les dispositions techniques intègrent la sécurisation physique des composants du RRF, une sécurisation technique des données à toutes les étapes de son utilisation (intégrant l'authentification des utilisateurs et des terminaux et le chiffrement des données) et une supervision SSI opérée par le centre de cyberdéfense du ministère de l'Intérieur. Des règles organisationnelles complèteront ces dispositions et comporteront notamment des actions de sensibilisation des utilisateurs au bon usage de la donnée.

Le RRF est construit selon un principe de cloisonnement entre communautés utilisatrices, et au sein de ces dernières. Ce cloisonnement garantit la limitation de l'accès des utilisateurs aux communications qu'ils ont à connaître spécifiquement. Ainsi, chaque communauté dispose de son propre environnement de communication, par défaut fermé aux autres utilisateurs. Ces derniers sont strictement identifiés et authentifiés, et rattachés à une communauté.

Les communications s'organisent au sein de ces environnements à travers des groupes de communication fermés, appelés « conférences ». Ces conférences sont également fermées par défaut, et ne rassemblent que les utilisateurs habilités à accéder aux données. Au sein de ces conférences, les utilisateurs ont accès à des fonctionnalités d'échange multimédia, permettant une communication riche entre membres.

Chaque communauté organise son arborescence de conférences en fonction de sa doctrine d'emploi. Une conférence peut être permanente ou temporaire, active à tout moment ou à la demande. Des conférences peuvent ainsi être définies pour correspondre à des périmètres géographiques fixes (la zone d'intervention du centre d'incendie et de secours du département en question), à un service ou un ensemble de services (les services composants une direction départementale de la sécurité publique par exemple), à une intervention précise (les services engagés à la suite d'un accident de la route) ou à toute autre fin définie par la communauté.

Ces principes d'organisation des conférences s'appliquent aux communications au sein d'une communauté, comme entre plusieurs communautés. Vecteur d'interopérabilité, le RRF permet ainsi de créer, à la volée ou de manière pérenne, des conférences associant utilisateurs de différentes communautés, habilités à accéder aux données d'un même sujet d'intérêt ou d'une même intervention. Par exemple, il sera possible de créer une conférence associant des utilisateurs issus de l'escadron départemental de sécurité routière du Vaucluse, de la direction interrégionale des routes Méditerranée, du SDIS du Vaucluse et de l'opérateur des autoroutes du Sud de la France - dans les mêmes conditions d'accès et de cloisonnement que pour une conférence propre à une

communauté. Une doctrine d'interopérabilité viendra définir les principes de communication interservices généraux et propres à chaque environnement (local ou thématique).
Trois types d'utilisateurs sont définis au sein du RRF, en fonction de leurs rôles et des droits qui leurs sont associés :

- Administrateur fonctionnel d'entité, en charge de créer et de gérer les conférences permanentes, et de créer et gérer les droits des utilisateurs de sa communauté. Un administrateur fonctionnel n'a, par défaut, pas accès aux contenus des échanges transitant sur une communauté ;
- Opérateur de salle de commandement, et dont la mission consiste à exploiter en temps réel les conférences dont il a la charge, d'autoriser leur accès aux utilisateurs et de définir les droits de ces derniers au sein des conférences. Il peut également créer des conférences à la volée s'il dispose des droits pour ce faire ;
- Opérationnel, qui correspond à la grande majorité des futurs utilisateurs ayant accès aux conférences définies dans leurs droits par l'administrateur fonctionnel, et dans les conditions définies par l'opérateur de salle de commandement.

Ces principes de cloisonnement et de gestion fine des droits et des accès garantissent une diffusion des données captées restreinte aux utilisateurs habilités à accéder aux données. Ces garanties restent applicables également dans le cadre d'un environnement plus complexe, par exemple lors d'une intervention en interopérabilité mobilisant un grand nombre d'acteurs issus de différentes communautés. Cette architecture garantit un accès exclusif de certains types de données aux seuls utilisateurs habilités à y accéder (comme, par exemple, les données de santé).

Une communication directe multimédia entre deux ou plusieurs utilisateurs d'une communauté est par ailleurs également possible, dans le respect des mêmes doctrines d'emplois et règles de gestion métier. Un utilisateur ne pourra contacter qu'un ensemble de destinataires définis par ces dernières. Ce type de communication est également possible entre utilisateurs de communautés différentes, si les règles de gestion définies en fonction des doctrines d'emplois le permettent.

Planning et Plan de déploiement du RRF

La démarche de déploiement du RRF vise prioritairement les territoires pilotes des grands évènements sportifs des années à venir. L'objectif principal en termes de déploiement du RRF est d'être au rendez-vous des deux échéances majeures que sont la coupe du monde rugby de 2023 et les jeux olympiques et paralympiques de 2024 sur les territoires hôtes de ces deux événements, prioritairement pour ce qui concerne les acteurs clés en charge de la sécurité et des secours : préfectures, services de police et de gendarmerie nationales, services d'incendie et de secours (SIS), SAMU/SMUR, militaires de l'opération Sentinelle, polices municipales.

Ces deux grandes échéances conditionnent la conception et le déploiement de ce projet. Ainsi, l'avis de marché en vue de sélectionner les industriels qui apporteront leur concours à la réalisation du cœur technique de RRF a été publié le 1er décembre 2020. La passation des marchés devrait intervenir en novembre prochain, ce qui permettra de déployer le RRF auprès des entités utilisatrices pilotes au premier semestre 2023. Un plan de construction de l'architecture par versions successives a ainsi été mis en place afin de sécuriser la disponibilité des principaux services en version 1 (premier opérateur raccordé, fonctionnalités essentielles et déploiement des 90 000 premiers abonnés mobiles) dès fin 2023 avant de gagner en fonctionnalités pour les versions suivantes du RRF. Puis raccordement du deuxième opérateur, déploiement de nouvelles fonctionnalités et extension du périmètre de déploiement à 100 000 abonnés mobiles supplémentaires pour la V2 disponible début 2024. Enfin, fonctionnalités complètes déployées sur l'ensemble du périmètre d'abonnés mobiles cible pour la V3 à compter de début 2025.

Au total, plus de 300 000 agents sont susceptibles d'être utilisateurs de ce système de communications. Le continuum des acteurs de sécurité et de secours est l'ambition d'offre de services et d'interopérabilité du RRF.

Dès octobre 2017, à l'occasion de son discours aux forces de sécurité et de secours, le Président de la République a lancé le programme RRF en soulignant les enjeux majeurs attachés à sa réalisation, « *Un des grands projets régaliens sera le réseau radio du futur à haut débit commun à la*

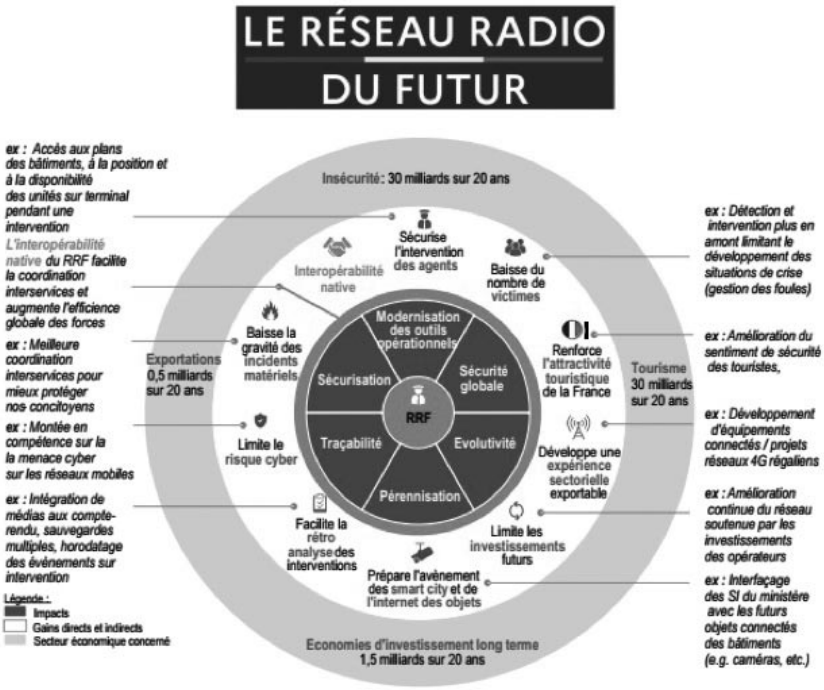
police, la gendarmerie et la sécurité civile qui devra bénéficier d'un haut niveau de résilience en cas de crise et des meilleures technologies numériques disponibles. Ce sera un grand projet industriel français et européen dont le déploiement doit se faire le plus rapidement possible et fait aussi l'objet d'un engagement clair en termes financiers dans le cadre du grand plan d'investissement. »

Ce nouveau système offrira à celles et ceux qui nous protègent des bénéfices opérationnels majeurs. La capacité de partager une même information, notamment à l'aide de flux vidéo, sur le terrain et en salles de commandement, améliorera l'intelligence situationnelle des communautés utilisatrices, permettant un meilleur engagement et un meilleur pilotage des moyens. Les intervenants sur le terrain verront leur sécurité renforcée grâce au partage de leurs géolocalisations et à une meilleure compréhension de leurs environnements d'intervention. L'interopérabilité native du RRF permettra d'étendre au besoin ces capacités aux échanges entre services et facilitera la coopération au quotidien.

Les retombées et les impacts pour la société civile touchent tous les secteurs (tourisme, exportation, insécurité, …). Les gains directs et indirects sont nombreux : (sécurisation des interventions des agents, baisse du nombre de victimes, …) avec de réelles économies d'échelle qui seront détaillées en annexe en fin d'article.

Le RRF permettra à la France de rejoindre les quatre autres premiers pays au monde ayant mis à disposition de leurs services de sécurité et de secours des outils de communications de dernière génération : le Royaume Uni avec son réseau ESN et le projet ESMCP, les Etats-Unis avec FirstNet, la Finlande avec Virve 2.0 et la Corée du Sud avec SafeNet.

Parue le 16 juillet 2021



Les impacts positifs attendus du déploiement du Réseau Radio du Futur

La cybersécurité n'est plus une option pour nos Territoires de projet !

JOSIANE CORNELOUP
Présidente
Association Nationale des Pôles d'équilibre territoriaux
et ruraux et des Pays (ANPP)
Députée de Saône-et-Loire

Sarrebourg, Évreux, Bayonne, La Rochelle, Angers, Houilles, Annecy, Aix-Marseille-Provence… autant de collectivités qui ont été victimes de cyberattaques ces derniers mois. La liste ne cesse de s'allonger à un rythme qui s'accélère depuis un an, notamment avec la digitalisation accentuée de nos modes de travailler, de consommer, de produire, de vivre tout simplement. Paralysie des services, pertes et fuites de données, rupture du lien de confiance avec les citoyens, image dégradée… autant d'impacts majeurs qu'une cyberattaque réussie entraîne pour une collectivité.

Aujourd'hui, la question n'est donc plus de savoir "si" les collectivités seront la cible d'une cyber-malveillance, mais "quand" : toutes sont concernées par cette menace en plein développement, quelles que soient leur taille et leur localisation géographique. Il est donc aujourd'hui indispensable de se doter d'une politique de cybersécurité cohérente et d'en faire un axe de leur culture, afin de sécuriser leurs missions au service des citoyens et habitants et des acteurs économiques présents sur leur territoire.

Alors même que le numérique devient de plus en plus omniprésent dans nos sociétés, la crise sanitaire que nous traversons actuellement a accéléré ce phénomène de transformation profonde, auquel n'échappent pas les collectivités. Nombre d'entre elles se sont engagées dans un

processus de modernisation continue de leur administration et des services qu'elles délivrent. Que ce soit sous l'impulsion des citoyens ou de la réglementation, elles sont au tournant de la numérisation de la "relation citoyen" : l'e-administration (*numérisation des démarches administratives, à laquelle s'ajoute une recherche de simplification*) est un axe important de la modernisation de l'action publique et répond à une demande effective des citoyens dans le cadre de l'e-démocratie. Elles détiennent par ailleurs une masse importante de données, parmi lesquelles des données à caractère personnel, dont la divulgation, la suppression, l'altération, le vol, la mauvaise utilisation sont susceptibles de porter atteinte aux droits et libertés des personnes ou à leur vie privée, ou à une mauvaise gestion de l'ensemble des responsabilités sociétales dont les collectivités ont la charge : état-civil, justificatifs de domicile, données fiscales, sociales, inscriptions en établissement scolaire, résultat de vote électronique, études foncières, projets de délibérations, schémas d'aménagement, documents budgétaires… En dehors de la réglementation, notamment le RGPD, la protection de ces données est ainsi non seulement un facteur de bon fonctionnement de la société mais aussi un élément de transparence et de confiance à l'égard des citoyens.

Au-delà de cet enjeu de protection des données, la cybersécurité est également au cœur des infrastructures que gère une collectivité : gestion de l'eau, des déchets, des systèmes de l'éclairage public, des infrastructures sportives, vidéosurveillance, mobilité intelligente, écoquartiers… autant de systèmes gérés par le numérique et le développement d'objets connectés qui se doivent d'être sécurisés, car exposés. Par exemple, la tentative récente avortée de sabotage via une attaque informatique du réseau de distribution d'eau de collectivités aux Etats-Unis en février dernier montre s'il en était besoin combien l'enjeu de la sécurisation de tels systèmes est impérieux.

Au-delà, les collectivités se sont lancées dans des plans de développement via le numérique au service des acteurs présents sur leur territoire : plan d'accompagnement à la transformation numérique des acteurs économiques, des commerçants aux industries, de développement de la e-santé ou de l'industrie 4.0, programmes

d'inclusion numérique, création de tiers lieux, accompagnement au déploiement du télétravail… Autant d'actions fondamentales aujourd'hui pour l'attractivité et le développement des territoires, mais qui constituent autant d'espaces vulnérables.

Cette transformation numérique profonde des collectivités opérée pour leurs propres infrastructures, induit de fait de nouveaux risques : face aux menaces numériques, la cybersécurité n'est plus une option. Or, la dimension sécuritaire n'est généralement pas suffisamment prise en compte dans les démarches de transformation numérique des collectivités, qui ne sont souvent orientées que vers les usages.

L'enjeu est donc de mieux sensibiliser et surtout éclairer sur les enjeux liés à cette menace, de faire de la sécurité un pilier majeur de la transformation numérique des collectivités et de leurs plans d'actions, et d'hisser cet enjeu comme étant un élément phare de la culture numérique de l'ensemble des élus et des collaborateurs.
La cybersécurité souffre en effet de son image technocratique et lointaine, jusqu'au jour où l'on est concerné. Elle est souvent vue comme un sujet purement technique, réservé à des experts. Cependant ce sujet, quand il est pris en compte et anticipé par les collectivités, est souvent enfermé dans la tour d'ivoire du service informatique, qui a bien souvent du mal à mettre ses recommandations en œuvre tant cette dimension est perçue au mieux comme accessoire ou frein à la mise en œuvre du développement des projets, au pire comme un seul facteur de coût.

Or, la sécurité numérique n'est pas uniquement un sujet technique. Elle repose avant tout sur de la gouvernance, du management, de l'organisation, de la sensibilisation, de la formation, du juridique, de relations avec l'ensemble de l'écosystème d'une collectivité : prestataires, partenaires… autant de dimensions qui sont hors de la simple sphère "informatique". Elle repose sur le facteur humain et à ce titre concerne l'ensemble des collaborateurs d'une structure : en matière de cybersécurité, l'adage veut que le maillon faible se situe entre le clavier et la chaise. Plus de 80% des incidents de sécurité relèvent d'une erreur humaine. Mais ce qui montre aussi que l'humain bien formé peut

devenir le maillon fort de la cybersécurité.

Face à ce phénomène de transformation numérique des collectivités, au recours au numérique comme facteur de développement des territoires, la sécurité numérique doit devenir un élément clef au cœur de l'action des collectivités, avec deux impératifs : que l'ensemble des élus s'approprient cette dimension dans leur vision stratégique de l'avenir des collectivités qu'ils dirigent, seuls capables d'insuffler l'impulsion nécessaire pour une politique de sécurité numérique transverse ; qu'elle devienne un des piliers de la culture de chaque agent, dans les missions qu'il conduit ou de ses usages des outils numériques.

Aujourd'hui, il ne peut y avoir de développement responsable et d'attractivité des territoires sans numérique, pas de numérique pérenne sans confiance numérique, et pas de confiance numérique sans sécurité numérique. C'est bien là que réside l'un des enjeux majeurs d'une transition numérique responsable.

Parution le 23 juillet 2021

Affronter la tempête cyber

GCA ÉRIC BUCQUET
Directeur de la Direction du Renseignement et
de la Sécurité de la Défense (DRSD),
Ministère des Armées

L'attaque *SOLARWINDS* d'une sophistication incroyable visait le pré-positionnement d'agents logiciels dormants dans des systèmes d'information sensibles ou critiques aux États-Unis.

L'attaque de l'opérateur d'oléoducs *COLONIAL PIPELINE* a généré une crise de plusieurs jours sur toute la côte Est des États-Unis privée de sa principale source de carburant et de kérosène.

Le récent siphonage des données de 700 millions d'utilisateurs de LinkedIn représente autant de possibilités par rebond de cyber malveillances, d'escroqueries ou de fraudes en tous genres, etc. La revente de données volées à des services de renseignement étrangers est désormais une option qu'il ne faut pas exclure.

Ces trois exemples récents sont symptomatiques du climat cyber actuel. La croissance du nombre d'attaques, de leur diversité, de leur intensité et de leur sophistication ne semble avoir aucune limite, aucune frontière. Les groupes mafieux se sont professionnalisés, certains ont formé des cartels, et ont acquis une telle expertise offensive que certains États n'hésitent pas à faire appel à leurs services.

Selon l'agence européenne de cybersécurité (ENISA), 38% des acteurs malveillants seraient rattachés à des États-nations[1].

A quel type d'attaque cybernétique majeure, la France numérisée doit-elle se préparer ?
Les services spécialisés de l'État seront-ils en mesure de prévenir ou de faire face à un cataclysme numérique d'ampleur nationale ? Comment affronter la Tempête Cyber ?

De l'amplitude et l'intensité d'attaques préoccupantes

Une prise de conscience progressive de la menace est palpable, mais la réalité de cette dernière est probablement sous-estimée.
Le Président Macron déclarait, le 18 février 2021, à propos de la menace cybernétique, qu'elle était « extrêmement sérieuse, parfois vitale et touchait tous les secteurs ».

Interrogé par la commission des Affaires européennes du Sénat, le directeur général de l'agence européenne de cybersécurité (ENISA), Juhan Lepassaar a donné des chiffres vertigineux. En 2020, le coût des cybercrimes s'est élevé à 5,5 milliards d'euros, un chiffre multiplié par deux par rapport à l'année précédente.

Pour l'ANSSI, « c'est fois 4. Il y a véritablement une explosion ». Et encore, ces chiffres ne recouvrent donc que les cas de rançonnage sur lesquels l'agence nationale a été amenée à intervenir. C'est ainsi que Guillaume Poupard a caractérisé la situation sur le front des cyberattaques stratégiques, en France, en 2020. Il identifie trois grandes menaces : l'espionnage « c'est une menace dont on ne parle pas », la grande criminalité, et « des risques quasiment militaires ». Sa conclusion est très claire : « l'impact sur notre sécurité nationale serait maximal », si d'aventure un acteur malveillant venait à passer à l'offensive.

Notre culture stratégique nationale comme celle de nombre de pays occidentaux s'est concentrée sur la défense de nos intérêts vitaux établissant une liste confidentielle d'environ 250 entreprises basées en France dans 12 secteurs d'activité.

Pour autant, leur talon d'Achille vient le plus souvent de leurs chaines d'approvisionnement, ces centaines et milliers de PME/ETI, sous-

traitants plus ou moins vulnérables de nos institutions et des grands groupes du CAC40. Pour le périmètre des entreprises de la sphère de défense dite « BITD »[2] ce sont ainsi 4 000 entreprises soit plus de 200 000 personnes dans un écosystème critique pour notre souveraineté nationale, sur lesquelles veille la DRSD en proximité. Ajoutons à ce chiffre les 10 000 entités suivies au titre de la protection du potentiel scientifique et technique de la Nation.

Le protocole signé le 4 mars de cette année entre la ministre des Armées et cybermalveillance.gouv.fr (GIP ACYMA) a permis au ministère, et à la DRSD qui le représente, de disposer d'une vision plus élargie de la cyber malveillance en France.

Ainsi, le bilan 2020 du dispositif Cybermalveillance.gouv.fr est éclairant et le constat que fait Jérôme Notin, directeur général du GIP ACYMA est clair : il existe de très fortes similitudes, à quelques nuances près, entre les professionnels du public et ceux du privé ayant requis une assistance. Cela tend à démontrer que ces deux catégories de publics sont touchées par les mêmes phénomènes cybercriminels dans des proportions comparables. En progression de 30%, les vagues d'attaques par rançongiciels sont devenues en 2020 la principale menace à laquelle les professionnels ont été confrontés. Les chiffres du 1er semestre 2021 confirment que les rançonnages tiennent la première place des attaques, immédiatement suivis par les piratages de comptes en lignes qui font un bond depuis l'assouplissement des mesures sanitaires et la conséquente reprise d'activité.

Jérôme Notin fait, par ailleurs, état de 837 entreprises touchées en 2020, contre 667 en 2019. Une chose est certaine, l'écart dans l'observabilité effective des attaques est énorme et Jérôme Notin est lui-même certain de ne pas disposer d'une image complète de la situation réelle.

Nous n'avons tous qu'une image partielle. La DRSD contribue à la définition d'une image globale de la menace.

Quel serait alors l'impact d'une tempête cyber sur le territoire national ?

C'est une question fondamentale qui concerne l'ensemble des services de l'État et un grand nombre d'opérateurs privés car elle sous-tend notre stratégie nationale de cyberdéfense. Mais je vais essayer d'y répondre simplement et, afin éclairer cette réflexion, je ferai le parallèle avec les 2 tempêtes d'origine naturelle qui ont successivement ravagé la France en décembre 1999.

Le 26 décembre, un premier passage ravage le nord de la France, provoquant de nombreuses victimes et des dégâts sur les habitations et sur les réseaux d'infrastructure (routes, téléphone, électricité). Les services de secours sont saturés d'appels, ne peuvent intervenir partout à la fois et l'opérateur EDF est totalement débordé par l'ampleur des travaux d'assistance des usagers et les réparations de son réseau. La seconde tempête, 24 heures plus tard, ravage le sud de la France, provoquant un chaos supplémentaire. Malgré une solidarité exemplaire et une mobilisation collective, en faisant appel à des réservistes et des retraités, le bilan humain et matériel sera lourd et le retour à la normale prendra des mois.

Les ravages numériques causés lors d'un conflit dans le cyberespace par des bataillons de cyberattaquants seraient similaires aux effets des éléments naturels déchainés. A ce chapitre, l'attaque mondiale SOLARWINDS est un avertissement fort : une cyberattaque de ce niveau de sophistication, initiée à des fins de sabotage ou de destruction systémique, n'épargnerait personne.

Notre devoir est de nous préparer collectivement à ces « cyber tempêtes » qui seront fulgurantes. Ce n'est pas le jour de la tempête qu'il faudra construire les liens entre tous les acteurs publics et privés concernés. La DRSD s'emploie au quotidien à construire la confiance avec les entreprises dont elle a la charge.

Cela pourrait paraitre paradoxal pour un service tel que la DRSD mais quand bien même nous nous qualifierions de « service de

renseignement discret », le brin d'ADN endémique de notre direction est bel et bien la protection du secret de la Défense nationale. Ainsi, depuis 150 ans, nous veillons à la sécurité physique et depuis une quarantaine d'année à la sécurité numérique de l'écosystème de défense français face aux menaces TESSCO[3].

Comment se préparer aux pires et aux moins mauvaises météo cyber ?

Premier point : Anticiper l'indisponibilité des systèmes d'information et de communication. Notre action commence tout d'abord par de la sensibilisation et de la formation de populations très diverses, des dirigeants d'administrations ou d'entreprises aux collaborateurs en passant par les officiers de sécurité et les responsables de la sécurité des systèmes numériques.

J'utilise volontairement cette sémantique de « systèmes numériques » car notre compétence porte à la fois sur les traditionnels systèmes d'informations et sur les systèmes électroniques de sécurité (contrôle d'accès ou d'intrusion, vidéoprotection, etc.).

En 2020, malgré la pandémie, le Service a mené 230 actions de sensibilisation de PME/ETI dans les territoires et 7 auprès des COMEX de grands groupes de défense essentiellement localisés en Ile de France. Selon le public ciblé plusieurs formes de sensibilisations peuvent être offertes, de la présentation de type « PowerPoint » à la simulation ad hoc d'attaque cyber par ingénierie sociale, en passant simulation générique d'attaques de type vol de mot de passe ou rançonnage (avec notre plateforme CENTAURE).

Nous avons également un rôle d'audit et de contrôle du respect des lois et règlementations, garantissant le secret de la défense nationale. En 2020, plus de 130 inspections ont ainsi été effectuées dont 85% en milieu industriel.

Dans le contexte actuel de crise sanitaire, « l'industrie de défense est dans l'œil du cyclone ». Cette phrase est tirée de l'excellent rapport

d'information n° 605 (2019-2020) de messieurs Pascal Allizard et Michel Boutant, fait au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, déposé le 8 juillet 2020.
Conjugué à l'explosion du cybercrime, c'est notre écosystème de défense qui est structurellement menacé. Nous avons par conséquent engagé des travaux de transformation de notre mission historique de contrôle règlementaire vers une logique démultipliée de connaissance partagée des failles et vulnérabilités et des menaces, de conseil, pragmatique basé sur des cas réels, et d'assistance à la maîtrise du risque numérique.

Cette maîtrise du risque et le renforcement des fondamentaux de la cybersécurité, les bonnes pratiques d'hygiène informatique sont des prérequis au bon fonctionnement des entreprises en temps normal. Ils ne suffiraient probablement pas à éviter des bataillons de cyberattaquants de niveau étatique mais cela permettrait de se relever, de redémarrer plus rapidement et plus facilement après la tempête.
Par ailleurs, dans le cadre de la convention cyberdéfense signée par le ministère des Armées et 8 grands maitres d'œuvre industriels, un travail conséquent a été accompli sur le volet capacitaire aboutissant à la constitution d'un groupe sectoriel des CSIRTs de défense doté de règles de gouvernance et d'outils de partage communs.

Cette phase de développement capacitaire est suivie par une phase de préparation opérationnelle, de formation et d'entrainement aux opérations de cybersécurité au profit de l'ensemble de l'écosystème de défense, des plus forts aux plus fragiles. La DRSD entend bien assumer ses responsabilités aux cotés de l'ANSSI pour ce qui concerne les OIV de défense et sur l'ensemble des 4000 TPE/PME/ETI de la BITD.

Avis de tempête

A l'opposé des prévisions météorologiques, il n'existe pas à ce jour de modélisation prédictive des attaques dans le cyberespace à l'échelle mondiale ou nationale.

Pour autant, certaines manœuvres de groupes malveillants peuvent être

observées et concourir à anticiper des postures d'attaque. Cette connaissance des menaces, plus ou moins focalisées, plus ou moins stratégiques, est partagée dans des cercles restreints d'analystes et experts en cybersécurité du secteur public et du secteur privé, en France, en Europe et dans le monde. La consolidation et le partage de ces données techniques sur les cybermenaces que l'on appelle communément « *CTI - Cyber Threat Intelligence* » permettrait de mieux anticiper les attaques et par conséquent d'être en mesure de produire des avis de vigilance cyber voire des avis de tempête transcendante sur le cyberespace. L'objectif est d'avoir et de partager une vision plus large et exhaustive de la menace.

Comment venir au secours des victimes les plus fragiles ?

L'enjeu premier n'est pas de comprendre les causes, mais de pallier les conséquences déstabilisant l'organisation sociétale.

Il s'agit donc pour les décideurs face à une catastrophe naturelle de masse, de classer, prioriser et coordonner l'action des services de secours spécialisés, qui dans l'assistance aux personnes, qui dans la réparation de services vitaux, qui dans la logistique ou l'acheminement des moyens de secours matériels et humains, etc.

En matière cyber l'approche est très comparable. Le secrétariat général de la défense nationale (SGDSN) dans la dernière revue de la stratégie nationale de cyberdéfense[4] a introduit le concept de classement des attaques informatiques selon la gravité de l'événement de 0 à 5. Cet outil d'aide à la décision a été adopté par l'ANSSI, le COMCYBER et de nombreux CSIRTs en France.

Il est désormais intégré dans la doctrine d'engagement des éléments d'intervention cyber de la DRSD (cf. infra). Au-delà de son usage collectif à l'échelle nationale, il permet de construire une vision partagée de la situation opérationnelle cyber dans l'union européenne et devrait favoriser la collaboration internationale de réponse à incident majeur. En ligne avec la LPM 2019-2025[5], le renforcement capacitaire de notre direction est continu ; notre effectif a augmenté passant de

1330 agents en 2018 à plus de 1500 agents en 2020, dont 30% de femmes, 32% de civils.

40 postes supplémentaires du domaine cyber sont à pourvoir d'ici 2025.

Le renforcement capacitaire porte notamment sur la mise en place d'une capacité de réponse aux compromissions de systèmes numériques : l'élément d'intervention cyber (EIC).

Cette force d'intervention actuellement positionnée auprès de notre SOC (Security Operation Center)[6] en région parisienne constitue l'élément fondateur du CERT DRSD. Cette capacité sera progressivement développée dans l'ensemble de nos directions en régions au gré de recrutements d'ingénieurs et techniciens cyber et de formations dispensées par notre propre centre de formation ou par des prestataires spécialisés. Cette capacité de primo intervention de proximité et la combinaison d'expertise métiers ou techniques, est une des clés de la réponse aux cyberattaques du quotidien.

En cas d'agression d'ampleur, elle serait mobilisée aux côtés des autres services de l'État à l'échelon interministériel et au niveau des zones de défense et sécurité pour répondre le plus efficacement possible aux nombreuses demandes d'assistance des victimes sur l'ensemble du territoire national et pour appuyer la phase de reconstruction éventuelle des lignes de défense.

Cette organisation générale repose sur la disponibilité d'outils critiques de communication, communs ou interopérables, assurant une circulation fluide de l'information. De ce point de vue, nous pouvons dire que la crise du COVID aura été un accélérateur de modernisation de ces outils de communication et de partage rapide. Il n'en reste pas moins que certains outils restent propres à certains services de l'État comme c'est le cas à la DRSD et c'est une force en soit car la redondance de plateformes numériques prendrait tout son sens si une autorité venait à être impactée par le cataclysme d'origine cybernétique.

Quid de la coopération européenne ?

L'ancien chef du CERT-FR de 2017 à 2019, représentant la France dans le réseau des centres de cybersécurité nationaux de l'UE - le *CSIRT Network* - me disait combien la construction de la cyberdéfense européenne avait drastiquement progressé en quelques années au bénéfice des services essentiels tels que définis par la première directive SRI[7] - *NIS directive* - malgré les différences historiques ou culturelles des approches nationales.

La prochaine mouture de cette directive NIS, au spectre sectoriel élargi, la création officielle fin 2020 du réseau CyCLONe (Cyber Crisis Liaison Organisation Network)[8] sont la suite logique du travail de coopération des États membres pour se préparer et répondre en cas d'incident cyber d'ampleur ou de crise transfrontalière. Gageons que CyCLONe et l'ensemble des cyberforces vives en France seront suffisamment puissants pour faire face, unis, aux attaques tempétueuses contre nos services essentiels voire vitaux !

Pour une « Boussole stratégique » cybersécurisée

Cette dynamique de coopération cyber du domaine civil transnational gagnerait à être instillée au domaine des activités de défenses domestiques, très souvent souveraines alors même que nos champions industriels ont de leur côté noué de nombreux partenariats à l'international, et que la structuration d'une défense européenne progresse. Un potentiel axe de réflexion pour le volet cyber de la prochaine présidence française du conseil de l'UE.

Parution le 3 septembre 2021

[1] https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cyber-espionage-ebook-en-fr.pdf
[2] BITD - Base industrielle et technologique de défense.
[3] TESSCO - Terrorisme, espionnage, subversion, sabotage, crime organisé.
[4] SGDSN - Revue nationale de cyberdéfense - 12 février 2018.
[5] LPM - Loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025.
[6] SOC - Le centre opérationnel de sécurité assure la supervision des systèmes d'information au sein d'une entité afin de se protéger des cyberattaques.
[7] La loi française de transposition de la directive européenne 2016/1148 de sécurité des réseaux et de l'information (Network and Information Security - NIS) du 6 juillet 2016 a été promulguée lundi 26 février 2018.
[8] CyCLONe - Réseau de coopération stratégique des Etats membres de l'union européenne.

Assurance Cyber : prendre le point de vue de l'assureur pour améliorer sa posture cybersécuritaire

ÉRIC VAUTIER
RSSI
Groupe Aéroports de Paris

De manière assez inattendue, la cyber-assurance suit le fameux « hype cycle de Gartner », d'ordinaire appliqué aux technologies : après une phase de lancement plutôt réussie ces dernières années, elle semble être au fond DU "Gouffre des désillusions", peu de temps après la déclaration de Guillaume Poupard[1] sur le "jeu trouble de certains assureurs", qui, en couvrant le paiement des rançons, encourageraient involontairement les cybercriminels à s'attaquer aux entreprises assurées. Si l'argument fait mouche, ne fournit-il pas aussi aux assureurs un bon prétexte pour revisiter des clauses qui furent peut-être établies légèrement et dont les effets pécuniaires se firent sentir dès l'attaque NotPetya[2] ?

Il nous semble donc intéressant de profiter de cette phase de flottement pour réfléchir à un usage pertinent de la cyber-assurance par les RSSI (Responsable de la Sécurité des Systèmes d'Information), entre le parapluie qu'on ouvre à la première attaque réussie et la police inapplicable tant il y a de clauses d'exclusion, pour établir de vraies relations de confiance et, espérons-le, gravir la "Pente de l'Illumination".

A la lecture de ce qui suit, certains RSSI pourront nous taxer d'angélisme, voire de parti-pris, tant l'argumentaire qui suit penche en faveur des assureurs. Il est évident que la réalité est plus nuancée. Certaines clauses sont encore suffisamment absconses pour que des contentieux comme celui de Merck

puissent exister, ce qui jette un voile de défiance sur l'ensemble du sujet. Finalement, les RSSI ne devraient-ils pas adopter résolument les réflexes d'un assureur - imaginer le pire en ne parlant que d'argent - sans pour autant oublier de lire très attentivement les fameuses "petites lignes" du contrat ?

Imaginer le pire

Pour l'entreprise, mener son analyse de risques cyber est finalement assez simple : on liste des événements redoutés et on ne conserve que les plus probables à fort impact. Puis on en tire des plans d'action pluriannuels : pour le Métier, ce sera d'essayer de diminuer l'impact de l'incident ; pour la DSI, ce sera de mettre en œuvre des protections pour baisser la probabilité ; et pour les deux conjointement, de prévoir les plans de continuité et de reprise. Ainsi, on obtient une cartographie des risques résiduels qui satisfait toutes les parties, y compris la Direction Générale de l'entreprise.

L'assureur, de son côté, va se saisir de la cartographie des risques bruts et retenir les scénarios qui vont représenter les coûts les plus importants (pertes d'exploitation, coûts de remise en service, dédommagements des tiers, etc.), puisque, dans le pire des cas, c'est ce montant qu'il faudra verser à son client - sans la franchise.

Cette différence d'approche - minimiser en considérant les contre-mesures versus maximiser en faisant l'hypothèse qu'elles ne fonctionneront pas - crée une incompréhension entre les assureurs et les RSSI qui admettent difficilement que les mesures de protection puissent ne pas être efficaces. Ce côté émotionnel, finalement inattendu dans ce contexte, engendre de facto un biais dans l'évaluation des risques. L'assureur, extérieur au sujet et analysant à froid les éléments, apporte finalement un regard plus réaliste et donc plus pertinent.
Dans cet exercice de définition du contrat de cyber-assurance, il nous apparaît donc préférable de partir des risques bruts et de quantifier les coûts globaux en imaginant le pire.

Ne parler que d'argent

Sans trahir de secrets corporatistes, il existe des biais dans la gestion du

risque : l'appréciation des impacts et/ou de la vraisemblance fait l'objet de débats parfois houleux où les arguments ne sont pas toujours de bonne foi : on peut délaisser un domaine historiquement complexe ou à l'inverse privilégier un domaine de sa zone de confort, au détriment finalement du "vrai" risque. En se focalisant sur le coût, on objective le débat - on peut bien sûr ergoter sur le montant final mais, si on l'a sous-estimé, il faudra assumer le jour de l'évaluation des dégâts.
La discussion avec l'assureur peut ainsi aider à estimer un retour sur investissement des mesures qu'on souhaite mettre en œuvre en corrélant une mesure à une diminution de la prime. La franchise quant à elle, utilisée intelligemment, peut équivaloir à un seuil de criticité et aider à la sélection des risques que l'on doit traiter.
Autre avantage de cette approche : sortir de la pensée technologique. Sans trop tomber dans la caricature, la volonté de tout connecter est parfois l'expression d'une forme de facilité managériale : au lieu de fournir deux écrans ou deux téléphones, on va vouloir tout placer sur le même appareil, en faisant souvent cohabiter des environnements de criticités différentes et donc en affaiblissant les mesures de sécurité du plus critique. La meilleure solution est souvent de simplement supprimer ces interconnexions. Ce choix ne sera pas gratuit puisque l'on dégrade probablement l'efficacité opérationnelles des utilisateurs, notion d'ailleurs très difficilement quantifiable.

Les "petites lignes" de bas de page

Même si elles n'existent plus depuis longtemps, il subsiste dans l'imaginaire collectif que tous les contrats d'assurance comportent des lignes de bas de page, écrites en petits caractères et listant des clauses permettant de ne pas payer ce que l'assuré pensait percevoir. Étonnamment, les politiques Sécurité pourraient parfois en remontrer à ces contrats d'une autre époque. Pas de petites lignes certes, mais des exceptions à la règle pas toujours si connues : "tous les PC sont sécurisés sauf dans telle entité", "tous les utilisateurs ont une authentification forte sauf les VIP", etc. Ces exceptions, souvent fruits d'impossibilités techniques dues à un historique ou de complexités politiques difficiles à faire disparaître, fragilisent à la fois le système d'information et la position du RSSI.
Pour l'assureur, ce sont justement dans ces zones grises que se trouvent fort

probablement les causes des incidents futurs, et il voudra donc logiquement obtenir un inventaire exhaustif avant de proposer un contrat. Là encore, ce regard externe doit pousser l'entreprise à se poser les bonnes questions sur le périmètre à assurer : est-il raisonnable d'assurer un périmètre au niveau de sécurité incertain, en sachant que l'on ne saura pas démontrer à l'assureur la mise en œuvre des bonnes pratiques ? A l'inverse, l'identification de ces zones "non assurables" peut permettre une prise de conscience et déclencher un vrai plan d'actions dont la réalisation est nécessaire pour les assurer.

Conclusion

Il apparaît donc évident que l'assureur, en posant les questions visant à estimer son propre risque financier à la signature d'un contrat, contribue à une meilleure appréciation par l'entreprise de ses cyber-risques, en imposant une quantification pécuniaire systématique de l'impact d'un incident. Cette meilleure appréciation, couplée à une mesure précise de l'efficacité supposée des actions de réduction des risques, favorisera l'établissement de plans d'actions plus pertinents.
Ces éléments nous semblent les bases indispensables pour engager des négociations contractuelles permettant à chacun de remplir au mieux son rôle : d'un côté, l'entreprise qui se doit d'assurer la résilience en cas d'incident de cybersécurité et de l'autre, l'assureur accompagnant son client dans la couverture de ce nouveau type de sinistre.
La cybersécurité s'est aujourd'hui débarrassée de sa réputation de sujet purement informatique - et c'est heureux - mais les RSSI continuent encore trop souvent de raisonner en informaticiens. Nous devons résolument nous ouvrir aux autres expertises, en commençant par celle des assureurs, la résilience de nos entreprises n'en sera que meilleure.

Parue le 10 septembre 2021

[1] http://videos.senat.fr/video.2251670_60761aa01efc4.table-ronde-sur--la-cybersecurite-des-eti-pme-tpe--la-reponse-des-pouvoirs-publics-?timecode=1101000
[2] NotPetya : Merck bataille avec les assureurs pour 1,3 Md $ d'indemnisation - Le Monde Informatique

Cybersécurité comportementale à travers les enjeux et spécificités des collectivités territoriales :l'intérêt d'une cyber-culture individuelle et collective

ASTRID FROIDURE
Chargée de Relations Publiques
Avant de Cliquer

Au cœur de l'évolution numérique, les collectivités territoriales se retrouvent dans un process de transformation accéléré depuis une dizaine d'années. Indispensable pour s'adapter à la vie quotidienne des citoyens comme pour mener les projets les plus ambitieux, le « chantier du numérique » est certainement le plus stratégique pour les organisations publiques.

Echanges dematerialises avec les citoyens, les acteurs économiques et autres administrations publiques, e-administration, sites interactifs, communication réseaux… les interfaces numériques se sont multipliées. Dans le même temps, bien que les bénéfices de ces évolutions soient considérables, les collectivités sont aussi devenues des cibles d'attaques informatiques de plus en plus nombreuses (fragilité des systèmes d'information, faible acculturation numérique, mauvaise prise en compte des menaces). L'improvisation du recours au télétravail face à la crise du Covid 19, a ouvert un grand nombre de brèches sécuritaires, facilitant les attaques des hackers.

Hameçonnage, déni de service, piratage de compte, vol de données, défiguration de site, rançongiciels, la menace est quotidienne. Parmi les 70 victimes déclarées officiellement en 2020, on trouve des collectivités de toutes tailles, de la métropole d'Aix-Marseille-Provence à des petites villes de l'Oise. Qu'il s'agisse de défaçages, c'est-à-dire une intrusion sur le site web pour en modifier le contenu ; d'attaques par rançongiciels, aux conséquences souvent

désastreuses ; de minages, c'est-à-dire l'utilisation des ordinateurs de la collectivité pour fabriquer des crypto-monnaies ou d'autres encore, comme le cheval de Troie Emotet qui ouvre une porte dans l'infrastructure pour faciliter les utilisations frauduleuses... l'ampleur des conséquences est proportionnelle à la qualité de l'anticipation des cyberattaques.

Ces attaques constituent de véritable menace pour le fonctionnement global des collectivités locales. Le chiffrement des données peut bloquer l'accès aux systèmes d'informations des services pendant plusieurs jours, voire plusieurs semaines. Au-delà de l'empêchement des agents d'accéder à leur outil de travail, elle conduit à une restriction massive des services disponibles pour les utilisateurs. Elles impliquent également un coût financier conséquent (redéploiement des terminaux, modification des serveurs, pertes des données) dans un contexte de diminution importante des budgets. La réputation est aussi impactée par une décrédibilisation de la collectivité auprès de sa population, mais également auprès des partenaires publics et privés. Enfin, ces attaques entrainent nécessairement des procédures juridiques longues et fastidieuses, notamment en l'absence de plan de continuité et de reprise d'activité.

Les collectivités publiques : nouvelles cibles privilégiées

Les cyberattaques se déplacent de plus en plus vers les organisations publiques, collectivités territoriales, structures hospitalières, détentrices de volumes importants de données confidentielles et porteuses des services essentiels pour les citoyens français. Elles sont devenues, en quelques années, les cibles privilégiés pour trois raisons majeures :

Un service public empreint de bienveillance
Tout d'abord, fondamentalement, les collectivités territoriales, comme les établissements hospitaliers, répondent aux caractéristiques de service public : entraide, solidarité, secours. Agents comme élus, mués par ces valeurs, rencontrent des difficultés à imaginer des attaques dommageables à leurs missions d'intérêt général. De surcroît, les cyberattaques ayant d'abord visé les entreprises, les organisations publiques concentrées sur leur transformation numérique accélérée ont principalement axé leur mutation sur les aspects techniques et matériels au service des publics sans toujours réaliser le danger.

Des inégalités de territoire croissantes face au numérique
La disparité des collectivités locales complique la mise en place d'un process de sécurité unifié. Or les inégalités entre les territoires français s'accentuent. Les territoires intégrés à la mondialisation concentrent les interactions économiques nécessitant un développement numérique fort. Les régions littorales, à l'ouest et au sud du pays, sont attractives et profitent de leur interface pour développer les échanges. Par exemple, les zones industrialo-portuaires (ZIP) de Dunkerque ou du Havre, ouvertes sur la Northern Range, s'imbriquent dans une nécessaire modernisation numérique des collectivités locales de ce territoire. Les régions frontalières du territoire sont également connectées à la mondialisation par l'intensité des échanges transfrontaliers.

Les inégalités entre les collectivités territoriales tendent à s'accélérer depuis les dernières réformes territoriales (Loi MAPTAM, et Loi NOTRe notamment) accompagnant le mouvement de métropolisation. L'avenir favorable aux métropoles concentrant emplois, économie et services accentue la fragilité des villes moyennes et des zones rurales (France Stratégie).

L'accès et l'utilisation des nouvelles technologies numériques, les inégalités entre territoires s'accroissent proportionnellement aux ressources tant techniques (infrastructures réseaux, équipement…) qu'humaines (services informatiques avec personnels dédiés : DSI, RSSI, DPO…).

Des élus et des agents non sensibilisés et formés aux cyberisques
La nature même des collectivités territoriales, leur fonctionnement démocratique et le principe électif consubstantiel aux collectivités locales françaises impliquent plus de 520 000 élus locaux. Ces élus aux parcours divers et singuliers sont faiblement sensibilisés à la sécurité informatique.
La pression de la transformation numérique conduit à voir cette évolution comme un moyen performant d'amélioration des services, sans pour autant bien assimiler les risques qu'ils impliquent.

Souvent mal accompagnés pendant le début de leur mandat, élus, comme fonctionnaires, subissent de plein fouet les fractures numériques du territoire. Au-delà des grandes collectivités dotées d'un service informatique et malgré l'évolution sociétale, les petites collectivités s'équipent et s'organisent souvent

proportionnellement au niveau de l'utilisation personnelle des outils numériques par ses dirigeants. Infrastructure, équipement, sécurité informatique, formation, deviendront ou non prioritaires lors des débats budgétaires.

De la sécurité informatique à la cybersécurité comportementale

Proportionnellement au développement d'un arsenal technique en matière de sécurité numérique reposant sur des systèmes de sécurité supervisés par des équipes informatiques, la vulnérabilité humaine est devenue la faille la plus évidente des organisations. Du fait du facteur humain, il est nécessaire de renforcer la stratégie cyber autour de la sensibilisation et de l'apprentissage. L'apparition du concept de sécurité comportementale est récente en France. Il est né d'un constat simple : malgré toutes les sécurités techniques et organisationnelles, des cyberattaques parviennent tous les jours à paralyser, rançonner voire anéantir le fonctionnement des organisations françaises.

Le couple ransomware / phishing représente plus de 80% des cyberattaques françaises et tant l'ensemble des organisations publiques et privées que les citoyens, deviennent potentiellement une cible pour les hackers. Les courriels d'hameçonnage sont de plus en plus sophistiqués, les données les plus anodines convoitées pour les intégrer dans des mails crédibilisés par de « vraies » informations récupérées aisément sur les réseaux sociaux ou dans l'actualité. Il devient ainsi de plus en plus difficile de distinguer un mail malveillant d'un mail authentique.

La mise en place d'une culture organisationnelle et comportementale devient incontournable face à cette évolution afin que tous puissent acquérir les réflexes nécessaires à la protection de la collectivité. Une responsabilité collective s'installe reposant sur une nouvelle transversalité : nous ne sommes jamais trop petit pour être victime et la nouvelle campagne de l'Agence du Numérique en Santé « TOUS CYBERVIGILANTS ! » s'applique totalement aux collectivités territoriales.

Ainsi renforcer le pouvoir défensif des collectivités va impliquer plusieurs notions complémentaires :

• contribuer à une prise de conscience du rôle, à la fois individuel et collectif, de tous les agents et élus, quelles que soient leurs missions et compétences, en matière de cybervigilance ;

• intégrer élus et agents dans une mobilisation générale afin de protéger leur outil de travail et les données récoltées en associant sensibilisation, connaissances et responsabilités ;

• apprendre à communiquer tant vers la collectivité que ses partenaires, associations, prestataires, citoyens sur ces nouvelles menaces pour expliquer, rassurer et les accompagner dans une culture de cybersécurité partagée.

Installer une culture préventive forte peut s'appuyer sur différents outils mêlant habilement formation et communication. On pourrait penser qu'un grand séminaire de sensibilisation incluant tous les agents et élus pourrait déclencher une dynamique vers l'attitude de prophylaxie attendue.

Selon le rapport « Building a Cyber Smart Culture » réalisé par Fujitsu, il est important dans ce contexte particulier, d'intégrer une approche différente de la formation. L'objectif n'étant pas seulement de diffuser des connaissances mais d'acquérir des réflexes de cybersécurité.

Ainsi le rapport souligne qu'une bonne formation de sensibilisation se concentre sur deux aspects fondamentaux.

Le premier est le changement de comportement : motiver les gens à penser et à agir différemment. Ce type de formation doit reconnaître que les différentes sections des salariés, agents, élus sont motivées de différentes manières.

Le deuxième aspect d'une bonne formation de sensibilisation est l'intégration par la formation des gestes qui sauvent et des comportements à adopter selon les cas. Lorsque les employés sont confrontés à des tentatives d'hameçonnage, ils doivent immédiatement savoir ce qu'ils doivent faire, ce qu'ils ne doivent pas faire et qui ils doivent informer. En résumé « une formation innovante et interactive sur les problèmes que les employés rencontrent dans leur contexte personnel est susceptible d'obtenir un fort engagement ».

Face à ce constat, des outils se développent, portés par les entreprises spécialisées du monde numérique qui essaient d'intégrer de plus en plus des solutions de sensibilisation à la cybersécurité à leurs prestations.

Les outils de la cybersécurité comportementale

La première étape consiste à réaliser un audit de vulnérabilité afin d'évaluer la résistance collective et individuelle. Quelles que soient les structures, publiques ou privées, le service concerné ou la sociologie des utilisateurs, le taux de vulnérabilité face à des attaques dites « de masse » (non personnalisées pour l'établissement) est en moyenne de 24% sur les structures n'ayant pas mis en place de programme spécifique de cybersécurité comportementale.

Réalisé de manière impromptu, avec des caractéristiques prédéterminées conjointement avec les responsables des services informatiques, un audit consiste à envoyer de « faux mails de phishing » à tous les utilisateurs : élus et agents, sur une durée déterminée avec un degré de difficulté croissant. Les clics malencontreux les rassureront en les informant qu'il s'agit d'une évaluation globale de la vulnérabilité de la structure.

Au-delà de l'établissement d'un référentiel de base sur la vulnérabilité de la structure, les résultats de cet audit font généralement l'effet d'un électrochoc pour les dirigeants lorsqu'ils réalisent que près d'un quart des utilisateurs cliquent sur un mail imitant un mail malveillant lors d'un audit d'une semaine.

Les méthodes de sensibilisation à la cybersécurité

Elles sont nombreuses et en pleine évolution.
Ainsi on distinguera :

Les actions de formation en présentiel
Que ce soit sous forme de journée(s) de formation ou de séminaires d'équipes, voire de séminaires annuels permettent une interaction directe avec les formateurs et intervenants avec des réponses immédiates aux questions et un partage d'expérience. Accompagnées d'une gestion logistique

et administrative importante, elles mobilisent les collaborateurs en impliquant une organisation de continuité d'activité. Les coûts directs et indirects s'additionnent. La complexité pour les collectivités est particulière car leurs engagements en matière de formation sont principalement noués avec le CNFPT (Centre National de la Fonction Publique Territoriale) avec des modules de formations indépendants dispensés sur des temps limités. Importants sur la dimension technique et de sensibilisation, leur impact est cependant limité par l'approche forcément généraliste de la problématique cyber face à une menace de plus en plus ciblée et personnalisée des attaques par phishing.

Le e-learning ou formation en ligne
De nombreux modules de formation permettent d'accroitre les connaissances sur la cybersécurité. Solution flexible, asynchrone, le e-learning permet d'assister à la séance à l'endroit et au moment de son choix. Il n'est malheureusement pas adapté à tous les publics car il nécessite, au-delà d'une certaine pratique du numérique, rigueur, autonomie, et de savoir s'auto-évaluer. Aussi, il est parfois difficile d'obtenir l'adhésion de tous dans la pérennité. Leur prix est variable et va dépendre de l'outil utilisé et de la personnalisation possible pour la collectivité. Certains MOOC de sécurité numérique ont été réalisés par les structures de l'Etat comme le MOOC de l'ANSSI ou celui de la CNIL et sont mis à disposition gratuitement sur leur site. Des plateformes spécifiques de e-learning se développent de plus en plus. Proposées en complément des outils techniques par de nombreux opérateurs, certaines entreprises ont choisi de développer des plateformes de e-learning modulables en fonction des spécificités des utilisateurs.

Les outils de communication visuelle
Affiches, écrans de veille permettent à la fois de rappeler les bonnes pratiques et de donner les consignes en cas d'alerte : premiers gestes, coordonnées du service informatique… Le kit de sensibilisation de Cybermalveillance étant particulièrement adapté aux collectivités.

Des guides et livrets utilisateurs
La mise à disposition de guides ou de livrets spécifiques pour les utilisateurs et notamment remis aux nouveaux arrivants, accompagne de plus en plus les prises de poste. Certains sont spécifiques pour les collectivités territoriales

comme celui élaboré par l'ANSSI avec l'AMF et nombreux destinés initialement aux entreprises sont aussi adaptables aux collectivités (Cybermalveillance, Medef, Gendarmerie nationale…).

La formation par le jeu
La formation par le jeu, comme les serious-games ou les escape-games, se développe souvent en parallèle des formations professionnelles ou des plateformes d'e-learning. Plus ludiques, elles permettent de mettre l'utilisateur dans différents contextes et abordent aussi les notions de sécurité physique et économique.

Des campagnes de phishing régulières
Les campagnes de phishing régulières sont parfois instaurées dans l'objectif de garder en alerte les utilisateurs. Souvent accompagnées d'une plateforme d'e-learning, ces campagnes sont alors répétées annuellement ou semestriellement. Elles permettent de réaliser une photographie de la vulnérabilité cyber à un instant T et de suivre son évolution au fil du temps. Malheureusement, leur effet est temporaire, sans accompagnement par une formation associée pour permettre de développer des réflexes de cybersécurité.

La sensibilisation sur poste de travail
Elle consiste à envoyer régulièrement des mails d'apprentissages imitant une cyberattaque par phishing. Lorsqu'un utilisateur clique malencontreusement sur un mail, une page d'information (ou une mini vidéo) va s'ouvrir afin de lui expliquer comment il aurait pu déjouer l'attaque et ce qu'il aurait dû vérifier avant de cliquer. Certaines sociétés ont développé plusieurs degrés d'attaques spécifiques : de l'attaque de masse aux attaques personnalisées en s'inspirant de mails réels internes à la structure ou à son environnement de travail. Au-delà de la pédagogie par l'action, l'intérêt de cette méthode d'apprentissage est une mise en place pour tous les agents, même en télétravail.

Le bouton d'alerte phishing
Ce bouton est installé sur la barre d'outils des messageries des utilisateurs. Il permet lorsque ceux-ci détectent une attaque de transférer directement le mail suspect au service informatique qui sera alors en capacité d'analyser les attaques et de prendre les mesures appropriées. Son utilisation entraine un

écran de félicitations qui va entretenir la culture de veille cyber et développer le sentiment d'appartenance pour protéger la collectivité.

Certaines sociétés comme « Avant de Cliquer » se sont spécialisées pour développer une culture de cybersécurité pérenne. Elles mettent en place un programme complet avec tous les outils existants : audit, rapport de vulnérabilité, plateforme de e-learning, outils de communication visuelle et bouton d'alerte cyber en les interfaçant entre eux afin d'optimiser l'acquisition de réflexes pérennes. De plus, les décideurs et services informatiques ont un tableau de bord permettant de suivre l'évolution de la vulnérabilité de leur collectivité tout en évaluant les risques d'attaques.

Parce que les attaques par phishing constituent plus de 80% des cyberattaques et que dans une collectivité, comme dans une entreprise, chaque élu, chaque agent, a une boite mail, la cybersécurité est devenue l'affaire de tous. Quelle que soit la personne qui aura cliqué sur un courriel malveillant, l'impact sera le même. Sans oublier que la responsabilité de chacun pour protéger la collectivité s'étend bien au-delà par l'interconnexion avec l'ensemble du territoire, associations, entreprises, citoyens.

Devant l'inégalité structurelle des territoires tant en compétences qu'organisationnelle, il semble évident que la mutualisation des services informatiques doit devenir une priorité pour les petites collectivités. Est-ce au cœur des EPCI qui rencontrent les mêmes difficultés que des collectivités de taille moyenne ou les PME à recruter des RSI et à former leurs équipes, ou plus largement au sein des Centres de Gestion Départementaux qui gèrent déjà les services de ressources humaines, archives, remplacements, des « petites » collectivités territoriales ? La dynamique de l'Etat, notamment avec le Plan France Relance, joue le rôle d'accélérateur à la fois de soutien vers des projets concrets et de prise de conscience par les élus de la réalité des menaces.

L'implication des dirigeants, élus, DGS, responsables juridiques et de service informatique, doit se matérialiser par une anticipation de leur sécurité. Développer une culture de cybersécurité n'est pas une dépense, c'est un investissement. La cybersécurité devient un enjeu majeur de management et de direction pour réussir à transformer le maillon faible en un maillon fort. Comme le relève Cybermalveillance dans son rapport d'activité 2020, la

sensibilisation est la première arme contre les cyberattaques. La cybersécurité doit ainsi dépasser la formation individuelle pour intégrer le socle de la culture territoriale pour tous, agents comme élus, avec des outils spécifiques, innovants, inscrits sur la durée, permettant de mettre en place une cyberculture territoriale pérenne.

Quelques références :

- Les collectivités face aux enjeux de cybersécurité / ANSSI
- Rapport d'activité 2020 – Kit de sensibilisation aux risques numériques / Cybermalveillance
- L'essentiel de la sécurité numérique pour les dirigeants et les dirigeantes / Challenge
- Quels sont les axes majeurs pour lutter contre les cyberattaques ? / L'usine digitale
- Cybersécurité : comment former les télétravailleurs pour réduire les vulnérabilités comportementales / IT Social
- Vigilance face aux cyberattaques : les collectivités sont toutes concernées ! / Cybermalveillance
- "Au moins 4% des communes françaises ont été piratées en 2020" Jérôme Notin – Cybermalveillance / Journal Du Net
- Le rapport Fujitsu sur la cyberculture

Parue le 17 septembre 2021

Améliorer la sécurité numérique : une urgence absolue pour nos démocraties. Les recommandations de la Commission supérieure du numérique et des postes

MIREILLE CLAPOT
Députée de la Drôme
Présidente de la CSNP

Les attaques informatiques d'origine criminelle ou initiées par des Etats ou des groupes terroristes se sont multipliées à un rythme quasi-exponentiel ces deux dernières années et révèlent la fragilité de nos démocraties face à ces formes d'attaques, qui ne sont pas nouvelles, mais qui revêtent désormais une ampleur sans précédent.

Nous avons tous conscience que les moyens pour parer ces attaques doivent être renforcés, notamment ceux déployés par les collectivités locales et établissements publics insuffisamment préparés jusqu'à présent, mais nous savons également que les cybercriminels auront toujours « un coup d'avance » et que la sécurité numérique absolue n'existe pas.

C'est dans ce contexte que les membres de la Commission supérieure du numérique et des postes ont accueilli les annonces du plan d'accélération cyber annoncé par le Président de la République le 18 février dernier.

Pour les membres de la CSNP, le renforcement des moyens - 1 milliard d'euros dont 720 millions de financements publics – et la mise en place de nouveaux dispositifs, le site cybermalveillance.gouv.fr et le cybercampus par exemple, vont dans le bon sens.

Mais pour notre commission transpartisane, composée de 7 députés, de 7

sénateurs et de 3 personnalités qualifiées, il nous est apparu, après avoir conduit un certain nombre d'auditions et rencontré des experts reconnus dans ce secteur, qu'un changement de paradigme s'impose en introduisant une approche holistique de la sécurité numérique, en instaurant un véritable ordre public dans l'espace numérique et en posant les bases d'une souveraineté numérique nationale et européenne.

Ce constat nous a amené à formuler plusieurs recommandations dans un avis publié le 29 avril 2021[1].

Une approche holistique de la sécurité numérique

Pour les membres de la CSNP, la sécurité numérique ne peut plus être l'affaire des seuls experts mais passe par une véritable prise de conscience généralisée. La multiplication des attaques a *de facto* sensibilisé nos concitoyens, les collectivités locales, les établissements publics, nos PME-TPE à leur vulnérabilité dans l'espace numérique.

Cette sensibilisation accrue aux enjeux de sécurité numérique doit cependant être accompagnée par des réponses opérationnelles.

La CSNP préconise d'accélérer la diffusion et l'appropriation des solutions d'identité numérique régalienne par nos concitoyens (recommandation n°19) : il s'agit d'un passage obligé pour sécuriser les démarches en ligne. Elle doit naturellement s'accompagner de communication adaptée selon les publics.
Pour le renforcement de la sécurité numérique dans les territoires, la CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale afin de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques. (Recommandation n°9).

Pour les acteurs privés, et particulièrement pour nos PME-TPE, nous préconisons des mesures incitatives afin d'encourager les entrepreneurs à intensifier leurs investissements dans la sécurité numérique de leur organisation et de leurs outils de production : il paraît opportun de mettre en place des mesures d'incitation fiscale sous la forme de suramortissements

des investissements en sécurité numérique et/ou un crédit d'impôt sur les dépenses et investissements engagés dans ce domaine (Recommandation n°16).

Enfin, il nous faut dépasser rapidement l'incantation pour mettre en place le plus rapidement possible les bonnes pratiques aux niveaux individuels et collectifs. Cela suppose une volonté politique et la mobilisation de plusieurs départements ministériels et administratifs. Ce pilotage est essentiel du point de vue de la CSNP.

Vers un ordre public renforçant la sécurité numérique des biens et des personnes

De la même manière que l'Etat se doit de mettre en œuvre un ordre public assurant la sécurité physique des biens et des personnes, il apparaît urgent que l'Etat se dote des moyens nécessaires pour renforcer la sécurité numérique de nos concitoyens et de leurs biens.

C'est la raison pour laquelle nous nous référons dans notre avis à la notion de sécurité numérique plutôt qu'à la notion plus restrictive de cybersécurité.

En premier lieu, cette dimension numérique de l'ordre public suppose un renforcement significatif des moyens judiciaires et policiers dans le domaine de la sécurité numérique (Recommandations 1 à 5).

Depuis la publication de notre avis, plusieurs mesures ont été annoncées pour renforcer les moyens de la police et de la gendarmerie dans le domaine de la cybersécurité et nous nous en félicitons. Ainsi, depuis le 1er août, le commandement de la gendarmerie dans le cyberspace ComCyberGend pose le premier jalon d'un service cyber mixte réunissant police et gendarmerie chargé de lutter contre la cybercriminalité.

Cependant, nous constatons que le renforcement des moyens judiciaires et la création d'un parquet cyber n'est toujours pas à l'ordre du jour du ministère de la Justice et nous le regrettons.

Ce silence est d'autant plus regrettable que, depuis la parution de notre avis

en avril dernier, notre proposition de renforcer les moyens judiciaires et de créer un véritable parquet cyber européen a été accueillie très favorablement par l'écosystème. Notamment les entreprises qui ont subi des cyberattaques et ont tenté, avec de grandes difficultés, de mobiliser les services judiciaires pour des crimes et délits qui ont presque systématiquement une dimension internationale, estiment que la réponse judiciaire n'est pas à la hauteur des préjudices subis.

Au-delà du renforcement des services régaliens, nous avons appelé à l'introduction de normes de sécurité numérique pour les objets connectés et les services informatiques.
En effet, comment expliquer à nos concitoyens que la mise sur le marché de la plupart des produits que nous utilisons quotidiennement est soumise à des normes de sécurité françaises et européennes alors que les produits connectés et les services informatiques et numériques ne sont toujours pas encadrés par la moindre norme de sécurité numérique ?

Notre recommandation d'instaurer des normes minimales de sécurité numérique et d'introduire des normes de sécurité par conception, sur l'ensemble de la durée de vie des produits, en ligne avec les recommandations de l'OCDE, semble remporter l'adhésion des acteurs économiques et des utilisateurs. Nous souhaitons que les discussions aboutissent ou, à tout le moins, avancent rapidement au cours de la Présidence française de l'Union européenne.

A l'instar des normes de sécurité qui sont mises en place dans le secteur aéronautique, il nous semble que c'est toute la chaîne de fournisseurs et de sous-traitants qui doit être incluse dans le périmètre des normes de sécurité numérique que nous appelons de nos vœux.

Quelle souveraineté numérique dans un monde dominé par des acteurs extra-européens ?

La question de la souveraineté numérique se pose parce que les grands acteurs du numériques sont très largement extra-européens principalement américains et chinois.

Les membres de la CSNP ont émis plusieurs recommandations pour renforcer la filière industrielle spécialisée dans la sécurité numérique et faire émerger des champions français et européens. Ainsi nous recommandons d'utiliser plus largement le levier de la commande publique.

Nous proposons d'étudier si la directive du 26 février 2014 relative à la commande publique des opérateurs de réseaux doit être modifiée, notamment pour permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens.

Il nous semble qu'a minima, il conviendrait de définir que la cybersécurité entre dans le champ d'exclusion de l'application de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance européennes.

Cette proposition est favorablement accueillie au sein de l'écosystème cyber puisque le livre blanc du Think Tank stratégique du FIC, rendu public le 9 septembre dernier à Lille, reprenait peu ou prou cette proposition en recommandant l'adoption d'un Buy Digital European Act.

L'Union européenne doit se donner les moyens de sa souveraineté et favoriser l'émergence de champions européens de la cybersécurité.

Le ministère des Armées soutient activement les initiatives privées et les start-up prometteuses du secteur. Pour autant nous sommes encore loin de la « symbiose » que nous pouvons observer de l'autre côté de l'Atlantique, où les leaders de la tech américaine, la Maison blanche et la Cybersecurity and Infrastructure Security Agency ont annoncé il y a quelques semaines un accord pour renforcer, avec des moyens financiers conséquents, la lutte contre les attaques cyber.
Compte tenu du retard que nous avons pris sur nos partenaires internationaux, que ce soit dans la collecte de données, leur hébergement, les modes d'exploitation des systèmes informatiques et numériques, il serait

sans doute opportun d'appréhender différemment le concept de souveraineté numérique : l'autarcie en matière numérique est à court terme une illusion, les dépendances existeront, il faut les maîtriser.

Il ne s'agit pas de baisser les bras et de renoncer à une politique volontariste mais d'envisager de manière réaliste comment nous pouvons limiter les atteintes à la souveraineté nationale et européenne et comment l'Etat français et l'Union européenne peuvent exercer leur souveraineté dans l'espace numérique de manière crédible.

Parue le 24 septembre 2021

[1] Avis-n2021-03-du-29-avril-2021-portant-recommandations-sur-la-sécurité-numérique.pdf (csnp.fr)

Les technologies de sécurité sont pour la France un enjeu de souveraineté et une opportunité industrielle et économique

JEAN-MICHEL MIS
Député de la Loire,
Membre de la commission des lois
Membre du Conseil national du numérique
Membre de la Commission supérieure du numérique et des postes

Dans la continuité de mes travaux à l'Assemblée nationale sur les questions liées aux nouvelles technologies, et dans la continuité de mes engagements sur les questions de sécurité, et notamment comme rapporteur du projet de loi Responsabilité pénale et sécurité intérieure, voté cette semaine à l'Assemblée nationale, j'ai remis le 9 septembre dernier au Premier ministre mon rapport sur « l'utilisation des nouvelles technologies dans le domaine de la sécurité ».
Pour conduire mes travaux, et face au large champ des nouvelles technologies de sécurité, j'ai souhaité retenir une approche opérationnelle et pragmatique en définissant les usages qui semblent prioritaires.

Les technologies offrent, en effet, désormais de nouvelles opportunités aux acteurs publics dans le champ de la sécurité. Elles sont des outils qui peuvent aider l'action des forces, en leur fournissant une aide à la décision et un appui opérationnel dans une société toujours plus complexe.

Par ailleurs, les forces de sécurité sont confrontées à de nouvelles menaces qui reposent sur l'utilisation croissante du numérique. Il existe, de ce fait, un risque d'asymétrie entre les moyens des forces et ceux de leurs adversaires.
C'est la raison pour laquelle nous devons moderniser les outils des forces et leurs équipements, à la fois pour répondre à leurs besoins structurels mais

aussi en prévision des grands évènements sportifs que la France accueillera. Les grands évènements sportifs concentreront des enjeux forts en matière de sécurité qui doivent être anticipés en procédant à des expérimentations.
Il faut pour cela déterminer quelles sont les expérimentations qui auront lieu à droit constant et quelles sont celles qui doivent être autorisées par voie réglementaire ou législative, mais aussi ouvrir les crédits nécessaires à leur financement.

Les technologies de sécurité sont pour la France un enjeu de souveraineté et une opportunité industrielle et économique.

Nous disposons d'acteurs industriels de pointe dans le secteur de la sécurité qui sont pourvoyeurs d'emploi mais aussi de recettes à l'exportation. Le renforcement de notre base industrielle est un enjeu de souveraineté technologique afin de conserver notre autonomie dans la définition de nos choix stratégiques. Nous devons accompagner le développement de nos entreprises à l'international, mais aussi mobiliser plus largement l'investissement et la commande publics pour renforcer la filière française de sécurité.

Les cas d'usage doivent être déterminés au cas par cas et assortis de garanties strictes

Mais ces technologies soulèvent des enjeux majeurs pour les libertés et suscitent des craintes quand elles sont employées à des fins de sécurité.

Ces craintes portent sur la protection de la vie privée et des données personnelles. En particulier, le traitement des données biométriques et l'opacité associée à certaines technologies, comme l'effet « boîte noire » des algorithmes d'intelligence artificielle, font l'objet de préoccupations spécifiques.

L'emploi de ces technologies par les forces de sécurité n'est pas anodin et c'est la raison pour laquelle les cas d'usage doivent être déterminés au cas par cas et assortis de garanties strictes.

Dans le climat de défiance que ressent une partie de la population vis-à-vis

de l'État et de la fonction de sécurité qui lui est confiée, l'emploi des nouvelles technologies par les forces de sécurité peut être aussi associé à la surveillance de masse.

C'est la raison pour laquelle je crois qu'il est indispensable d'inscrire l'emploi des technologies de sécurité dans un pacte de confiance plus large entre les forces et la population.

Dans cette optique, j'ai souhaité déterminer de manière opérationnelle et pragmatique les technologies de sécurité qui sont prioritaires au regard de trois critères : répondre aux besoins des forces, préserver les libertés, privilégier des technologies mûres d'un point de vue technique.

Expérimenter en situation réelle

C'est ainsi que je pense qu'il faut expérimenter en situation réelle les technologies qui facilitent l'identification des situations de danger.
A court terme, il s'agit de tester les technologies qui permettent de détecter de manière automatisée des anomalies dans l'espace public et de renforcer les contrôles d'accès à des sites sensibles pendant les jeux olympiques (par exemple à l'aide de scanners corporels).

A moyen terme, il est nécessaire de répondre aux besoins structurels des forces de sécurité en autorisant à titre expérimental l'exploitation automatique des données rendues publiques par les utilisateurs sur Internet pour identifier des situations anormales de danger.

Il est aussi possible de permettre la constitution de jeux d'apprentissage de données réelles afin de favoriser les projets de R&D en matière d'intelligence artificielle.

J'appelle aussi à bien peser l'équilibre entre l'intérêt que peuvent représenter les nouvelles technologies biométriques et leur caractère intrusif. Les techniques biométriques sont celles qui suscitent le plus d'inquiétudes dans le débat public.

Si des dispositifs d'authentification biométrique peuvent être déployés dans

le cadre des grands évènements afin de sécuriser l'accès aux sites sensibles, l'identification biométrique en temps réel dans l'espace public doit faire l'objet d'une approche prudente et progressive compte tenu de son caractère particulièrement intrusif pour la vie privée.

C'est la raison pour laquelle l'ouverture d'un cadre d'expérimentation en situation réelle devrait être soumis au débat public dans un premier temps pour les usages les plus graves dans le cadre de la lutte contre le terrorisme.

Enfin, il faut que les équipements des forces de sécurité soient modernisés en clarifiant le régime juridique de la captation d'images par drones mais aussi par caméras embarquées.

Toutefois au regard des inquiétudes qui se font jour quant à l'impact pour les libertés, il nous faut apporter des garanties à l'emploi des technologies de sécurité afin de construire une relation de confiance entre les forces et les Français.

L'action des forces de sécurité doit être guidée par plusieurs principes communs : maîtrise de la technologie par l'humain, maturité technologique, solutions souveraines pour les usages les plus critiques.

Nécessité d'accroître la confiance

Il convient également de protéger nos données personnelles et de soutenir aux expérimentations. Nous devons collectivement nous mobiliser pour décider ensemble des usages des nouvelles technologies.

Plusieurs facteurs viennent aujourd'hui expliquer les difficultés à accepter l'emploi des technologies dans le champ de la sécurité : le manque d'information et la polarisation croissante du débat public, la réticence au partage de données et le climat de défiance envers les institutions qui dépasse le seul champ de la sécurité.
Il est possible d'accroître la confiance dans les nouvelles technologies en sensibilisant et en formant le grand public mais aussi en gagnant en transparence, par exemple en organisant la feuille de route du ministère de l'Intérieur sur l'ouverture des données et des codes sources.

Il serait donc souhaitable de décider collectivement de nos choix de société en organisant un débat public sur les grandes évolutions technologiques sur le modèle des lois bioéthiques.
Il est enfin nécessaire, au même titre que pour tout outil sensible, de superviser l'emploi des technologies par les forces sécurité.
L'action des forces de sécurité pourrait être mieux évaluée en sollicitant, de manière plus systématique, les inspections sur l'emploi par les forces de sécurité des nouvelles technologies.
Les pouvoirs et les moyens qui sont alloués aux autorités de contrôle pourraient être renforcés, dans la mesure où ils sont indispensables pour articuler soigneusement les libertés avec les nécessités de sécurité publique.

Je me félicite que, d'ores et déjà, suite à l'adoption en première lecture cette semaine du projet de loi responsabilité pénale et sécurité intérieure, dont j'étais rapporteur, nous permettions par la loi, la possibilité aux forces de police, de gendarmerie et aux douanes de recourir aux caméras aéroportées ou embarquées pour des finalités désormais clairement définies.

Parce qu'il nous faut apporter soutien, protection et reconnaissance à nos forces de l'ordre, je me réjouis des annonces du Président de la République dans le cadre de la clôture du Beauvau de la Sécurité, et notamment de la présentation en janvier prochain en conseil des ministres de la Loi d'orientation et de programmation pour la sécurité intérieure.

Il est en effet primordial de construire un plan de modernisation de la politique publique de sécurité au bénéfice des policiers, des gendarmes et de l'ensemble des Français. Nous nous devons de penser la police et la gendarmerie de 2030.

Parution le 1er octobre 2021

Conformité et sécurité : un cran au-dessus ?

FRANÇOIS COUPEZ
Avocat à la Cour
Fondateur Level Up Legal
Senior Advisor du CyberCercle

Sécurité des systèmes d'information et conformité, notamment en matière de protection des données, sont deux concepts qui sont fortement liés à l'heure actuelle, que ce soit par la réglementation ou les régulateurs.

Il fut toutefois un temps où la situation était différente. L'auteur de ces lignes se rappelle encore l'émoi qu'a causé, il y a quelques années, la volonté d'envoyer des documents hautement confidentiels sous forme chiffrée à un régulateur européen, celui-ci ayant plutôt insisté pour recevoir plutôt un bon vieux fichier Excel par message électronique…

Mais tel n'est définitivement plus le cas aujourd'hui. La sécurité des systèmes d'information faisant régulièrement la une des journaux, la « culture sécurité » infusant dans tous les secteurs économiques, les régulateurs ont changé de vision et intègrent cet élément de façon cruciale dans leurs audits des entreprises dont ils ont la supervision. Pour la CNIL par exemple, la sécurité est un angle d'audit d'autant plus important que plusieurs facteurs se coagulent : l'afflux d'anciens de l'ANSSI dans ses rangs a accru sa compétence, le RGPD s'inscrit dans la droite ligne de la loi du 6 janvier 1978 et se fonde peu ou prou sur la sécurisation des systèmes d'information, la protection des données ne peut être assurée que si la sécurité des systèmes d'information et des infrastructures est elle-même renforcée, etc.

PDCA et protection des données

Si l'on étudie justement le sujet de la protection des données personnelles sous cet angle, on se rend compte que la situation a nettement évolué avec l'avènement du RGPD d'une part, et depuis son entrée en vigueur en 2016 puis en application en 2018 de l'autre. En cela, le cycle PDA, central les normes ISO en matière de qualité, puis de management de la sécurité de SI, semble produire tous ses effets.

Rappelons que PDCA signifie Plan Do Check Act et qu'il désigne une méthode de conception et de gestion itérative utilisée dans les entreprises pour le contrôle et l'amélioration continue des processus et des produits[1]. Cette méthode est composée des phases de notions de planification, d'exécution/de développement, de vérification/contrôle, mais surtout de réaction/ajustement pour optimiser et améliorer les process concernés.

En clair : on peut (et il faut) toujours mieux faire !

Or cette notion est centrale dans les normes ISO qui peuvent exister en matière de qualité (9001) et de systèmes de management (14 001 en matière d'environnement… et 27 001 et suivants en matière de sécurité de système d'information).

Si le RGPD ne mentionne la notion que dans son article 32d comme un exemple des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque », la notion irrigue en réalité la règlementation en la matière, surtout telle qu'elle est interprétée par les régulateurs (CEPD, CNIL, etc.).

Si l'on s'intéresse par exemple à la notion de violation de données à caractère personnel, l'ancêtre du CEPD indiquait, par exemple, dans ses « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 » dès leur première version d'octobre 2017, que l'obligation de notification ne s'arrêtait pas au fait de constater une violation et allait bien plus loin. L'organe rassemblant les régulateurs européens en matière de protection des

données indiquait ainsi que « Le responsable du traitement se voit ainsi tenu de prendre les mesures nécessaires pour s'assurer de prendre "connaissance" de toute violation dans les meilleurs délais afin de pouvoir réagir de façon appropriée ». Pour le G29/CEPD, l'obligation prévue devait donc largement être mise en perspective par rapport aux objectifs de protection des personnes concernées…. Et l'obligation initiale devait nécessairement s'assortir d'une vision à 360° plus globale.

De la même façon, les positions de régulateurs n'ont été que crescendo concernant les scénarios de risque à établir préalablement aux traitements qui le nécessitent. Si l'on s'intéresse au résultat final de ces scénarios, soit les notifications à mettre en œuvre quand les hypothèses se réalisent, la différence est ici frappante entre les lignes directrices précitées, ne donnant que quelques exemples utilisables en pratique (annexe B p. 35 à 38), et les « Lignes directrices du 14 janvier 2021 » dont la trentaine de pages est dédiée à ce seul et unique sujet.

Vers un autre niveau d'exigence de conformité

Sur tous les sujets, le niveau de maturité augmente et les exigences en termes de conformité ne font que croître, en France comme à l'étranger.

Si l'on reprend l'exemple de la protection des données personnelles :

- Avant 2016, le fait pour une entreprise privée d'avoir un CIL, voire mieux, un réseau de correspondants locaux au niveau d'un Groupe, était le signe de meilleures pratiques.
- En 2018, avoir un DPO/DPD est devenu obligatoire dans nombre de cas, c'est alors devenu la norme.
- Depuis, les exigences augmentent encore et l'on s'intéresse maintenant aux compétences et au rôle pratique du DPO dans l'entité. En l'occurrence :
- A la réelle indépendance du DPO/DPD. Est-il en situation de conflit d'intérêts du fait de ses multiples fonctions ? Rappelons que l'Autorité de protection belge (APD) a infligé une amende de 50 000 euros à un responsable de traitement pour non-respect de l'obligation d'éviter tout conflit d'intérêts, le DPD étant également directeur de la compliance, du risk management et directeur de l'audit interne ;

- ou même s'il n'a pas outrepassé en réalité ses fonctions de DPO pour agir comme un responsable de traitement. À ce titre, une autre décision de la même APD du 28 mai 2019 est très intéressante : elle sanctionne un responsable du traitement parce que son DPD avait pris de lui-même la décision d'effacer des données à caractère personnel en réponse à un droit d'accès… se comportant *de facto* comme un mandataire du responsable de traitement[2].
- Difficile de ne pas mentionner ici le niveau des sanctions, qui lui également ne cesse de croître :
- Plus de 3 M EUR pour les filiales du Groupe Carrefour au total en novembre 2020, 100 M EUR pour les filiales de Google et 35 M pour Amazon en décembre 2020, 500 000 EUR pour Brico Privé en juin 2021, 1,75 M pour AG2R La Mondiale, 50 000 EUR pour les cookies du Figaro et surtout 746 M EUR pour Amazon en juillet 2021 ;
- Et la pression européenne sur l'autorité irlandaise de protection des données qui finit par payer, avec une sanction historique de 255 M EUR concernant WhatsApp qui vient d'être annoncée.

Des exigences de sécurité comme base de la conformité… et du business !

Les effets de cette maturité croissante en la matière ne s'arrêtent pas là. Face aux cyberattaques par ransomware par exemple[3] :

- Il devient à l'heure actuelle de plus en plus difficile de souscrire une « assurance cyber », certains assureurs se retirant peu à peu du marché (nous parlons bien ici des assurances globales, hors option spécifique du paiement des rançons) ;
- Et surtout les assureurs imposent de façon préalable la mise à niveau de la sécurisation des SI de l'entité, avec des questionnaires s'inspirant plus que fortement des normes ISO 2700x.

En réalité, ces éléments ne sont que le signe d'exigences croissantes en matière de sécurité des systèmes d'information de la part des principaux acteurs économiques. Ayant pris conscience de ces fortes exigences, ils ont été conduits à identifier leurs partenaires économiques et prestataires comme des vecteurs d'attaque malgré eux et leur imposent depuis quelques années un niveau de sécurisation minimum avant d'entrer en relation contractuelle.

La nouveauté est, là aussi, que :
- Ces exigences se renforcent très fortement[4] et surtout se systématisent, quelle que soit la taille de l'interlocuteur économique ;
- Et se diffusent elles-mêmes auprès d'opérateurs économiques de taille toujours plus restreinte. En réaction, les prestataires de grands groupes challengent leurs propres prestataires pour répondre aux impératifs, comprenant que ce n'est ni une lubie passagère, ni un domaine qui ne donnera jamais lieu à vérification, audit… ou défaut de conformité susceptible d'être publiquement connu !

Plus encore qu'hier, la conformité et la sécurité des systèmes d'information doivent marcher de concert pour permettre le développement du business et non conduire à ce que les portes des marchés se ferment.

Pour conclure, il est intéressant à ce titre de faire un parallèle avec les expériences de deux start-ups ayant connu un contrôle de la CNIL. L'une, Fidzup, considérait que la régulation devait s'adapter au business. Ayant notamment perdu clients et investisseurs à la suite d'une mise en demeure de la CNIL pour non-conformité, la start-up n'a tout simplement pas survécu à l'expérience et a publiquement accusé la CNIL d'avoir causé sa perte[5]. L'autre, Alan, avait anticipé un certain nombre de problématiques, a profité de l'expérience pour renforcer la sécurité de ses process… et a renforcé son image sur le plan médiatique pour avoir bien fait savoir qu'ils avaient passé le contrôle sans encombre[6].

Et vous, quel camp choisirez-vous ?

Parution le 15 octobre 2021

[1] Transposée graphiquement sous la forme d'une « roue de Deming », du nom du statisticien l'ayant fait connaître dans les années 1950

[2] Une question centrale commence enfin à être posée en pratique, même si CNIL et CEPD avaient pour le moment jeté un voile pudique sur cette problématique : à quel titre le DPO aurait-il la possibilité de remplir un registre de traitement ? Donc en lieu et place du responsable de traitement ? En tant que son mandataire ? Mais quid alors des situations de conflits d'intérêts quand il agit ainsi ?

[3] Nous ne traiterons pas ici de l'intéressante question du paiement des cyberrançons et renvoyons le lecteur intéressé vers un débat récent sur le sujet : https://www.youtube.com/watch?v=Bqy3jOi3Yms.

[4] Les questionnaires sécurité représentant très souvent des annexes de taille conséquente lors des négociations avec les directions des achats, avec des engagements souvent imposés

[5] https://business.lesechos.fr/entrepreneurs/actu/0602712976681-fidzup-tirele-rideau-et-accuse-la-cnil-de-l-avoir-tue-334901.php.

[6] https://blog.alan.com/tech-et-produit/controles-par-la-cnil

L'industrie 4.0, cheval de Troie d'une cybersécurité intégrée ? Une occasion historique à saisir

FLORIAN MANET
Colonel de la gendarmerie nationale
Commandant la Section de Recherches de Bretagne
Chercheur associé à la chaire de géopolitique
de Rennes School of Business

L'Industrie 4.0 révolutionne la production industrielle au sein de chaînes de valeur interconnectées. Elle interroge sur la pleine maîtrise par l'homme de cet écosystème numérique complexe. Le capitaine d'industrie est-il encore maître dans son propre navire ?

Le terme d'« Industrie 4.0 » est apparu pour la première fois sous la plume du professeur Wolfgang Wahlster, directeur du Centre allemand pour la Recherche sur l'Intelligence Artificielle. Le 1er avril 2011, il publia un article intitulé « *Industry 4.0 : With the Internet of Things on the Way to Fourth Industrial Revolution* ». D'emblée, ce concept fait référence à la quatrième révolution industrielle qui repose sur la numérisation. D'où, par ailleurs, la sémantique « 4.0 » empruntée aux sciences de l'information.

Un ré-enchantement de la production par la numérisation des process ?

Dès lors, l'industrie s'est appropriée, avec succès, ce concept novateur qui, aujourd'hui, connaît des réalisations concrètes de plus en plus nombreuses. Un phénomène global de numérisation de l'espace industriel tant au niveau de la production que des process mis en œuvre a redessiné les équilibres globaux. Ainsi, il embrasse toute la chaîne de production :
• Conception du produit (usine virtuelle, continuité numérique),

- Contrôle et pilotage (automatisation des flux et des équipements : usines/lignes connectées, capteurs/Internet des Objets, logistique automatisée),
- Procédés de fabrication (machine intelligente, fabrication additive, robots collaboratifs ou cobotiques)
- Maintenance conditionnelle (*big data*, télé-maintenance),
- Organisation du travail (opérateur assisté, organisation apprenante).

La *smart industry* apparaît comme un lieu porteur de valeurs qu'il convient de partager. Mieux encore, la production elle-même s'inscrit dans un dialogue constant avec le client désireux d'obtenir un bien sur-mesure dont il peut suivre à distance la réalisation et en influer le cours à sa guise. Ce dispositif industriel est intégré dans un maillage serré d'interconnexions. L'Internet des Objets fait interagir les objets connectés, équipements ou process au sein de la chaîne de production. Plus largement, par la mise en réseau des systèmes d'information, cette *smart industry* s'insère étroitement dans l'ensemble de l'écosystème industriel l'environnant aussi bien en amont comme en aval.

La donnée, moteur de performance collective

Œuvre collaborative, ce processus industriel exploite les possibilités infinies qu'offrent les nouvelles technologies de l'information. À ce titre, la donnée devient le centre de gravité d'un système en recherche d'une performance accrue et d'une production centrée sur le client.

Clé de voûte, la donnée est valorisée par trois innovations majeures :
- L'informatique avancée ou décisionnelle avec les machines apprenantes, l'exploitation du *big data* et du *cloud*,
- Les objets connectés avec la possibilité de faire le lien avec des objets physiques et d'autres numériques,
- La robotique avancée avec des robots collaboratifs.

Au total, le principe d'une entité « *smart* » se fonde sur l'utilisation et l'exploitation des données et des algorithmes afin d'appliquer des processus intelligents qui pourraient, ensuite, être exécutées, évaluées et améliorées. Ces entités sont conçues nativement pour détenir la capacité d'apprendre et de prendre des décisions en autonomie.

Des risques 4.0, corolaires de l'interconnexion digitale ?

Cette révolution industrielle induit un changement fondamental de paradigme, source d'opportunités, mais aussi de risques émergents. La littérature explicitant le concept est prolifique. Toutefois, l'évaluation des risques liés aux technologies digitales interconnectées mérite d'être encore approfondie en décortiquant méthodiquement ce changement d'ère. Loin de ne présenter que des impacts environnementaux ou productifs, l'Industrie 4.0 génère aussi une révolution sociale au cœur des chaînes de production et d'approvisionnement. Décloisonnant l'espace industriel à l'extrême, elle contribue, malgré elle, à le rapprocher d'acteurs malveillants qui exploiteront, sans état d'âme, les opportunités offertes par ce progrès technologique. Au total, cette réorganisation industrielle suscite un nouveau modèle économique dont le maillon… fort doit demeurer l'Homme, garant de la résilience collective. À ce titre, la *smart factory* constitue une formidable opportunité pour renforcer la cybersécurité. Alors, considérons ce concept comme le cheval de Troie d'une cybernétique sécure !

Une révolution managériale en marche ?

L'Industrie 4.0 engendre une révolution managériale au sein des organisations industrielles. Pièce maîtresse, le directeur du site est à la croisée des chemins de la traditionnelle verticalité qui donne du sens à l'action et d'une horizontalité de plus en plus prégnante qui souligne la dimension collaborative de la chaîne de production intelligente. Ce contexte exige un niveau élevé de compréhension des mécanismes digitaux et de leurs impacts sur la production industrielle. Pour ce faire, le dirigeant s'appuie sur des fonctions support ou expertes telles le *Chief Digital Officier* (CDO). Responsable de la transformation numérique, le directeur du digital produit des études d'impact sur les nouvelles technologies et sur leur adaptation aux besoins. Il supervise la bonne mise en œuvre de la stratégie numérique et de sa coordination avec la stratégie globale de l'entreprise. Par ailleurs, il veille à la cohérence des interconnexions établies par les acteurs du site avec

l'écosystème. Il s'efforce d'anticiper les risques et de construire des plans de continuité d'activités adaptées aux scénarii de crise. Dans les faits, il s'en suit un partage du pouvoir entre le directeur et le CDO. La complémentarité et la qualité des relations entre ces deux figures essentielles conditionnent la réussite globale de l'entreprise. Affectant les relations managériales, cette révolution s'accompagne corrélativement d'un effort essentiel de communication et de partage avec l'ensemble des collaborateurs qu'il faut embarquer dans ce tout numérique.

De plus, la *smart factory* suppose une très forte agilité des salariés, acteurs essentiels du dialogue Homme – Machine et Machine-Machine. L'enjeu majeur est aussi la constitution d'une ressource humaine hautement qualifiée et la qualité d'une formation continue, incluant une forte dimension de cybersécurité. L'effort de formation est capital pour la conduite des projets industriels. En effet, l'homme reste au cœur d'un système complexe : il donne du sens et de la cohérence aux données collectées. Son esprit d'analyse facilite la prise de décision. Mais, avouons-le, il demeure un maillon fragile susceptible de contribuer, bien souvent malgré lui, à la compromission des systèmes numériques.

La cybercriminalité, valeur dominante du portefeuille risque

À l'avenir, les gestionnaires de risque auront un portefeuille où le volet cyber prédominera, au-delà des atteintes physiques sur les collaborateurs et sur les infrastructures. En retour, cette tendance est susceptible d'impacter les solutions d'assurance face à des évènements de sûreté caractérisés par un préjudice exceptionnel. Cristallisant les enjeux de souveraineté, la valeur de la donnée épouse le contour de la nécessaire maîtrise de son identité personnelle, de la propriété intellectuelle et du savoir-faire, sans négliger la réputation de l'entreprise. Le montant des rançons exigées par des cybercriminels est illustratif des réalités d'un capitalisme criminel dont l'enjeu contemporain semble être la souveraineté de la donnée quelle qu'elle soit.

Le spectre du cyber-chaos, horizon inéluctable ?

Peu importe le mode opératoire, l'effet produit se traduit immanquablement

sous la forme d'un déni de service. La ligne de production est arrêtée, les serveurs de *control and command* ne sont plus opérants, le fichier clients ou la dernière innovation ont disparu. Fruit d'une interconnexion recherchée à dessein, cet écosystème interdépendant peut se trouver amputé et perturbé. Le rançongiciel NOT PETYA est illustratif des effets produits sur la logistique mondiale et du caractère irrémédiable d'un tel déni de service opéré sur 50 000 terminaux portuaires contraints à une reprise manuelle sur 600 sites répartis dans 130 pays. Les pertes directes supportées par l'opérateur s'élèvent à plus de 300 millions de dollars. Quel est le montant global de la facture pour l'ensemble des victimes collatérales de ce dérèglement logistique ?

Une Sagesse 4.0 ?

Cette quatrième révolution industrielle revêt des impacts socio-économiques, organisationnels, juridiques et sécuritaires. Source d'innovations, elle invite, avant tout, à promouvoir une approche intégrée au sein des organisations interconnectées. Dans ce contexte de complexification des chaînes de production, les capacités humaines peuvent être dépassées et inaptes à saisir les facteurs pertinents dans l'action ainsi que dans la prise de décision. Ainsi, le danger majeur pourrait provenir d'une confiance absolue dans la technologie sans en identifier les limites et vulnérabilités. Cette situation invite à un partage d'expérience avec d'autres secteurs d'activité complexe tels que le nucléaire, la pétrochimie ou l'aviation qui sont, eux aussi, confrontés à des problèmes de performance humaine. Au fil des expériences, ils ont développé des méthodes d'analyse et des protocoles de prise de décision raisonnée dans le cadre d'une gestion intégrée des risques. L'homme y a toute sa place.

Finalement, l'Industrie 4.0 est en soi une Sagesse.

Les opinions exprimées ci-après sont celles de son auteur.
Elles n'engagent aucunement la gendarmerie nationale.

Parution le 28 octobre 2021

Détection des incidents de sécurité : Pourquoi faudrait-il choisir entre vision systèmes et écoute réseau ?

CHARLES BLANC ROLIN
RSSI
Centre hospitalier de Moulins-Yzeure

Lors de la dernière édition des RIAMS, ce prestigieux évènement imaginé et conçu en 2005 par Michel Van Den Berghe, deux questions soulevées par des RSSI de grands groupes français m'ont interpellé sur la compréhension que nous pouvons avoir de certains outils, cachés derrière des acronymes dont on perd parfois la définition et des propagandes commerciales parfois malhabiles.

Lors d'un retour d'expérience sur le thème de la détection réseau, le cofondateur d'une entreprise française éditrice de plusieurs solutions de sécurité, dont une sonde de détection réseau qualifiée par l'ANSSI, s'est vu interpellé sur l'intérêt d'une telle solution :

« Je dispose déjà d'un EDR, que pourrait bien m'apporter de plus votre solution ? »

D'un point de vue technique, ce sont des solutions totalement différentes qui ne devraient pas être mises en concurrence selon moi. Elles apportent toutes les deux des informations précieuses et complémentaires. Faire le choix entre EDR et NDR par exemple, reviendrait à choisir entre l'ouïe et la vue. Dans la mesure du possible évidemment, il est tout de même plus confortable de disposer des deux. Comble du luxe, pour améliorer notre compréhension de la menace, nous pourrions les interconnecter et rapprocher les informations que ces deux solutions renvoient dans un SIEM, que l'on

pourrait comparer au cerveau pour pousser l'allégorie un peu plus loin.

Même si les solutions évoquées ne s'arrêtent pas à la détection et la collecte d'informations, nous nous intéresserons ici, uniquement à cette partie.

Là où le rôle de l'EDR va être de détecter des actions suspectes dans logs systèmes et applicatifs remontés par l'agent installé sur les postes et serveurs, des processus malicieux en mémoire, des modifications du système, des changements de permissions, etc.
Celui de l'IDS, et désormais du NDR si nous souhaitons aller un peu plus loin, est de détecter des comportements anormaux ou suspects sur le réseau, tels que des connexions vers un serveur C2, des exploitations de vulnérabilités, des déplacements latéraux, etc.

Évidemment certaines informations peuvent se rejoindre, et c'est tout l'intérêt pour permettre une détection plus rapide et plus fiable d'un incident, dans le but de tenter de le contenir. De la même manière, dans une phase d'investigation, disposer d'informations en lien avec ce qui a pu se passer sur une machine potentiellement compromise et les corréler avec celles relatives à ce qui s'est passé sur le réseau, pourra permettre de mieux comprendre la chronologie des faits, et les chemins empruntés par l'attaquant.

Si les informations collectées sur les machines (logs, processus en mémoire, mft…) permettent généralement d'apporter plus de clarté sur les actions réalisées par le ou les attaquant(s), et qu'il ne faut donc surtout pas s'en dispenser lorsque nous pouvons les avoir, je vois deux principaux avantages à la détection réseau.
Tout d'abord, il est beaucoup plus difficile pour un attaquant de supprimer les traces qu'il va laisser, ou « faire mentir » le réseau. Je n'ai jamais vu, ce qui ne veut pas dire que cela ne s'est jamais produit, de rapports sur une compromission dans laquelle l'attaquant aurait volontairement généré du bruit sur le réseau pour tenter de dissimuler ses traces, car cela représenterait un risque supplémentaire de détection pour lui. Pour supprimer ses traces, il faudrait qu'il trouve la ou les sondes IDS et /ou la solution NDR, le collecteur de logs et/ou le SIEM et qu'il arrive à les compromettre, mission quasiment impossible.

Deuxième avantage, l'écoute réseau est possible sans avoir à déployer d'agent, et lorsque l'on se trouve sur des réseaux industriels, techniques ou biomédicaux, dans lesquels il n'est pas possible de déployer un agent sur les dispositifs, le réseau reste notre meilleur allié pour nous remonter des informations.

La seconde question bonus posée lors du RETEX était :

« Aujourd'hui, la majorité des flux est chiffrée, si votre solution ne les déchiffre pas, elle ne verra rien passer ? »

Là encore, c'est à mon sens une fausse idée reçue.

Pour commencer, tous les flux ne sont pas chiffrés, et notamment dans le cadre de certaines attaques. Ensuite, l'écoute des flux chiffrés via SSL/TLS permet malgré tout de remonter des informations qui peuvent s'avérer intéressantes, telles que le nom d'hôte de la machine contactée, l'ensemble des informations relatives au certificat présenté par le serveur, les empreintes JA3 et JA3S pouvant permettre d'identifier de manière plus ou moins précise clients et serveurs. Clients pouvant être reconnus comme malveillants. On l'oublie également, mais une simple connexion vers une adresse IP, lorsqu'elle est connue comme fréquemment ou fraîchement utilisée dans le cadre d'attaques, est une information importante. Tout comme une requête DNS. Il sera également possible de détecter des anomalies sur les protocoles, des attaques connues, des déplacements latéraux... suivant où est placée la sonde.

Pour conclure, si j'ai le choix, je préfère ne pas avoir à choisir entre les deux solutions et les utiliser ensemble.

Parution le 5 novembre 2021

Données de santé, le nouvel El Dorado

DAVID SYGULA
Analyste Senior en cybersécurité
CybelAngel

En décembre 2020, j'ai vécu une expérience saisissante : je suis allé chez le dentiste. Cela faisait plusieurs années - ne me jugez pas s'il vous plaît, mes dents vont bien - et je n'avais pas imaginé une telle numérisation des outils. Dès mon arrivée j'ai dû remplir un formulaire sur une tablette, qui s'est verrouillée le temps que je m'installe, et dont les questions étaient pour certaines assez personnelles. Inutile de retourner demander le code : ma tentative de bruteforce a réussi au bout d'un essai (123456). Je l'ai ensuite rendue au secrétariat et, en feignant de ne pas apercevoir le mot de passe du poste sur un petit bout de papier collé à l'écran (admin123), je demande, un peu inquiet : « Savez-vous ce qu'il advient des données de votre questionnaire, qui y a accès ? Sont-elles chiffrées ? » Regard coi.
L'ironie, c'est que quelques jours plus tôt, nous venions de publier une étude sur l'exposition mondiale des données médicales, notamment issues de cabinets de dentistes[1]. Les mois qui ont suivi, les données de santé, particulièrement françaises, ont par ailleurs fait couler beaucoup d'encre : attaques par rançongiciel de centres de soins[2], vente d'accès vers des applications d'hôpitaux[3], fuite de centaines de milliers de données de patients[4], vol d'1,4 million de résultats de tests Covid[5], etc.

Comment trouve-t-on ces données ?

Il serait facile de porter le blâme sur de mauvaises pratiques de sécurité d'utilisateurs (quels qu'ils soient), mais ne tirons pas sur l'ambulance, la réalité est beaucoup plus complexe. Comme souvent en cybersécurité, c'est l'enchaînement de plusieurs actions (ou inactions) qui permettent à une attaque d'aboutir, quand il ne s'agit pas de l'emploi d'une faille 0-day[6]. On peut par exemple y voir l'ouverture d'une pièce jointe malveillante comme un antispam ou un antivirus défaillant en premier lieu.

Mais allons encore plus loin : sans même attaquer qui que ce soit, Internet offre un choix insensé de données sur des espaces non protégés qui sont faciles à identifier pour qui sait où chercher. Pour donner un ordre d'idée, chaque jour 3 milliards de documents et lignes de bases de données passent par les moteurs de CybelAngel.
Ces éléments sont trouvés via des protocoles non sécurisés (utilisés par des NAS par exemple), mais également des applications Cloud, type Google Drive, Slideshare et autres Dropbox.

C'est également sans compter les téraoctets de documents exfiltrés et mis en libre téléchargement par des groupes de rançongiciels. Bien que ces derniers déclarent ne pas s'en prendre aux hôpitaux ni aux centres de soins, ils ne se privent pas pour attaquer cliniques, laboratoires, prestataires du domaine médical et puis bon, de temps en temps, un hôpital par-ci par-là malgré tout.

Régulièrement, sur les forums underground, quelques mois plus tard, ces mêmes données sont compilées et vendues, alors que l'acteur fait ressortir leur valeur - « dossiers de patients US », « 10 millions de numéros de sécurité sociale », « personnel hospitalier allemand », etc.

Bref, l'exposition est énorme, et nous n'avons même pas parlé des données patients qui se retrouvent indexées dans les moteurs de recherche à cause d'un serveur Web non protégé, ni de tous ces objets que nous nous évertuons à connecter à Internet, pour le meilleur et pour le pire - et comme chacun sait, tout ce qui est connecté est vulnérable.

Pourquoi un tel acharnement sur les données de santé ?

Précisons tout de suite que de leur côté, les acteurs cybercriminels n'ont pas attendu la crise sanitaire mondiale pour s'intéresser aux données médicales. Si des cas sont de plus en plus rapportés dans la presse en 2021, notamment via les attaques de rançongiciel contre les hôpitaux, sur les forums cybercriminels elles ont toujours eu la côte, où elles sont vendues près de dix fois plus cher que des données de type carte bancaire, email, numéros de téléphone, etc.

Les données de santé sont une mine inépuisable d'informations pour un large panel d'acteurs. D'abord, elles font fi des différences entre chaque individu

(sexe, âge, classe sociale, nationalité, etc.), tout le monde est logé à la même enseigne, et elles sont internationales. Un groupe sanguin, une maladie, un indice de masse corporelle n'a pas de frontière. Ensuite, elles sont propres à chaque individu, étant majoritairement rattachées à un numéro de sécurité sociale ou en tout cas un numéro d'identification citoyenne, peu importe le pays. Ce sont également des données que nous ne contrôlons pas, nous les « subissons », dans le sens où elles nous collent à la peau, mais nous ne pouvons pas les modifier, contrairement à toute l'empreinte numérique que nous créons quotidiennement - publications sur les réseaux sociaux, achats en ligne, commentaires sur des articles de journaux, etc. Mais surtout, elles contiennent des informations intimes qui ne regardent que le patient et son praticien, informations qui dans certains contextes peuvent mettre un individu à l'écart voire en danger.

Le premier risque auquel on pense est donc naturellement le chantage, à juste titre. Il y a aussi de quoi alimenter la fraude : aux États-Unis, le phénomène des « ghosts clinics » coûte des centaines de millions de dollars par an aux assurances - il s'agit de créer de faux rendez-vous patients, voire de faux établissements de santé, avec de vraies données.

Pour les groupes de rançongiciel, il y a une autre raison, plus pragmatique : en dehors de toute considération d'assurance cyber, en attaquant un centre de soins il y a plus de chances de recevoir un paiement qu'en attaquant la PME qui fabrique des lunettes. L'arrêt de la PME entraîne une perte de revenus pour la société, voire un arrêt définitif, mais il n'y a pas mort d'homme. Dans le cas du centre de soins, le scénario est tout à fait envisageable, en particulier en ces temps de pandémie.

Enfin, sans tomber dans la paranoïa, il y a clairement un intérêt qui dépasse la fraude, l'usurpation d'identité et le rançonnage. Qui achète ces données lorsqu'elles transitent sur les places de marché noir ? Mystère. Et qu'en font-elles ? Re-mystère.

Et pourtant ces datasets, d'une tranche de la population ou d'un pays entier, ont une valeur inestimable, au moins marchande, sinon les géants de l'Internet ne s'y intéresseraient pas[7].

La mine d'or n'est pas près de se tarir

Les données de santé sont au centre de tous les paradoxes :
- Elles sont de plus en plus numérisées donc nous élargissons la surface d'attaque, or nous avons de plus en plus à cœur le droit au respect de notre vie privée, notre anonymat ;
- Elles sont d'une grande valeur et criticité, or elles ne sont pas toujours bien protégées - on pourrait citer le manque de régulations (ou en tout cas leur application), le manque de sensibilisation et le manque de ressources comme explications principales, mais chaque raison vaudrait une tribune en soi ;
- Elles doivent cependant être protégées, or elles doivent être facilement accessibles afin d'être utilisables en urgence.

Paradoxe ultime, les smartphones proposent de plus en plus des fonctions natives pour indiquer ses informations de santé de base, qu'un secouriste pourrait consulter librement en prenant en charge le patient dans l'incapacité de répondre aux questions.
À l'ère du big data, nous ne devons pas oublier que nos données de santé ne sont pas des données classiques, même si tout ce qui transite ne semble être que des suites infinies de 0 et de 1. Elles doivent être traitées avec toutes les précautions qui s'imposent, et la première de toutes les étapes est la sensibilisation des personnes qui doivent les manipuler.

Je fus ainsi ravi lorsqu'en partant du cabinet de mon dentiste le secrétariat m'a interpellé : oui les données étaient stockées dans un endroit sûr, chez un prestataire certifié HDS et utilisées uniquement à des fins médicales. Le post-it était toujours là, mais petit à petit, les consciences évoluent.

Parution le 12 novembre 2021

[1] https://cybelangel.com/blog/medical-data-leaks/
[2] https://www.01net.com/actualites/ransomware-les-attaques-sur-leshopitaux-francais-se-multiplient-2035000.html
[3] https://cybelangel.com/blog/heathcare-data-targeted/
[4] Ibid
[5] https://www.numerama.com/tech/740608-apres-la-fuite-des-resultatsde-14-million-de-tests-covid-laphp-a-bien-ecrit-a-ses-patients.html
[6] https://www.lemagit.fr/actualites/252507013/Une-0-day-au-cur-du-volde-donnees-de-14-million-de-Franciliens-testes-Covid-19
[7] https://www.lopinion.fr/edition/wsj/enquete-comment-google-collectedonnees-medicales-americains-208360

L'intelligence artificielle au sein de l'espace cybernétique

COLONEL PATRICK PERROT, PHD
Coordonnateur pour l'intelligence artificielle
Chargé de la stratégie de la donnée
Service de la Transformation
Gendarmerie nationale

Il n'est plus un domaine qui échappe à l'intelligence artificielle tant elle est omniprésente au sein de notre monde, qu'il soit physique ou cybernétique. En matière de cybercriminalité, la question est de savoir si l'intelligence artificielle constitue le mal ou l'antidote. Comme bien souvent, c'est un peu des deux mais peut-être plus encore dans ce milieu spécifique où la célérité des actions comme des réactions nécessite une forte capacité d'anticipation. Il est difficile de définir précisément la cybercriminalité, nous prendrons donc en considération la proposition de l'Organisation des Nations Unies qui la définit comme étant « tous faits illégaux commis au moyen d'un système, d'un réseau informatique ou en relation avec un système informatique ».

Par son imprégnation dans nos vies quotidiennes (smartphone, chatbot, voiture autonome, médecine prédictive, systèmes de recommandations, réseaux sociaux et influence politique), l'intelligence artificielle représente pour les organisations criminelles comme pour l'individu, un moyen d'acquisition de profits considérables. Elle est une discipline qui démultiplie les opportunités d'attaques et accroît les capacités de nuisance. Et il est un terrain particulièrement fertile au développement de la cybercriminalité qui est encore en devenir : les territoires connectés. Demain, la connexion apportera une solution à la circulation de l'information, à la gestion de l'énergie, à la régulation des flux et de la mobilité, à la gestion des déchets comme à la protection des biens et des services, sans compter le développement des objets connectés individuels

qui ne manqueront pas d'équiper nos poignets ou nos vêtements. L'exploitation de toutes ces données reposera sur les méthodes d'intelligence artificielle afin d'améliorer les processus par un apprentissage continu.

L'intelligence artificielle, de nouvelles opportunités pour les cyberdélinquants

L'intelligence artificielle qui est à la source de plus en plus d'applications offre de belles opportunités aux délinquants pour accroître la quantité comme l'efficacité des attaques cyber par des actions répétitives auto-apprenantes. Les formes d'attaques peuvent revêtir différentes formes à partir de la phase d'acquisition des données, de la phase de traitement des données ou encore de la sortie du système.
Parmi les méthodes les plus communes, la technique du « data Poisoning », ou empoisonnement des données en français, consiste à polluer les jeux de données et donc à totalement perturber les systèmes automatiques. Elle s'attaque aux données utilisées pour entraîner les modèles d'apprentissage et permet ainsi, soit de fausser totalement les résultats, soit de contrôler le comportement prédictif du modèle entraîné. Il est alors possible de totalement corrompre le modèle et les capacités de classification, de détection ou de prédiction. L'objectif est de détourner le centre de gravité de l'application en modifiant les jeux de données d'entrée.

Les hypertrucages ou « deepfakes » permettent de constituer de faux corpus à l'imitation des véritables données. Dès lors, il est possible, par des jeux de données artificielles, de fausser la distribution des données réelles en déséquilibrant les catégories sur lesquelles se fondent les résultats. Mais les hypertrucages peuvent aussi être exploités pour réaliser des impostures dans le monde réel. C'est le cas par exemple pour l'infraction connue sous le nom d'« arnaque au Président ». Cette infraction reposait sur l'étude de l'ingénierie sociale d'une entreprise pour ensuite tenter de se faire passer pour le Président en appelant un secrétariat ou service comptable de l'entreprise et solliciter un virement conséquent. Désormais par les hypertrucages, l'imposture s'améliore considérablement parce qu'il est possible d'imiter la voix du Président, voire de diffuser un message à partir d'une vidéo truquée et ainsi de rendre l'arnaque encore plus crédible.

Les systèmes d'intelligence artificielle peuvent également être perturbés durant la phase de traitement par des méthodes d'inférence, c'est-à-dire des méthodes ayant pour objectif de comprendre le fonctionnement des systèmes par des requêtes successives. Les systèmes sont souvent considérés comme des boîtes noires mais en leur adressant un nombre illimité de requêtes et en analysant la réponse à chacune de ces requêtes, progressivement, la boîte noire révèle ses secrets à l'attaquant. Il s'agit en quelque sorte de méthodes de « reverse engineering » où l'étude du couple entrée-sortie du système permet de reconstruire le mécanisme interne du système. À titre d'illustration, de plus en plus d'études s'intéressent à l'estimation des poids des réseaux de neurones profonds à partir de ces méthodes. Ces approches sont exploitées par les hackers qui utilisent l'intelligence artificielle en détournant les algorithmes afin de les inciter à prendre de mauvaises décisions. Une attaque de ce type sur un système de trading de cryptomonnaies a été conduite de la sorte. Les criminels ont tenté de comprendre comment les robots effectuaient le trading, puis les ont utilisés pour tromper l'algorithme.

Autre technique utilisée pour altérer totalement la sortie des systèmes est celle des attaques adverses. Cela consiste à optimiser un bruit de façon à générer une perturbation indétectable mais qui altère totalement la réponse d'un système. C'est ainsi que, dans le domaine de la reconnaissance d'images, il est possible, en modifiant quelques pixels, de confondre un chien avec une voiture, un avion avec un gorille. En matière de développement des véhicules autonomes, les attaques adverses constituent une véritable menace considérant qu'un panneau « STOP » peut ne pas être reconnu par la simple apposition d'un autocollant bien placé de faible taille.

Les Botnets, qui sont des robots en réseaux permettant d'infecter les systèmes, voient aussi leurs capacités démultipliées par l'intelligence artificielle. L'objectif est encore d'enrichir les corpus et d'extraire de l'information des systèmes pour mieux en comprendre les failles et vulnérabilités. L'intelligence artificielle peut ainsi sélectionner ou adapter les logiciels malveillants et contrer activement les efforts de sécurité pour les rendre inefficaces.

Ainsi les méthodes d'exploitation des failles de l'intelligence artificielle tout au long du cycle de vie de la donnée sont légion et ne manquent pas d'ingéniosité. L'action malveillante a pour objectif d'analyser le comportement des systèmes, de récupérer des données ou de s'emparer du modèle d'apprentissage et dès lors de s'approprier la capacité de décision.

L'intelligence artificielle offre donc de belles perspectives aux cyberdélinquants pour détourner ou s'approprier à distance le fonctionnement des systèmes. Fort heureusement, pour protéger les systèmes contre les failles de l'intelligence artificielle, il est une arme capable de réagir avec efficacité et célérité : l'intelligence artificielle.

L'intelligence artificielle, une arme efficace contre les cyberdélinquants

En effet, face aux nombreuses possibilités d'attaques des cyberdélinquants, la seule défense efficace qui permettra de réagir de façon ciblée et dans le temps de l'attaque sera l'intelligence artificielle. Celle-ci permet de détecter les failles comme les menaces, d'adapter les dispositifs pour réagir et de le faire dans un temps suffisamment rapide pour minimiser l'impact des attaques. Grâce à sa capacité d'apprentissage, l'intelligence artificielle s'améliore en continu et est en mesure de proposer une défense ciblée, adaptative et évolutive contre l'action des cybercriminels. Comme pour l'attaque, la défense peut se concentrer sur trois volets : la maîtrise des données entrantes, la fiabilité du traitement et le contrôle des résultats.

L'intelligence artificielle permet de détecter les tentatives d'intrusion et les comportements atypiques et anticiper d'éventuelles attaques. Il est ainsi possible de mesurer le nombre de requêtes de même nature qui pourrait apparaître comme caractéristique d'un signal faible d'attaques de type inférence. Cette action de prévention d'actions suspectes est connue dans la littérature sous l'acronyme UEBA (User and Entity Behavior Analytics). L'UEBA consiste à surveiller les comportements des utilisateurs mais aussi des entités que sont les applications mobiles, en nuage ou en réseaux comme les serveurs. Par apprentissage, chaque entité ou utilisateur se voit modéliser et toute nouvelle action est comparée à ces modèles pour

détecter les situations atypiques ou non conformes au modèle.

Pour contrer les attaques ayant pour objet la prise en compte des capacités comme des données, la phase d'apprentissage des modèles doit faire l'objet d'une attention particulière. Il convient en prévention d'allonger la durée puis d'élargir le jeu de données de façon à diminuer la surface d'exposition aux modifications partielles des jeux d'apprentissage et donc d'accroître la robustesse. Une surveillance doit ensuite être mise en œuvre : il s'agit alors d'associer l'expertise métier (cohérence des données), le contrôle de l'intégrité des données (ingénierie des données) et de détecter les dérives de la modélisation (science des données) au fur et à mesure de l'entraînement.

Pour prévenir les attaques qui consistent à tester les systèmes en vue de connaître leur mode de fonctionnement, il est possible de multiplier les modèles de prédictions en fondant l'analyse sur des méthodes différentes. L'objectif est d'insérer des aléas afin de rendre inexploitables les failles de confidentialité. Cela complique la tâche de l'attaquant soit en multipliant les solutions possibles, soit en proposant des modèles différents. L'inconvénient est que l'injection des aléas peut également altérer le niveau de performance du système, il s'agira alors d'évaluer le compromis entre la performance et la protection.

Face aux hypertrucages, l'intelligence artificielle constitue également un remède efficace. Il est, par exemple, possible d'insérer durant l'apprentissage des perturbations adverses. Ainsi contrariés, les réseaux génératifs adverses à l'origine des hypertrucages, ne parviendront pas à correctement construire leur modèle d'imposture. La détection des impostures de type deepfakes est assimilable à une course à l'armement, à un conflit continu attaque-défense. Cette détection, pour être efficace, doit entraîner un modèle d'apprentissage à partir d'un maximum de méthodes afin de disposer de la plus grande capacité généralisatrice possible. À défaut, la détection sera trop spécialisée et perdra en performance. Or, dans cette discipline, la capacité de généralisation est le point d'orgue de l'adaptation des défenses aux attaques.

Ainsi que ce soit dans le monde physique ou virtuel, l'intelligence artificielle se révèle en double face. Elle constitue à la fois le moyen de réaliser et d'optimiser des attaques contre les systèmes d'information mais aussi de proposer les solutions pour s'en protéger. Il est indispensable pour les forces de sécurité intérieure de s'investir en partenariat avec les organismes de recherche dans la sécurité des modèles d'intelligence artificielle, au risque de voir cette discipline perdre en confiance chez le citoyen, usager des systèmes, et gagner en opportunité chez le délinquant.

Parution le 19 novembre 2021

Faire de la cybersécurité une valeur ajoutée pour l'entreprise

ANNE DORÉ
Co-auteure
« Cybersécurité – Méthode de Gestion de Crise »
Fondatrice ADHEL

La crise cyber est une nouvelle certitude que les entreprises doivent intégrer dans leur gestion des risques. Même les entreprises déjà victimes, ne sont pas à l'abri d'une nouvelle attaque et celles qui ont réussi jusqu'à maintenant, à passer à travers les mailles du filet, n'ont qu'à bien se préparer. Elles n'y échapperont pas.
La digitalisation de l'économie et des processus métier au sein des entreprises, dans un contexte de pandémie mondiale, a mis en exergue les faiblesses structurelles en matière de sécurité numérique et l'absence de préparation de nombreuses organisations, notamment celles non soumises à des contraintes règlementaires.
Pour autant, nombre d'entreprises cherchent à se rassurer et pense pouvoir gérer une crise cyber en se fiant à leurs expériences acquises lors de précédentes crises, la dernière étant celle de la Covid 19. Il faut néanmoins rappeler que la cybersécurité n'est pas une crise comme les autres !

La crise cyber résulte d'une action malveillante ayant la volonté de nuire à l'organisation. N'importe quelle organisation – publique ou privée –quel que soit son secteur d'activité ou sa taille, peut se retrouver de manière frontale face à des demandeurs de rançon ou à devoir faire barrage à des cybercriminels, paraétatiques ou activistes cherchant par tous les moyens à pénétrer au cœur du système d'information.

Les spécificités de la crise cyber résident dans le fait qu'on se retrouve face à un adversaire organisé, malveillant et souvent professionnel et que les

conséquences ne sont pas uniquement informatiques. Elles sont humaines si la cible est un CHU, économiques, financières, industrielles et, ou informationnels quand une attaque génère l'arrêt d'une chaine de production ou nuit à la réputation de l'entreprise en prenant par exemple le contrôle d'un vecteur de communication comme un site internet. La crise cyber est donc un risque métier qu'il faut appréhender, gérer et prévenir.

Elle exige donc de la part des organisations une réaction rapide, pertinente et efficace. La réaction apportée varie selon la nature, l'envergure et l'impact des risques générés et les scénarios de crise préalablement définis.

La complexité et le besoin de réactivité sont telles des réponses selon les risques métiers encourus et la nature de la crise. L'anticipation et la préparation sont des vecteurs clés de réussite dans la gestion de crise. Elles auront aussi pour mérite d'en limiter l'impact et d'éviter une crise dans la crise.

Dans la « Méthode de gestion de crise »[1] , nous décrivons comment cette préparation passe par un apprentissage permanent et itératif s'appuyant sur 2 cycles : le cycle nominal consistant à anticiper, préparer et prévenir la crise et le cycle de gestion de crise. Ces deux cycles interviennent à des moments différents, mais sont interdépendants et ont pour objectif commun d'améliorer en permanence la capacité de résilience de l'organisation.

Construire des organisations résilientes pour prévenir les attaques et limiter leurs impacts

La nature du risque et les objectifs déclinés en risque métier propre à chaque entreprise font que la préparation et la gestion d'une crise de nature cyber est complexe.

Une approche proactive est indispensable : les attaques sont ingénieuses et ciblées, aucune entreprise ne peut se considérer comme invulnérable. Il faut ainsi préparer les scénarii et adopter un plan de gestion de crise cyber qui guideront le tempo opérationnel.

Le premier cycle est vertueux. Il amène chaque organisation à mettre en

œuvre un dispositif lui permettant de se préparer dans les meilleures dispositions pour éviter, et si nécessaire s'apprêter à l'affronter. La clé de voûte de cette préparation réside dans la capacité pour chaque entreprise à déterminer les actifs, « joyaux de la couronne », qui doivent être protégés et à imaginer des scénarii selon le type et la nature de la crise.

Pour ce faire, l'entreprise doit en premier lieu s'assurer de la bonne mise en place de la gouvernance de la sécurité de son système d'information avec sa politique et son système de management approprié. Il convient aussi de pouvoir adresser les enjeux de prévention, de détection et de réponse à incidents.

Le second cycle est déclenché dès qu'un ensemble d'éléments fait que l'organisation ne peut plus ignorer la situation de crise, ou que la survie de celle-ci est en jeu. C'est le processus de gestion de la crise.
Le cycle de gestion de crise, préalablement défini dans le cycle nominal, vise à déterminer la démarche à suivre en cas de crise. La priorité absolue est de contenir l'attaque pour préserver les ressources de l'entreprise et pouvoir basculer au plus vite en phase de remédiation afin de limiter au maximum les conséquences négatives.

La complexité et la taille de la structure de l'organisation de gestion de crise dépendent bien évidemment des caractéristiques de l'entreprise. D'une manière générale, elle est constituée non pas d'une cellule, mais de plusieurs cellules de gestion de crise. L'idée est de scinder l'entité qui décide des entités qui exécutent tout en s'assurant d'une bonne communication et coordination entre les entités. Dans les petites entreprises, la structure se limitera à une cellule décisionnelle en charge du pilotage et de plusieurs cellules opérationnelles en charge de l'exécution.

La mise en place d'un plan de gestion de crise réduit de manière significative les risques associés et permet d'en atténuer l'impact, tout en garantissant un retour accéléré au mode nominal dans les meilleurs délais.
Mais au-delà de cette approche vertueuse, chaque crise cyber réelle ou simulée doit être perçue comme une opportunité d'accélérer la transformation de l'entreprise pour améliorer son organisation, ses processus et développer son capital humain.

Construire une organisation cyber-résiliente ou comment faire de la cybersécurité un avantage compétitif

La crise Covid et les nombreuses discussions sur le retour au « monde d'avant » illustrent que la probabilité d'un retour à la « normal » est quasi nulle. Autre constat, si les confinements successifs ont impacté toutes les sociétés, il en ressort que celles d'entre elles qui en ont profité pour accélérer la digitalisation de leur processus métier, la mise en place du télétravail ou par exemple, l'accès à de nouveaux marchés via l'utilisation d'internet ou de « marketplace » sont ressorties gagnantes.
Dans une étude publiée en avril 2020[2], le cabinet de stratégie BCG démontre que les entreprises les plus rentables depuis la crise de 2008, indépendamment du pays ou du secteur d'activité, ont traversé quatre phases : « la gestion de la turbulence, la stabilisation, la reprise et la poursuite de l'accélération ».

C'est pourquoi chaque crise, exercice de crise doit être une opportunité pour l'entreprise pour renforcer sa résilience cyber et identifier les améliorations à apporter au sein de son organisation, ses processus et sa gestion des RH afin d'être plus forte, plus innovante ou se transformer plus rapidement.

Dans son livre « Antifragile : Les bienfaits du désordre », Nassim Nicholas Taleb va d'ailleurs plus loin et affirme que les entreprises ne devraient pas être résilientes, pour éviter de revenir dans une situation d'avant crise. Les entreprises devraient être « anti-fragiles », à savoir qu'en situation « post crise », elles doivent être différentes de celle avant la crise, différentes de la situation nominale d'avant crise.

L'apprentissage permanent est donc un des maîtres mots de la gestion de crise. Apprendre de ces expériences « simulées » ou réelles pour se renforcer et développer la résilience de l'entreprise est un facteur clé de réussite pour mieux gérer la prochaine crise et sensibiliser encore plus l'ensemble des collaborateurs, dirigeants inclus.

Cet apprentissage et la mise en place de ce dispositif vertueux résultent de l'efficacité et l'opérabilité du retour d'expérience (RETEX) à chaud et froid

des exercices de crise et des crises elles-mêmes. Il en ressort alors des améliorations stratégiques ou opérationnelles (RH, équipements, outils, soutien, organisation…) qui devront être intégrées dans la gouvernance de l'entreprise et celle de la gestion de crise. Par ailleurs, une crise est une opportunité de renforcer une image de marque, d'apporter une autre dimension à la gestion des ressources humaines ou de renforcer la relation avec ses partenaires et ses clients.
La construction d'une organisation résiliente est donc source de valeur ajoutée et contribue à améliorer la performance économique et financière de l'entreprise.

Intégrer la cybersécurité dans la gouvernance de l'entreprise

Force est de constater une nouvelle fois que la cybersécurité et la construction d'une organisation cyber résiliente requièrent une approche transversale et 360°. Elles impactent la stratégie et l'organisation de l'entreprise. `
Si une crise cyber peut négativement impacter le bilan de l'entreprise, il peut aussi avoir des conséquences pour les dirigeants qui pourraient se voir reprocher par les investisseurs d'avoir négligé ou sous-estimé l'ampleur et les conséquences d'une telle crise. A contrario, une bonne gestion de crise cyber ne pourra que renforcer l'image et la réputation de l'entreprise au sein de l'écosystème et des investisseurs.

Le directeur général et les dirigeants de l'entreprise ont donc tout intérêt à s'impliquer dans la stratégie et la mise en œuvre de la cybersécurité de l'entreprise et plus encore celle de la gestion de crise. La cyber résilience est un volet à part entière de la gouvernance de l'entreprise. Il y va de sa réputation et de sa capacité à évoluer en permanence pour s'adapter aux besoins du marché et aux menaces. Elle constitue une véritable opportunité pour accélérer la mise en œuvre de la stratégie d'entreprises.

Parution le 26 novembre 2021

[1] https://www.va-editions.fr/cybersecurite-c2x35356757
[2] https://www.bcg.com/fr-fr/publications/2020/crisis-sparktransformation-renewal.aspx

La protection des systèmes d'information est aujourd'hui une nécessité à tous les niveaux

CHRISTOPHE GUILLOTEAU
Président
Département du Rhône

Dans le Rhône, le 15 février 2021, le centre hospitalier de Villefranche-sur-Saône a été la cible d'une cyberattaque.

Ce jour-là, le centre hospitalier de Villefranche-sur- Saône a été la cible d'une cyberattaque d'une grande ampleur, paralysant une grande partie de son système d'information et provoquant le report de plusieurs interventions. Il aura fallu plus de 15 semaines pour un retour à la normale.

Les attaques informatiques se multiplient : pas une seule semaine sans information sur une attaque majeure.

Escroqueries en ligne, cyberattaques, hameçonnages ou rançongiciels : quelles que soient les formes qu'elles prennent, les criminalités numériques font désormais partie de notre quotidien.

Et pire encore, elles ne cessent de se multiplier dans le contexte de crise sanitaire actuel avec une augmentation significative en 2020 liée aux confinements (télétravail, achats en ligne…).

En deux ans, le nombre d'attaques informatiques par des pirates réclamant une rançon a explosé en France comme dans le reste de l'Europe. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en 2020, le nombre de ces attaques aux « rançongiciels » aurait augmenté de 255% rien que sur les grandes entreprises publiques et privées y compris celles qui relèvent de la sécurité nationale, selon l'AFP.

Les attaques informatiques constituent donc aujourd'hui un vrai fléau qui touche aussi bien les particuliers que l'ensemble des entreprises ou administrations.

Face à ce contexte, la cyberdéfense est devenue une priorité pour les collectivités territoriales.
Rappelons que les collectivités traitent de nombreuses données fiscales, sociales et gèrent de nombreuses prestations… La divulgation ou le vol de ces données serait une atteinte majeure à la vie privée des citoyens, une atteinte très dommageable.

À titre d'exemple le Département du Rhône traite environ 25000 prestations par mois.

Pour faire face de manière efficace aux nombreuses menaces qui pèsent sur les données dématérialisées, les collectivités territoriales ont l'obligation de se soumettre à un cadre réglementaire solide de protection des données des usagers.

Ce cadre légal a sensiblement évolué depuis 2018, afin de prendre en compte les avancées digitales et une multitude et variété de canaux de diffusion (réseaux sociaux, cloud, etc..).
De plus les collectivités ont entrepris elles-mêmes une transformation numérique profonde.

En effet elles ont besoin de ces nouveaux moyens pour moderniser leurs actions, pour accompagner le développement de leur territoire et améliorer la qualité de service aux usagers : accès facilité aux services, efficacité et gain de temps dans le traitement des dossiers…
Ces mutations impliquent une augmentation des services en ligne, impliquant plus de risques, plus de répercussions sur le fonctionnement de l'administration et sur le service à l'usager.

Enfin, force est de constater que les données du territoire sont de plus en plus nombreuses et variées du fait d'une multiplication des sources (smartphone et réseaux sociaux, capteurs …). Ces nouvelles données sont difficilement exploitables avec les outils informatiques traditionnels.

Tout cela nous amène à repenser notre schéma de système d'information pour nous moderniser tout en assurant la protection des données.

Pour répondre à cette nécessité, les collectivités doivent être en capacité de se défendre, d'assurer la souveraineté des données pour lutter contre les cybermenaces. Trouvons une alternative en nous dotant d'outils innovants, en sensibilisant et formant les agents.

L'arrivée massive de nouveaux moyens de communication et le développement de l'internet ont nécessité une refonte complète de nos usages numériques en 2017.

Le Département de Rhône applique en son sein une stratégie transverse de cybersécurité et de protection des systèmes d'informations et des données afin de protéger les données des agents, des collaborateurs, des citoyens, et de maintenir l'exploitation des services en ligne et de son système d'information.

Au Département du Rhône nous avons mis en place un dispositif de cyberdéfense technique, opérationnel et organisationnel. Nous complétons actuellement ce plan d'actions en élaborant une politique globale de sécurité pour protéger nos systèmes d'information.
Dans ce cadre nous avons produit un livret des usages numériques.
Ce document, que nous réactualisons périodiquement, est la charte d'utilisation des outils informatiques mis à disposition des agents pour exercer leurs missions.

Parallèlement à ces bons usages nous avons mené une campagne de sensibilisation auprès de l'ensemble des agents. Dans ce cadre, une base documentaire est accessible à tous les agents sur l'intranet du Département avec des fiches pratiques adaptées aux situations.
Plus concrètement, le Département met en avant sur son site intranet les gestes simples (choix des mots de passe, séparation données personnelles et privées, utilisation restreinte de la messagerie électronique) qui permettent d'accroitre de manière significative la sécurité des données professionnelles de l'ensemble des agents départementaux.
Nous poussons également les agents intéressés par le sujet à s'inscrire sur la

plateforme de l'ANSSI pour suivre une formation d'initiation à la cybersécurité.

Enfin, nous veillons à la pertinence des systèmes de protection en les faisant évoluer selon l'état de l'art et les préconisations de l'ANSSI.
Le monde de la cybersécurité et de la cybercriminalité évolue sans cesse et très rapidement.

Dans la démarche d'amélioration continue de ses outils de protection face aux cybermenaces, le Département du Rhône, comme d'autres collectivités territoriales, étudie de près l'usage de solutions de protection et de défense « nouvelles générations » tirant partie des avancées technologiques apportées par l'univers de l'informatique en Nuage telles que l'Apprentissage Machine et l'Intelligence Artificiel.

Incontestablement, cette sensibilisation à la cybersécurité ne pourra se mettre en place sans l'appui de sociétés prestataires de confiance certifiés pour le choix et l'intégration de ces outils, et grâce à une formation poussée de tous les agents concernés par ce secteur aux enjeux considérables dans un monde 2.0 qui ne cesse de s'agrandir.

Parution le 3 décembre 2021

Lutter contre la cybercriminalité : une priorité stratégique pour 2022

MYRIAM QUEMENER
Avocat général
Docteur en droit

La disruption numérique[1] qui concerne désormais aussi bien les particuliers, les entreprises que les collectivités territoriales, apporte des améliorations indéniables aussi bien dans le quotidien que dans la gestion des organisations. Ce changement présente à la fois des avantages, tels qu'une plus grande agilité pour s'adapter aux nouveaux modes de fonctionnement et une réduction des coûts, mais également des inconvénients, comme la perte de visibilité de leurs actifs Internet, les incidents de sécurité, les violations, les atteintes à l'e-réputation.

Le constat

Selon une étude récente de l'éditeur de logiciels de cybersécurité McAfee[1] et du Centre d'études stratégiques et internationales (CSIS), la cybercriminalité, avec ses réseaux de plus en plus organisés, laisse derrière elle une note de plus de 1.000 milliards de dollars. Ce chiffre démontre l'ampleur des préjudices subis qui nécessitent des réponses pertinentes pour lutter contre ce fléau qui suppose, non seulement de la prévention, mais aussi la répression[3].

La gravité et la fréquence des cyberattaques contre les entreprises continuent d'augmenter à mesure que les techniques évoluent et que le travail à distance se développe. Avec l'essor du télétravail et le virage du numérique, jamais il n'a été aussi important de se protéger sur Internet, de choisir un antivirus pour son ordinateur, ou encore de faire attention aux newsletters et formulaires de commandes où l'on doit rentrer nos coordonnées.

Il est indispensable d'anticiper les crises liées aux cyberattaques, notamment dans le cadre d'une stratégie globale de cybersécurité : cloisonnement des systèmes, socle de sécurité opérationnel (SOC) avec en particulier la sensibilisation et un plan de continuité d'activité (PCA), au-delà d'un simple plan d'urgence, afin de préserver l'ensemble du patrimoine informationnel nécessaire.

Au niveau de la cyberdéfense, on constate un effort budgétaire important, ce qui est des plus justifiés. Ainsi, pour 2022[4], les crédits destinés à la coordination de la sécurité et de la défense, qui comprennent les moyens du Secrétariat général de la défense et de la sécurité nationale (SGDSN), les fonds spéciaux et les crédits du groupement interministériel de contrôle (GIC), sont confortés (+21,13 M€ en crédits de paiement).
Il conviendrait, dans le contexte actuel, d'augmenter également le budget de la justice pour traiter plus efficacement le volet contentieux de la cybercriminalité.

Les pistes d'amélioration

Ce contentieux en pleine expansion regroupe toutes les infractions pénales, tentées ou commises, à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet[5]. La cybercriminalité se manifeste ainsi notamment à travers les fraudes numériques qui se réalisent souvent par le biais de piratages, de cyberattaques et de manipulations informatiques. Elles ont pour objectif principal la récupération de données sensibles ou personnelles, qui sont par la suite facilement monnayables.

A l'heure d'un contexte économique difficile où l'on assiste à une pandémie non seulement sanitaire mais numérique, il est ainsi urgent de réaffirmer une stratégie et une politique pénales fortes en matière de lutte contre la cybercriminalité.

L'amélioration de la lutte contre la cybercriminalité passe par un renforcement de la coopération policière et judiciaire, tant sur le plan européen que sur le plan international. Il est urgent de créer une filière de cybermagistrats, au besoin par le biais d'une formation diplômante (DU Cyber par exemple).

Il faut inévitablement renforcer le pôle Cyber au niveau du parquet de Paris ainsi que la spécialisation d'une chambre du tribunal judiciaire en matière de droit du numérique et cybercriminalité. Il conviendrait également, au niveau de la cour d'appel de Paris, de mettre en place un département dédié au numérique et à la cybercriminalité, composé de magistrats du siège et du parquet. Il faut aussi accentuer les formations communes ENM/EFB et PN/GN/Douanes sur le droit du numérique et la lutte contre ce fléau, avec davantage de stages pratiques dans les services spécialisés. Il est enfin indispensable que ce cybercontentieux soit clairement identifié dans les structures judiciaires.

A la veille de la présidence française de l'Union européenne à compter de janvier 2022, il est fondamental de préparer des arguments afin que ce fléau soit pris en compte prioritairement, assorti de moyens plus adaptés à son ampleur.

Parution le 10 décembre 2021

[1] « Le droit face à la disruption numérique », Myriam Quéméner, Lextenso, 2018
[2] https://business.lesechos.fr/entrepreneurs/numeriquecybersecurite/0610096243873-cybercriminalite-la-facture-necesse-de-s-alourdir-341090.php
[3] « Quels droits face aux innovations numériques ? », Myriam Quéméner, Clément Wierre, Frédérique Dalle, Lextenso, 2020
[4] Rapport d'information n° 219, au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat sur la coordination du travail gouvernemental (cyberdéfense, SGDSN), par Olivier Cadic et Mickaël Vallet
[5] « Protéger les internautes, rapport sur la cybercriminalité », groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014
https://www.viepublique.fr/sites/default/files/rapport/pdf/144000372.pdf 6 « Le droit pénal à l'épreuve des cyberattaques », rapport du club des Juristes, avril 2021
https://www.leclubdesjuristes.com/lescommissions/publication-du-rapport-le-droit-penal-a-lepreuvedes-cyberattaques/

Penser la trace dans de nouvelles échelles

OLIVIER RIBAUX
Professeur
École des sciences criminelles
Université de Lausanne

Les signes d'un changement d'échelle

La quiétude de la paisible commune de Rolle, située au bord du lac Léman, entre Genève et Lausanne, est perturbée durant l'été 2021, lorsque des journalistes accèdent sur le *darkweb*, librement, à des données dérobées concernant notamment plus de 5 000 administrés. L'attaque de type rançongiciel a eu lieu dans la nuit du 29 au 30 mai, mais l'incident n'a été révélé que le 20 août par le média en ligne Watson[1]. Les autorités communales semblaient très empruntées quant à la manière de réagir et de communiquer. La syndique (la maire) répondait même maladroitement à la presse, dans un premier temps, qu'il s'agissait d'une « faible attaque », avant d'admettre l'ampleur du problème.

Ce genre de cas est devenu courant. Toutefois, ce qui était un problème réservé aux spécialistes est perçu maintenant directement par chacun d'entre nous. Tous les niveaux de la société sont ainsi déstabilisés. Autrement dit, nous sommes confrontés à un problème de changement d'échelles. La réaction des autorités de Rolle illustre que nous ne sommes pas vraiment préparés à affronter ces nouvelles dimensions. Les processus ne sont pas prêts.

Nous savions que toute technologie qui s'intègre dans nos activités routinières cause des transformations profondes. De l'imprimerie à l'automobile, en passant par le téléphone, la radio ou la télévision, toutes ces innovations ont bousculé nos sociétés. Nous avons toutefois eu besoin d'années de recul pour prendre la mesure de ces bouleversements, puis pour retrouver de la tranquillité. Des effets de bord imprévus et

désagréables ont chaque fois été rendus visibles lorsque les ordres de grandeur ont changé. Nous sommes maintenant dans cette situation. Nous sommes un peu désemparés, car nous manquons de distance.

Il faut se dépêcher pour réagir puisque nous avons déjà raté la période qui aurait pu nous permettre d'anticiper. Dans un cheminement difficile, nous proposons d'abord d'apprendre à penser dans ces nouvelles échelles.

Une représentation du problème

Pour prendre la mesure de l'ampleur du défi, construisons une image qui rend la situation plus intelligible. Le modèle des cinq « V » du *big data* peut constituer une base[2]. Cette approche est archiconnue et peut paraître trop élémentaire pour le lecteur. Mais je ne suis pas sûr qu'il soit toujours bien compris pour son potentiel à nous aider à penser les échelles. Nous sommes en effet toutes et tous d'accord que nous vivons dans un espace avec quelques « 0 » de plus qu'il n'y a pas si longtemps, sur chacune des dimensions du modèle. Ce constat est notamment évident lorsque nous parlons des Volumes de données qui représentent massivement des textes, des images, du son, ou des flux vidéo : des unités comme le Petaoctet, voire l'Exaoctet ou le Zettaoctet ne nous impressionnent plus. La Variété de ces données s'est bien sûr aussi étendue considérablement. Pensons à la diversité des traces numériques que nos activités quotidiennes produisent par l'utilisation des objets connectés et qui sont exigées pour évoluer dans notre société. Dans le modèle, la grandeur suivante exprime la Vélocité, pour garder le « V » de l'anglais *Velocity*, qui nous renvoie à l'échelle temporelle des traitements. À l'inverse des autres « V » en expansion, cette dimension se réduit, mais aussi en ordre de grandeur : possibilités d'exploiter de gigantesques quantités traces à une vitesse difficile à concevoir et nécessité de déléguer à un ordinateur de nombreuses tâches rendues irréalistes pour un être humain. Par exemple, la sécurité de beaucoup de systèmes d'information dépend directement de l'instantanéité de la détection des attaques informatiques par des méthodes qui relèvent de l'intelligence artificielle.

Le « V » suivant renvoie à la Valeur des données. Cette grandeur n'est pas seulement économique, elle est aussi morale et fait référence aux libertés fondamentales. Nous ne sommes pas au bout de nos peines pour intégrer dans une juste mesure les principes de la protection des données, ni même pour évaluer correctement cette valeur. C'est lorsqu'on se les fait voler ou qu'elles sont rendues inaccessibles par malveillance, par une panne ou par une erreur de manipulation qu'on se rend vraiment compte de cette valeur. La dernière dimension porte sur la Véracité : inutile de s'arrêter sur la qualité de l'information qui circule par les réseaux.

Nous sommes déjà convaincus des bouleversements d'échelles sur chacune de ces grandeurs. Imaginons-les maintenant dans un référentiel à cinq dimensions qui dépendent chacune l'une de l'autre, lui-même à considérer dans un écosystème composé d'objets connectés par des réseaux et d'êtres humains. Nous nous plongeons alors dans un espace complètement inconnu, car il doit être pensé à une échelle et à un degré de complexité dont nous n'avons pas l'habitude et pour lesquels nous ne sommes pas forcément constitués naturellement. L'incertitude y règne : on n'y maîtrise pas tout.

Pour mieux percevoir ces bouleversements, on peut aussi se souvenir d'un passé pas si lointain, mais déjà considéré comme ridicule par les jeunes générations. Mon premier Macintosh faisait fonctionner tant bien que mal un ensemble très réduit d'applications basiques, sans disque dur sur un système d'exploitation qui tenait sur une disquette de 640K. Il n'y a finalement pas si « longtemps » puisque c'est encore à vue humaine. On dit qu'une telle évolution a quelque chose d'exponentiel. Ce terme emprunté aux mathématiques est toujours plus utilisé dans le langage courant. Nous avons besoin de cette notion pour exprimer que la progression n'a rien de linéaire : il ne suffit donc pas d'étendre nos anciennes conceptions à la nouvelle situation, car nous sommes projetés dans un espace d'une autre complexité. Nous pouvons maintenant comprendre que, dans ce monde à explorer, plein de promesses, mais aussi de dangers, empiler des normes de sécurité ne suffira clairement pas. Les vieilles recettes peuvent avoir quelques vertus, mais leurs effets resteront limités, car, avec les échelles, c'est la nature des choses qui changent.

Admettre sans paniquer

En apprenant à penser dans de nouveaux ordres de grandeur, nous nous mettons dans de meilleures conditions pour reconnaître l'ampleur du problème. Mais nous allons alors prendre conscience de dangers. Cela ne nous arrange pas et explique les résistances farouches face à des évidences. Comment justifier de remettre en cause, même modestement, notre confort numérique, alors que notre quotidien, nos habitudes, nos loisirs et l'économie en dépendent tellement ?

Les expériences réalisées avec d'autres technologies, pourtant à une échelle réduite, l'ont déjà démontré. Le nombre de morts sur la route provoqué par l'automobile a diminué, mais il subsiste nécessairement des décès : malgré l'évidence, nous ne voulons pas admettre que l'être humain n'est pas physiquement constitué pour se déplacer à la vitesse d'une automobile. On peut contrôler, atténuer les risques, mais il y aura toujours des drames causés par la route, même si chacun d'eux est « inadmissible ».

Concrètement, reconnaître humblement que nous sommes propulsés dans un écosystème complexe plein d'incertitudes pour lequel nous ne sommes pas constitués, c'est donc aussi apprendre à vivre avec l'imprévu et le danger. Cette attitude est toutefois en tension avec l'analyse d'Ulrich Beck[3]. Bien avant l'émergence du big data, ce dernier concevait déjà une évolution d'une «société du risque » qui veut obstinément tendre vers l'impossible « risque zéro ». Si Beck a raison, dans notre nouveau contexte, la panique qui peut résulter d'une perception de risques toujours plus nombreux (en ordre de grandeur) et impossibles à maîtriser, constitue un nouveau risque réel pour la sécurité. Une théorie criminologique nous dit bien que l'insécurité peut entraîner l'insécurité dans un cercle vicieux. L'étape suivante consiste donc à identifier les façons d'atténuer ces inquiétudes.

Vivre avec les nouveaux risques

Par exemple, Dominique Boullier, en se référant à Gérard Berry, rend compte de l'inévitable « bug » qui résulte de la production de systèmes informatisés complexes :

« Le « bug » n'est ni un produit de l'erreur humaine ni un effet d'une quelconque mauvaise intention ou d'économies abusives sur les coûts de développement. Le bug est constitutif de l'informatique des systèmes complexes »[4].

Les grandes institutions comprennent progressivement le fait que le bug, aux conséquences parfois désastreuses, est aussi inévitable, impossible à éradiquer dans notre nouvel espace complexe, que les morts sur la route. Cela ne veut pas dire qu'on ne peut rien faire : le succès des programmes de type *bug bounty* qui consistent à soumettre volontairement les logiciels aux assauts de hackers indique les possibilités de vivre avec le risque, tout en tentant d'en atténuer les effets ou rendre plus rare son actualisation. Dans cette constellation de changements d'échelles, toute une variété de réponses qui vont dans notre sens semblent toutefois émerger.

La notion de risque est forcément liée à l'émergence d'assurances qui offrent toujours davantage de prestations. Qui veut exploiter des données se fait maintenant vite questionner sur la proportionnalité, la nécessité et la transparence des traitements prévus, surtout en matière judiciaire et dans l'économie. Ces concepts fondamentaux de la protection des données s'intègrent concrètement dans nos systèmes d'information. Au-delà, le débat éthique se renforce. La prévention s'organise aussi : les écoles élaborent des programmes d'«hygiène numérique ». Dans différentes organisations, on sensibilise toutes les collaboratrices et tous les collaborateurs à la responsabilité qu'ils ont en tant que gardien·ne des données produites et gérées par l'institution. Sur les plans managériaux et techniques, les standards en matière de cybersécurité, au sens large, se consolident. Le suivi des attaques et des modes opératoires à l'échelle mondiale devient systématique. En milieu judiciaire, les enquêteurs savent exploiter les erreurs commises par des malfaiteurs, eux aussi dépassés par la complexité des systèmes et producteurs inconscients de traces. La sécurité s'intègre directement dans la conception de base des systèmes. Les formations en cybersécurité prolifèrent et la recherche s'active. Des ressources et de nouveaux moyens sont dégagés.

En matière de réponses, des piliers se construisent donc indéniablement. Toutefois, nous avons le sentiment que ces approches restent très

cloisonnées : chacune et chacun reste dans son champ de spécialité pour étendre son approche traditionnelle aux questions numériques, par analogie. Quelle est alors la solidité de l'édifice ?

L'interdisciplinarité

L'analyse des ordres de grandeur nous incite à aborder les nouveaux problèmes en sortant des carcans disciplinaires traditionnels. Ces derniers distribuaient relativement bien le travail dans nos sociétés plus simples. Ils sont en revanche inopérants dans les nouveaux espaces esquissés. Nous ne sommes pas assez « indisciplinés » pour répondre à l'ampleur des changements et aux enjeux. L'interdisciplinarité est souvent affirmée et revendiquée, mais en fait très peu comprise et appliquée. Dans un domaine que nous connaissons bien dans notre École, nous constatons par exemple que l'intégration de la cybersécurité et des poursuites judiciaires n'est de très loin pas aboutie dans les pratiques, la recherche et la formation. L'articulation est pleine de malentendus. La notion de trace, qui peut pourtant jouer un rôle pivot tant elle est au centre des activités humaines et de la question des ordres de grandeur, devrait davantage rassembler en vue de construire une plateforme propice au développement de visions plus intégrées. C'est le rôle de la science forensique.

Boullier analyse cette situation, une fois de plus, avec pertinence : « Les systèmes institutionnels ont permis de maintenir la valorisation des disciplines alors que les questions qui présentent un intérêt sont nécessairement interdisciplinaires. Cette situation est d'autant plus dommageable qu'elle éclipse quiconque travaille à la frontière de deux champs disciplinaires »[5]. Nous avons vécu cela dans les premières années d'une formation interfacultaire de Maîtrise universitaire en droit, criminalité et sécurité des technologies de l'information que nous avions lancée avec des partenaires juristes et en sécurité des systèmes d'information, il y a presque vingt ans. Elle a été ignorée par le système universitaire durant de nombreuses années pour ne prendre un véritable envol que maintenant.

Conclusion

En bref, admettons d'abord les changements d'échelles pour prendre la mesure des enjeux et modifier notre manière de penser. Adoptons simultanément des attitudes courageuses en faisant face aux risques. Enfin, conceptualisons autour de la trace pour construire des visions stratégiques et des réponses opérationnelles réalistes, plus proactives et effectivement inter-disciplinaires. À ce titre, la science forensique, en tant que discipline, doit être davantage reconnue.
Mais dépêchons-nous.

Parution le 17 décembre 2021

[1] https://www.watson.ch/fr/suisse/vaud/323755680-vaud-rolle-a-ete-piratee-par-des-hackers-donnees-volees-sur-le-darknet
[2] BOURANY, T. 2018. Les 5V du big data. Regards croisés sur l'économie, 23, 27-31.
[3] Ulrich Beck. La société du risque. Sur la voie d'une autre modernité. Aubier, 2001
[4] Boullier, Dominique. Sociologie du numérique. Armand Colin. Édition du Kindle, 2016, p 24
[5] Dominique Boullier, Jacques Athanase Gilbert, Daphné Vignon, Armen Khatchatouro. Le grand entretien avec Dominique Boullier, Etudes digitales, Classiques Garnier, p. 247

Mettre fin au « Far West Numérique » fera-il reculer la désinformation en Europe ?

THIBAULT RENARD
Senior advisor
CyberCercle

L'audition de Frances Haugen devant le parlementant européen le 8 novembre 2021 aura été un temps fort de cette fin d'année 2021, qui a vu s'accélérer la lutte contre la désinformation au niveau européen, notamment via la régulation du numérique. Cette ex-cheffe de produit chez Facebook est en effet à l'origine des « Facebook Files », des milliers d'études internes prouvant que, depuis plusieurs années, le GAFAM était conscient, sans en avoir pour autant tenu compte, des effets délétères de ses algorithmes et de son business model sur les sociétés démocratiques. Faisant la démonstration devant les eurodéputés que la désinformation a aussi des racines économiques, et avant d'être également auditionnée au parlement français le 10 novembre, la lanceuse d'alerte américaine a mis en garde contre « la manipulation des élections, la désinformation et les nuisances pour la santé mentale des adolescents », tout en saluant le « potentiel énorme » du projet européen de régulation des géants du numérique. Au travers de la lutte contre la désinformation et de la nécessaire maîtrise des écosystèmes numériques, ce sont en effet de grandes tendances et un changement de cap qui émergent au sein de l'Union Européenne.

Une réponse encore en gestation face à un phénomène « sous surveillance mais pas sous contrôle »

Défendant une approche européenne, la réponse apportée par l'UE dans la lutte contre la désinformation était jusqu'ici bien timide. Hormis quelques actions de sensibilisation comme le projet Youcheck ! devenu cette année Youverify !, son action majeure avait été en 2018 le lancement

du Plan d'Action de lutte contre la désinformation. Le Service européen pour l'action extérieure (SEAE) a ainsi mis en place « trois task forces » réparties en zones géographiques : la task force pour les Balkans occidentaux, la task force South (Moyen-Orient, Afrique du Nord, région du Golfe), et enfin la plus avancée, la task force East StratCom, créée pour lutter contre les campagnes de désinformation russes. Cette dernière a créé le projet EUvsDisinfo qui propose articles, analyses, études, jeux… mais dont la consultation demeure confidentielle. A aussi été créé en mars 2019 un système d'alerte rapide (SAR) pour coordonner rapidement la réponse européenne à la diffusion de fausses informations, voir y riposter, mais il n'a encore jamais été employé. L'apport d'expériences nationales, comme en France la mise en place de Viginum, pourrait cependant être utile à la mise en place de ce système d'alertes. L'ensemble de ces réponses reste de fait trop embryonnaire et trop peu doté de moyens (50 millions d'euros entre 2015 et 2020 consacrées à la lutte contre la désinformation) pour dresser un véritable bilan. La Cour des comptes européenne a parfaitement résumé la situation dans un rapport dédié sorti en 2021 : « Le plan d'action de l'UE n'a pas été mis à jour depuis sa présentation en 2018. Il ne prévoit pas de dispositifs globaux pour faire en sorte que toute réponse de l'UE contre la désinformation soit bien coordonnée, efficace et proportionnée à la nature et à l'ampleur de la menace. En outre, il ne s'accompagnait d'aucun cadre de suivi, d'évaluation. » Dans l'attente d'une volonté politique de faire basculer ce plan dans une autre dimension, c'est donc vers le front de la régulation du numérique que s'est déplacée la lutte contre la désinformation en UE, avec cette fois plus de succès.

De l'autorégulation à la régulation

Pour réduire le flux de désinformation sur les grandes plateformes numériques, l'Europe a misé dans un premier temps sur l'autorégulation de ces dernières, via la publication en 2018 d'un Code de bonnes pratiques contre la désinformation. La désinformation y est définie comme « les informations dont on peut vérifier qu'elles sont fausses ou trompeuses », qui sont cumulativement « créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public » ; et « susceptibles de causer un préjudice public », au sens de « menaces aux processus politiques et d'élaboration des politiques démocratiques et aux

biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité ». La notion de « désinformation » n'englobe pas la publicité trompeuse, les erreurs de citation, la satire, la parodie, ni les informations et commentaires partisans clairement identifiés, et s'entend sans préjudice des obligations juridiques contraignantes, des codes d'autorégulation dans le secteur de la publicité et des normes relatives à la publicité trompeuse. »

Ce code sera signé notamment par Facebook, Google, Twitter, et Mozilla en octobre 2018, suivis par Microsoft en mai 2019 et TikTok en juin 2020. Son évaluation fin 2020 par la Commission européenne, qui conclura à de nombreuses lacunes et la nécessité de le réviser et de le renforcer, ainsi que le récent témoignage de Frances Haugen à la suite des Facebook files de 2021, ont mis en évidence l'échec de cette tentative d'autorégulation des grands acteurs du numérique. La conclusion logique fut donc la nécessité d'entrer dans une logique de régulation s'appuyant sur une règlementation, comme cela fut le cas avec la mise en place du RGPD.

Le Conseil de l'UE a ainsi validé à l'unanimité le 25 novembre 2021 deux grands projets de régulation : le Règlement sur les services numériques (Digital Services Act, DSA) qui vise les réseaux, et notamment les plateformes, et le Règlement sur les marchés numériques (Digital Markets Act, DMA), qui concerne les services en ligne, notamment le commerce.

La nécessité d'un DSA-DMA « fort »

Portés par le commissaire au Marché intérieur, Thierry Breton, avec la vice-présidente de la Commission, Margrethe Vestager, les DSA et DMA, initiés en décembre 2020, visent à mettre de l'ordre dans ce qui apparait au mieux un « far west » pour les uns, une « zone de non droit » numérique pour les autres, la seule certitude étant que ce sont les GAFAM qui y font leur loi. "Ce qui a été mis en lumière par Frances Haugen démontre qu'il y a vraiment une urgence à légiférer et à ne pas faiblir", a ainsi commenté Thierry Breton. La tonalité est donc désormais celle de la confrontation. Ainsi, "les algorithmes remettent en cause nos démocraties en répandant la haine et la division, les géants de la tech remettent en cause nos règles

de concurrence équitable, et les plateformes de marché en ligne remettent en cause nos normes de protection des consommateurs et la sécurité des produits. Il faut que cela cesse. C'est pourquoi nous construisons un nouveau cadre, afin que ce qui est illégal hors ligne le soit aussi en ligne", a déclaré la députée européenne Christel Schaldemose, rapporteuse du texte au Parlement Européen.

Le DSA se veut par conséquent ambitieux en matière de désinformation, mais pas seulement. Sa cible sera les contenus avec de nouvelles obligations et responsabilités appliquées à l'ensemble des acteurs. Services intermédiaires et d'hébergement, plateformes en ligne de commerce, très grandes plateformes… le DSA va concerner près de 10.000 plateformes et intermédiaires. Point essentiel, les règles seront asymétriques : plus grande est la taille, plus strictes sont les règles. Inspiré du RGPD, les amendes se voudront dissuasives avec un seuil minimal des amendes fixé de 4%, pouvant aller jusqu' à 20% du chiffre d'affaires mondial. Le 14 décembre, le DSA a été voté en commission du marché intérieur et de la protection des consommateurs et sera soumis au Parlement en janvier 2022.

Le DMA quant à lui s'attaquera aux marchés numériques, notamment aux abus de positions dominantes et aux contrôles des acquisitions. Considérant les plateformes comme des "contrôleurs d'accès", il définira les pratiques déloyales, les contraintes et les obligations imposées, selon des seuils capitalistiques. Cette fois, les grandes plateformes sont directement visées, car ce sont celles qui, selon le projet, "ont une forte incidence sur le marché intérieur, qui constituent un point d'accès important des entreprises utilisatrices pour toucher leur clientèle, et qui occupent ou occuperont dans un avenir prévisible une position solide et durable". Le 15 décembre, le DMA a été voté par 642 voix pour et 8 contre en séance plénière du Parlement européen, légèrement en avance sur le DSA donc.

Malgré l'activisme du lobby des plateformes, la Computer & Communications Industry Association (CCIA), un DSA-DMA « fort » est donc désormais sur les rails, Conseil de l'UE et Parlement devant désormais négocier pour aboutir à un texte définitif. Dès lors, la Présidence

française du conseil de l'UE aura un rôle déterminant pour faire adopter rapidement et mettre en œuvre la réglementation en 2023, voir fin 2022. Pour Cédric O, secrétaire d'État chargé de la Transition numérique, « la France engagera tous ses efforts pour faire avancer les négociations avec le Parlement européen sur ce chantier législatif structurant et prioritaire pour l'Europe ». Déjà des initiatives nationales se font jour, notamment au Sénat. « Le DSA et le DMA sont l'étalon-or de la régulation numérique, mais nous voulions aller plus loin, être plus défensifs », ont ainsi expliqué Catherine Morin-Desailly et Florence Blatrix-Contat, deux sénatrices qui y portent l'initiative de durcir encore plus le dispositif.

Un rapprochement numérique - audiovisuel

Point incontournable d'un DSA « fort » : un Code de bonnes pratiques contre la désinformation renforcé et contraignant, dont la commission a préconisé en 2021 la révision en profondeur. Signe de l'enjeu, en novembre 2021, alors qu'à l'origine il se limitait plutôt aux grandes plateformes, seize nouveaux signataires potentiels dont Twitch, Adobe, The Bright App, Havas, Reporters sans frontières, le moteur de recherche Neeva… ont été annoncés pour contribuer à sa réécriture. La révision et le renforcement du code est ainsi l'occasion d'assister au positionnement des uns et des autres. Le Comité économique et social européen (CESE), via un avis de son rapporteur Thierry Libaert le 9 décembre 2021 sur les Orientations de la Commission européenne visant à renforcer le code, appelait non seulement à « une politique globale, résolument offensive et intégrant un maximum de parties prenantes », mais soulignait également que « la désinformation ne se réduit pas aux réseaux sociaux. Les médias traditionnels ont aussi une responsabilité majeure ».

Et en effet, il apparait que de plus en plus la frontière entre numérique et audiovisuel s'estompe, et que leur réglementation doit désormais s'aborder de manière globale. Le Groupe des régulateurs européens des services de médias audiovisuels (ERGA), qui regroupe les vingt-sept autorités de régulation nationales de l'UE dans le domaine des services de médias audiovisuels, est désormais partie prenante des débats actuels, et a soumis ses recommandations à la Commission et au Parlement européens en vue du vote du DSA. Après un rapport sur le code et la désinformation en

2019, l'ERGA se positionne en faveur d'un DSA et un code de bonne pratiques « forts », mais surtout, pour que l'application du DSA soit véritablement effective, a appelé le 5 octobre 2021 à une collaboration accrue des régulateurs.

Ce rapprochement, via la régulation, entre numérique et audiovisuel traduit ainsi une tendance de fond. En France, la fusion du CSA et de l'Hadopi, qui donnera naissance le 1er janvier 2022 à l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), pourra à nouveau permettre à notre pays d'être à la pointe sur la thématique et de prendre des initiatives.

La lutte contre la désinformation constitue donc un élément moteur et révélateur d'une irrésistible dynamique européenne enclenchée autour la régulation du numérique et de son articulation avec l'audiovisuel. Cette lutte ne se limite d'ailleurs pas aux seuls DSA-DMA. La problématique des deep fake pourrait aussi trouver une solution dans la proposition du règlement européen sur l'intelligence artificielle du 21 avril 2021, ou celle du règlement sur la gouvernance européenne des données, le futur Data Governance Act (DGA), dont le cœur des enjeux se situe autour du ciblage et du partage des données des individus.

La Présidence française du Conseil de l'UE aura donc un rôle essentiel à jouer en matière d'accélération, mais également de mise en ordre de bataille, de ce foisonnement européen.

Parution le 24 décembre 2021

Table des matières

CyberCercle - 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com - cybercercle.com

Réalisation : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

Directeur de la publication : Bénédicte PILLIET
CyberCercle – 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com – cybercercle.com