CYBER CERCLE

collection

PAROLES D'EXPERTS

2020

PAROLES D'EXPERTS

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

Préface

BENEDICTE PILLIET
Présidente
CyberCercle

Si la situation inédite que nous avons connue en 2020 a eu un effet positif, c'est de nous pousser à sortir de nos habitudes, de nos process installés, pour être agile et innover, pour continuer à avoir ces liens, ces partages indispensables. Pour nous au CyberCercle, cela s'est notamment traduit par l'intensification de notre production d'écrits, avec la création de notre collection d'ouvrages collectifs, Regards croisés, et à travers notre rubrique Paroles d'Experts.

Depuis avril 2020, 33 personnalités de la confiance et de la sécurité numériques, élus, représentants d'entreprises, d'administrations d'Etat, de collectivités, ont accepté de partager leur expertise, leur analyse, leur vision. Je les en remercie très sincèrement.

Chaque semaine nous avons ainsi eu l'honneur de publier des contributions éclairantes sur des sujets traitant de gouvernance, de règlementation, d'éthique, d'enjeux sectoriels, d'évolution de cette société numérique qui rend la confiance et la sécurité numériques d'autant plus indispensables.
Ce sont ces tribunes que vous pourrez retrouver dans ce recueil, dont nous sommes particulièrement fiers.

Premier du genre, il inaugure une série dont nous espérons de nombreux numéros. Et en attendant l'opus 2021, vous pourrez retrouver chaque vendredi une nouvelle contribution dans la rubrique Paroles d'Experts de notre site.

Bonne lecture !

Pandémie : une situation exceptionnelle… aussi sur le front cyber

LOIC GUEZO
Senior Director, Cybersecurity Strategy SEMEA, Proofpoint
Réserviste Cybermenaces Police Nationale

Notre équipe de Recherche sur les menaces cyber (Cyber Threat Intelligence) constate désormais un volume cumulé de leurres électroniques sur le sujet du coronavirus qui en fait la plus grande collection de types d'attaques qu'elle ait vu depuis des années, voire même encore jamais vu sur un thème unique ! Les cybercriminels se nourrissent de perturbations et d'incertitudes et ne perdent pas de temps pour exploiter au maximum les opportunités qui s'offrent à eux. Les attaques de phishing liées au coronavirus sont nombreuses, qu'il s'agisse de celles qui proposent un remède ou de celles qui collectent les informations nécessaires pour alimenter les « bases de données gouvernementales ».
Certaines de ces attaques prétendent même provenir de l'Organisation Mondiale de la Santé (OMS), encourageant les destinataires à télécharger documents, applications ou à se connecter à leur site web.

Toutes invitent les victimes à cliquer sur des liens malveillants et à communiquer leurs identifiants ou d'autres informations personnelles.
Plus de 80 % des menaces utilisent d'une manière ou d'une autre des thèmes liés à la crise sanitaire actuelle. Cela inclut désormais des attaques qui ne mentionnent plus directement le coronavirus dans l'objet ou le corps d'un message, mais qui y font plutôt référence dans les pièces jointes, les liens ou les leurres.

Les messages que nous avons observés sont véritablement le reflet d'opérations d'ingénierie sociale à l'échelle mondiale où chacun d'entre eux est soigneusement conçu pour convaincre les victimes potentielles d'effectuer une action (cliquer sur un lien malveillant, télécharger des pièces jointes

malveillantes ou effectuer un paiement frauduleux...).
Ces exemples de courriels « coronavirus » visent essentiellement à tromper les personnes qui reçoivent ces messages en jouant sur l'humain via l'urgence, la peur voire la promesse d'un remède miracle.
À ce jour, nous avons vu plus de 500 000 messages, 300 000 URL malveillantes, 200 000 pièces jointes malveillantes ayant pour thème le coronavirus dans plus de 140 campagnes (et ce nombre continue d'augmenter[1]). Notre défi est que les attaquants persistent à envoyer des menaces liées au Covid-19 parce que leurs tactiques fonctionnent clairement.

Recours massif au télétravail, partout dans le monde…

Sur les conseils de la communauté médicale, le monde des affaires a appliqué des stratégies numériques pour participer à la limitation de la propagation du virus tout en maintenant la « continuité de service ».
Apple, Amazon, Facebook et Twitter ne sont que quelques-unes des organisations qui ont rapidement restreint les voyages ou imposé le travail à distance par mesure de précaution.
À Londres, le géant pétrolier Chevron a été la première entreprise à renvoyer ses 300 employés chez eux, et de nombreux autres lui ont emboîté le pas de par le monde.
Les cybercriminels ne sont que trop conscients que les entreprises s'appuient plus que jamais sur les outils de collaboration en ligne, ce qui augmente considérablement la taille de leur cible et surface d'attaque correspondante.
Si la connectivité numérique est une bouée de sauvetage pour les entreprises dans des périodes comme celle-ci, elle pose également des problèmes qui lui sont propres. La cybersécurité peut ne pas sembler être une priorité au regard des enjeux de santé mondiale ; mais en fait elle est plus importante que jamais.

Travailler à distance ? Comment être en sécurité !

Le confinement sanitaire a mené de nombreuses organisations à mettre en place le télétravail. Cet usage assure la continuité d'activité... mais il n'est pas sans risque !
La mise en œuvre de ces mesures de télétravail là où il est possible, demandé par le gouvernement français, nécessite pour beaucoup d'employeurs de mettre en œuvre ou de renforcer ces moyens de télétravail dans l'urgence.

Ces moyens d'accès à distance augmentent mécaniquement l'exposition des systèmes d'informations sur l'Internet, dans un contexte où les risques pour leur sécurité sont très élevés avec les découvertes récentes de vulnérabilités critiques touchant certaines de ces solutions d'accès VPN[2].

Enfin, un grand nombre de fraudes se développent qui peuvent notamment cibler et affecter les personnes en situation de télétravail. Il est nécessaire de sensibiliser ses équipes à ces risques qui peuvent les affecter à titre professionnel, mais également personnel.

Tout comme nous avons tous un rôle à jouer pour arrêter la propagation du virus (confinement, gestes barrière, distanciation sociale…[3]), chacun dans son organisation a un rôle à jouer pour en assurer la cybersécurité, en télétravail[4].

En complément des règles d'hygiène numérique déjà connues et mises en œuvre par les organisations (dont appliquer les correctifs de sécurité rapidement et effectuer des sauvegardes hors ligne pour les données critiques) voici cinq conseils simples, à partager autour de vous et appliquer dès aujourd'hui[5] en situation de télétravail :

1 - Réfléchissez à deux fois avant de cliquer sur des liens
En télétravail, soyez conscient que vous ne bénéficiez plus toujours de la protection apportée par le réseau interne de l'entreprise notamment le filtrage des sites web ou de messagerie lors de vos usages personnels. Vous êtes donc plus vulnérable aux phishings. Les courriels de phishing conduisent à des sites web dangereux qui volent des données personnelles, des mots de passe et des informations sur les cartes de crédit. Saisissez plutôt l'adresse d'un site web connu directement dans votre navigateur !

2 - Confirmez toutes les demandes de transaction par téléphone
Évitez les escroqueries par courrier électronique en vérifiant oralement que toutes les demandes de paiement et de transfert de données sensibles sont réelles et autorisées.

3 - Utilisez des mots de passe forts
Ne réutilisez pas le même mot de passe deux fois. Envisagez d'utiliser un gestionnaire de mots de passe pour rendre votre navigation en ligne transparente, tout en restant sûre.

4 - Renforcez le WiFi
Changez le mot de passe par défaut de votre routeur wi-fi domestique et activez le chiffrement WPA/WPA2.

5 - Protégez votre connexion VPN
Les cybercriminels cherchent à se connecter au VPN d'entreprise pour accéder directement à tous les courriers électroniques, aux données et aux applications en nuage. Il appartient à l'organisation de vérifier que les utilisateurs distants sont limités aux seuls systèmes nécessaires et idéalement de mettre en place une solution d'authentification forte (MFA). Trop peu d'organisations ont encore pu déployer les nouvelles architectures d'accès dites « Zero Trust » : si votre accès VPN est détourné, alors c'est bien votre identité numérique professionnelle qui sera alors usurpée !

Enfin, concernant le télétravail ou le nomadisme numérique, il est toujours bon de (re)lire les recommandations de l'ANSSI[6] et de suivre l'actualité du CERT-FR[7].

Et en France, très concrètement ?

Sans oublier les derniers points d'actualité[8] avec du DDOS ou du rançongiciel, la Direction Centrale de la Police Judiciaire a déjà constaté de nombreuses escroqueries sous le prétexte de la crise sanitaire du coronavirus. Par exemple, des groupes criminels organisés ont profité du début de la crise pour usurper l'identité de sociétés produisant ou distribuant des masques de protection et du gel hydro-alcoolique et cibler de nombreuses pharmacies, afin de les inciter à effectuer des commandes et des paiements sur des comptes bancaires français ou étrangers. Ce même type d'escroquerie est également en cours à l'encontre des hôpitaux, des EHPAD et des fournisseurs de matériel de protection médicale. Selon INTERPOL[9], plus de 2.000 bannières publicitaires en lien avec le COVID-19 ont été recensées sur Internet, proposant principalement des masques et des gels hydro-alcooliques

contrefaits et/ou de mauvaise qualité et des activités de démarchage direct par téléphone sont même identifiées.

Plus largement, en cette période de confinement et de télétravail, les entreprises, n'ayant pas l'habitude d'appliquer le travail à distance, sont rendues plus vulnérables aux éventuelles fraudes car les processus habituels, mis en place au sein des sociétés pour lutter contre les fraudes financières, dont celle au changement de relevé d'identité bancaire, se retrouvent désorganisés.

Les fraudeurs peuvent espérer profiter de cette situation de crise sanitaire pour s'immiscer dans les chaînes de paiements des entreprises en ciblant les bons acteurs et percevoir des virements à leur insu…
Aujourd'hui, une stratégie de sécurité centrée sur l'infrastructure se révèle clairement insuffisante ; « protéger les personnes » garantit ici aux entreprises qui ont mis en place de tels programmes une vraie longueur d'avance : que les gens travaillent à domicile ou au bureau, une stratégie de sécurité centrée sur les personnes sera toujours payante...

Restons vigilants et confinés, nous ne sommes qu'au début de la vague…

Parution le 8 avril 2020

[1] https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
[2] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
[3] https://solidarites-sante.gouv.fr/IMG/pdf/coronavirus_400x600_ech_1_option1_003_.pdf
[4] https://www.proofpoint.com/fr/learn-more/working-remotely-awareness-materials
[5] En cas de doute ou de pratiques complémentaires indiquées par votre organisation, il vous appartient de les respecter et de prendre attache avec votre service de support informatique si besoin.
[6] https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/
[7] https://www.cert.ssi.gouv.fr/
[8] https://www.lemonde.fr/pixels/article/2019/11/26/apres-la-cyberattaque-au-chu-de-rouen-l-enquete-s-oriente-vers-la-piste-crapuleuse_6020609_4408996.html
https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html
http://www.leparisien.fr/high-tech/une-vaste-cyberattaque-cible-le-fabricant-de-verres-de-lunettes-essilor-25-03-2020-8287713.php
[9] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19

Cybercontrefaçon et pandémie sanitaire

MYRIAM QUEMENER
Magistrat
Docteur en droit

Selon le Parlement européen et le Conseil de l'Union européenne (directive 2011/62/UE[1]), « la vente illégale de médicaments au public via l'Internet représente une menace majeure pour la santé publique étant donné que des médicaments falsifiés peuvent être distribués au public de cette manière ». L'Union européenne est particulièrement touchée puisque les produits contrefaits représenteraient 6,8 % de ses importations, avec une proportion croissante de produits dangereux pour la santé et la sécurité des consommateurs. La contrefaçon fait perdre 60 milliards d'euros par an à 13 secteurs économiques clés en Europe, d'après l'EUIPO (Office de l'Union européenne pour la propriété intellectuelle). En France, le manque à gagner des entreprises s'élève à 6,7 milliards d'euros, soit 102 euros par an et par habitant, et signifierait la perte de 35 000 emplois tous les ans[2].

De nombreux organismes comme par exemple l'Organisation Mondiale de la Santé (OMS), la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCRF)[3] ou des associations alertent de plus en plus les particuliers sur les dangers des faux médicaments diffusés par Internet[4].

Rappelons tout d'abord que la contrefaçon est le produit résultant de l'usage frauduleux d'un droit de propriété intellectuelle (DPI) dont un tiers est titulaire, sur un territoire où il est protégé. La contrefaçon est souvent considérée à tort comme une fraude sans victime, ce qui ne favorise pas une juste appréhension de son ampleur et de ses effets.

Le commerce de contrefaçons tire profit des avantages que procure la

révolution numérique : il jouit d'une visibilité inégalée en plus d'un anonymat propice Internet et les réseaux sociaux ont également influencé la manière dont les consommateurs en ligne envisagent la contrefaçon.

L'OMS[5] n'utilise pas le terme « Contrefaçon » car la notion de propriété intellectuelle qui sous-tend ce terme est entendue, appréciée et protégée de façon très variable entre les pays, ce qui restreint le champ de la lutte contre les médicaments falsifiés. La falsification est donc la définition la plus étendue, qui englobe les contrefaçons et permet un champ d'action plus large.

Ainsi, de multiples sites illégaux de vente de faux médicaments ont été identifiés en France et à l'étranger et les réseaux criminels profitent de la crise sanitaire pour promouvoir et vendre des matériels et médicaments dangereux. Environ 2 000 annonces en ligne concernant des faux produits pharmaceutiques liés au Coronavirus ont été démantelées par Interpol. Plusieurs milliers de faux masques chirurgicaux saisis.

Récemment Europol a signalé la recrudescence des ventes de prétendus remèdes contre Covid-19 ainsi que des contrefaçons de produits de protection comme les masques ou le gel hydroalcoolique. Des milliers de nouveaux sites se créent tous les jours autour de Covid-19, la délinquance se reportant sur les réseaux pour exploiter les phénomènes de pénuries et de panique partout dans le monde. Selon une étude américaine[6].

La lutte contre la contrefaçon est justifiée par les nombreux dangers qu'elle créent : l'ampleur des risques associés à leur développement : atteintes à la santé et à la sécurité des consommateurs ; dommages portés à l'environnement ; pertes substantielles de ressources fiscales et sociales pour les États ; impacts négatifs sur l'économie et les entreprises en nuisant aux efforts d'innovation et la confiance des consommateurs ; financement du crime organisé et potentiellement d'organisations terroristes.
Interpol a coordonné une opération à l'échelle mondiale ayant permis la saisie de 4 millions de produits et l'arrestation de plus d'une centaine de personnes, ce sont quelques 2 500 liens Internet qui ont été fermés vers des sites vendant ces produits frauduleux.

Le recours à Internet est désormais le premier vecteur de distribution des produits de contrefaçon, porte atteinte aux droits de propriété intellectuelle et complexifie la lutte contre ce fléau. Il a fragmenté la contrefaçon et a été à l'origine d'une multiplication et d'une diversification des *modus operandi* au service des contrefacteurs.

Le commerce en ligne participe largement à la diffusion de ces fraudes avec l'envoi de colis transportant plus de 95 % des articles contrefaisants acquis sur internet. Les sites de vente en ligne sont pour la plupart des hébergeurs ce qui signifie juridiquement qu'ils ne sont pas responsables de l'authenticité des produits proposés par les particuliers. Pour tenter d'enrayer ce trafic, chaque jour les douanes passent au crible des centaines de colis.

Comment renforcer la lutte ?

Il est tout d'abord essentiel de connaître la règlementation de la vente de médicaments en ligne telle que rappelée par l'ordre national des pharmaciens[7] qui tient à jour la liste des sites français autorisés à vendre des médicaments en ligne qui est aussi consultable sur le site du Ministère chargé de la santé. Depuis le 2 janvier 2013, les pharmaciens établis en France, titulaires d'une pharmacie d'officine ou gérants d'une pharmacie mutualiste ou d'une pharmacie de secours minière, peuvent vendre des médicaments sur Internet. Cette pratique est encadrée par le code de la santé publique (articles L. 5121-5, L. 5125-33 et suivants, et R. 5125-70 et suivants du CSP) et par les arrêtés du 28 novembre 2016 relatifs aux bonnes pratiques de dispensation des médicaments et aux règles techniques applicables aux sites internet de commerce électronique de médicaments.

Malgré la création d'un pôle santé publique, composé de juges spécialisés, en 2003, et celle un an plus tard d'un Office central de police judiciaire, chargé de la lutte contre les atteintes à l'environnement et à la santé publique (l'OCLAESP), les procédures de faux médicaments en France sont encore trop rares.

Dans un rapport récent sur les contrefaçons[8], la Cour des comptes préconise de renforcer les obligations juridiques des plateformes numériques pour mieux lutter contre le commerce de contrefaçons et dresse une liste de recommandations dont notamment :

- Accentuer les obligations des sites de e-commerce qui bénéficient, au titre de la directive européenne commerce électronique, d'un régime de responsabilité limitée excluant tout devoir de surveillance et n'impose un retrait des produits illégaux qu'une fois signalé. À la suite des titulaires de droit, la Cour des comptes considère que l'insuffisante diligence des plateformes résultant de ce régime est considérée comme l'un des principaux freins à une lutte efficace contre le développement du commerce de contrefaçons en ligne.
  Pour la Cour, il serait pertinent d'agir dans le cadre des travaux préparatoires à la révision de la directive en question. La Cour des comptes estime qu'il n'est pas suffisant d'employer des lignes directrices ou des accords volontaires non contraignants négociés avec les plateformes.

- Rétablir des contrôles des douanes : faire adopter au niveau de l'Union européenne les textes permettant de rétablir les contrôles des douanes sur les marchandises en transit et transbordement et de mieux lutter contre la cyber-contrefaçon.

- Créer une structure stratégique interministérielle telle une instance de réflexion stratégique et de pilotage opérationnel de la lutte contre la contrefaçon.

Les enjeux en matière de cybercontrefaçon se situent donc sur le terrain de la santé publique et à cet égard, de nombreuses opérations internationales coordonnées par Interpol[9] sont mise en œuvre pour démanteler des réseaux.

Interpol[10] a publié récemment des directives internationales afin d'améliorer la sécurité et l'efficacité de l'application des lois dans le contexte de la pandémie de COVID-19. Conçues conformément aux meilleures pratiques internationales et aux recommandations de l'Organisation mondiale de la santé (OMS), les lignes directrices fournissent des informations sur la manière dont les agents peuvent se protéger et protéger leurs familles, et décrivent les

différents rôles assumés par les forces de l'ordre pendant une pandémie. Les directives mettent également en garde contre les délits liés à la pandémie, notamment l'intimidation et les tentatives de diffusion délibérée, la fraude ou le phishing, la cybercriminalité et la contrefaçon.

Les résultats de l'opération Pangea, menée par Interpol en mars 2020 montrent une augmentation de la mise sur le marché de produits médicaux faux ou contrefaits, parmi lesquels : des masques chirurgicaux jetables, des produits désinfectants pour les mains, des antiviraux, des antipaludéens, des vaccins et des tests de dépistage du COVID-19.

Par ailleurs, l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP) a participé à une opération menée sur Internet destinée à la lutte contre les ventes illicites de produits contrefaisants et/ou ne répondant pas aux normes du marché, opération coordonnée notamment par Interpol et l'Organisation Mondiale des Douanes (OMD). Sur le plan juridique, la convention Medicrime a été adoptée en 2010 par le comité des ministres du Conseil de l'Europe, représentant 47 pays, et ratifiée par la France en 2016. Elle vise à unifier et à durcir la répression, introduit en particulier des circonstances aggravantes lorsque l'infraction a entraîné la mort ou porté atteinte à la santé physique ou mentale de la victime, et fixe des règles de coopération internationale. La Convention sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique de 2011 (« Convention MEDICRIME ») a été ratifiée par 16 pays et signée par 16 autres en Europe et au-delà. La Convention établit un cadre favorisant l'instauration d'une coopération nationale et internationale entre les autorités sanitaires, policières et douanières compétentes tant au niveau national qu'international, l'adoption de mesures destinées à prévenir la criminalité en y associant le secteur privé ainsi que la poursuite effective des délinquants en justice et la protection des victimes et des témoins. Cependant, elle n'est pas ratifiée par assez de pays.

Cette lutte doit aussi s'inscrire dans le cadre également d'une coopération public/privé et internationale indispensable, certaines associations comme l'UNIFAB[11] ou l'IRACM[12] par exemple ayant des relais et d'excellentes connaissances de ces phénomènes.

Il est en conséquence plus que jamais fondamental et urgent de renforcer la lutte contre la contrefaçon largement diffusée en ligne et ce d'autant plus en période de pandémie liée au Covid 19 en instaurant une véritable stratégie globale faite de prévention et de répression.

Parution le 15 avril 2020

[1] https://eur-lex.europa.eu/
[2] https://www.lsa-conso.fr/l-unifab-lance-une-vaste-campagne-anti-contrefacon-en-ligne,324966
[3] https://www.iracm.com/2020/04/france-face-la-proliferation-des-escroqueries-pendant-la-crise-du-coronavirus-la-direction-generale-de-la-concurrence-de-la-consommation-et-de-la-repression-des-fraudes-dgccrf-appelle-la-vig/
[4] https://www.who.int/fr/news-room/fact-sheets/detail/substandard-and-falsified-medical-products
[5] https://www.who.int/fr/
[6] https://www.ajtmh.org/content/journals/10.4269/ajtmh.18-0981
[7] http://www.ordre.pharmacien.fr/layout/set/print/layout/set/print/Les-patients/Vente-de-medicaments-sur-Internet-en-France
[8] La lutte contre les contrefaçons - février 2020 Cour des comptes - www.ccomptes.fr - @Courdescomptes
[9] https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation
[10] www.interpol.int
[11] https://www.unifab.com
[12] https://www.iracm.com/wp-content/uploads/2013/09/A-Rapport-Etude_IRACM_Contrefacon-de-Medicaments-et-Organisations-Criminelles_FR_FINAL-copie-2.pdf

L'identité numérique, c'est aussi un enjeu de souveraineté

JEAN-MICHEL MIS
Député de la Loire

Le contexte de crise sanitaire actuel met en lumière la nécessité des outils numériques et accentue l'importance de développer une solution régalienne d'identité numérique.

L'identité numérique peut être définie comme l'ensemble des traces numériques d'un individu ou d'une collectivité. La notion d'identité vit des mutations profondes, dans le contexte actuel de multiplication des services en ligne et de la dématérialisation croissante des démarches administratives. Prérogative de l'Etat depuis la création de l'état civil en 1792, la gestion de l'identité est formalisée par la délivrance d'un certain nombre de documents administratifs (passeport, carte d'identité, carte d'assurance maladie…). De nombreux secteurs ont besoin d'une identification de garantie élevée de personnes : le secteur bancaire, le secteur des jeux en ligne, les transports, le secteur médical…

La France dispose, depuis 2016, d'un premier dispositif d'identité numérique, « France Connect », qui permet de s'authentifier par un service en ligne par le biais d'un compte préexistant sur un service public. Afin de renforcer la sécurité de ce dispositif, une solution d'identité numérique régalienne appelée « Alicem » (authentification en ligne certifiée sur mobile), a été développée par le Ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS). Cette solution vise à permettre aux utilisateurs de prouver leur identité de manière sécurisée sur internet, grâce à un logiciel de comparaison faciale. Elle n'est pas obligatoire.

De plus, le Règlement « eIDAS » du 23 juillet 2014 vise à accroître la

confiance dans les transactions électroniques au sein de l'Union européenne. Ce cadre européen en matière d'identification électronique et de services de confiance ne serait que renforcé par des solutions régaliennes d'identité numérique.

Enfin, avec le Règlement du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union, la France est invitée par l'Union européenne à doter ses ressortissants d'une carte nationale d'identité électronique, à partir de l'été 2021. Ce nouvel usage est une opportunité de se questionner sur une utilisation de l'identité en ligne pour son éventuelle utilisation pour certains services de l'Etat ainsi que pour certains services privés.

Plusieurs Etats européens ont déjà engagé des procédures visant à la mise en place d'une identité numérique. La France semble plutôt en retard dans ce domaine, notamment parce qu'elle démontre une sensibilité forte au respect des libertés fondamentales, et, notamment, le respect de la vie privée.

Les enjeux de l'identité numérique sont multiples.

Il s'agit, tout d'abord, de clarifier et d'inclure tous les citoyens dans un débat qui concerne un sujet technique, mais important. Puisqu'elle renvoie aux traces laissées par un internaute dans la sphère numérique, l'identité numérique permettrait à chacun de garantir sa véritable identité sur internet. Il existe aujourd'hui un trop grand nombre de sites demandant au grand public de prouver son identité en ligne. Le mot de passe, moyen d'identification le plus répandu, n'est pas suffisamment protecteur des données identificatrices qu'il doit couvrir. Par une uniformisation du biais par lequel l'identité réelle de la personne est assurée en ligne, l'identité numérique lève le problème de la multiplication des mots de passe et offre plus de garanties de sécurité aux citoyens. L'identité numérique protégera les citoyens contre les risques croissants d'usurpation d'identité en ligne.

L'identité numérique est également un vecteur de réduction de la fracture numérique entre les citoyens, en simplifiant les démarches administratives par la numérisation. L'accès aux services numériques sera facilité par une identité numérique unique et uniformisée pour tous les services en ligne,

c'est-à-dire, sans avoir recours à de nouveaux identifiants à chaque fois.

Une solution régalienne d'identité numérique offre également une sécurité supplémentaire aux citoyens pour conserver leurs données personnelles. Chaque citoyen saura sur quelle structure sont enregistrées ses données et l'accès à celles-ci sera subordonné à la confirmation de l'identité par des éléments biométriques de l'individu.

Enfin, créer une identité numérique en France est un enjeu de souveraineté. L'avance prise par les grands acteurs américains du Web ainsi que par les GAFAM est telle qu'il devient urgent de permettre à notre pays de conserver une souveraineté nationale sur l'identité des internautes. L'Etat doit garantir l'identité des personnes dans la sphère numérique, de la même manière qu'il le fait dans le monde physique. Il faut déployer les services le plus vite possible, avant que des entreprises privées ne le fassent.

Toutefois, le déploiement d'une identité numérique vient nécessairement poser la question des risques et limites éthiques inhérents à cette technologie. Pour assurer le développement d'une identité numérique basée sur la confiance, plusieurs principes peuvent être mis en place :

- contrôle de l'outil technologique par la mise en place d'un cadre juridique approprié et du suivi des avis de la CNIL
- appropriation
- égalité de traitement
- transparence des données utilisées et des modalités de conservation de celles-ci
- protection de la vie privée : pour cela, il convient de déterminer en amont quelles données seront consultables et par qui
- inclusion numérique, formation pour apporter des solutions aux personnes qui n'utilisent pas de services en ligne

Tandis que le Gouvernement avait lancé en 2018 une mission interministérielle consacrée au déploiement d'un parcours d'identification numérique sécurisé, l'Assemblée nationale a également souhaité se saisir du sujet. Je suis, depuis quelques semaines, rapporteur de la mission d'information sur l'identité numérique aux côtés de Christine Hennion et présidée par Madame Marietta Karamanli.

Cette mission a déjà lancé sur le site de l'Assemblée, une consultation citoyenne à laquelle chacun est invité à participer sur le sujet de l'identité numérique, jusqu'au 19 avril 2020.

Dans le contexte actuel nos travaux sont suspendus. Le succès de la diffusion d'une solution d'identité numérique dépend fortement de la capacité des citoyens à s'en saisir pour leurs usages de la vie quotidienne. La consultation citoyenne organisée doit ainsi permettre de recueillir l'opinion des citoyens, afin de renforcer l'adéquation entre les attentes et besoins des citoyens et les caractéristiques de la solution d'identité numérique proposée.

Cette mission présentera des recommandations sur l'identité numérique en prenant en compte les avis des citoyens sur des questions d'éthique, de confiance, de sécurité et d'inclusion des citoyens et de protection de leurs droits.

Parution le 23 avril 2020

Télétravail : échanger en gardant le contrôle de ses données

CHARLES BLANC ROLIN
RSSI
GHT 15

La situation sans précédent que nous vivons a clairement fait augmenter nos besoins en matière de télétravail et d'échanges numériques. De nombreuses organisations n'étaient pas prêtes, ou pas dans une telle mesure en tout cas. Accès Internet, VPN ou solution de bastion, partage de fichiers, vidéo-conférences, etc... Quelle DSI peut prétendre avoir tout anticipé et permis à l'ensemble des employés de « télétravailler » en toute sécurité ?

Dans le secteur de la santé, nous n'étions, évidemment, pour la plupart, pas préparés à mettre en place une telle organisation de travail à distance pour un aussi grand nombre. À notre « décharge », la majorité des activités, et notamment celles qui composent le cœur de métier de nos établissements, ne peut pas être réalisée à distance. Malgré tout, de nouveaux besoins numériques se sont fait sentir, en particulier les vidéo-conférences, parfois même d'un bout à l'autre de l'établissement, ainsi que les partages « en masse » de fichiers.

Beaucoup ont opté pour les solutions « faciles » proposées par les géants américains du numérique, comme Teams, la solution collaborative de Microsoft qui permet entre autres le partage de fichiers, ainsi que la mise en place de vidéo-conférences, et qui n'a d'ailleurs pas résisté à l'effet Covid-19[1] . L'application de vidéo-conférence Zoom a elle aussi connu la rançon du succès en se faisant décortiquer par les experts en sécurité de la planète. Les résultats ont de quoi faire peur, plusieurs vulnérabilités, un discours commercial pas très franc, un chiffrement très loin d'être digne d'un vieux décodeur Canal + et des données qui transitent par la Chine[2]…

Entre le Cloud Act américain et le niveau de protection des données à caractère personnel chinois reconnu inadéquat par l'Union Européenne, il n'y a pas de quoi se réjouir.

Vous me direz, tout dépend des usages, tant que des informations sensibles ne sont pas échangées, cela ne pose pas vraiment de problèmes.

Dans le cas contraire, quelles solutions utiliser sans perdre le contrôle total de nos données ?

Quitte à investir dans des solutions, pourquoi ne pas se tourner vers des produits français, et cerise sur le gâteau, reconnus par notre Agence Nationale de la Sécurité des Systèmes d'Information ?

Côté partage de fichiers, Oodrive propose des services Saas qualifiés Secnumcloud par l'ANSSI[3], et pour ne rien gâcher, la société est également certifiée Hébergeur de Données de Santé[4], ce qui permet à nos établissements d'y déposer en toute légalité, des données qui concerneraient nos patients.

Sur le plan vidéo-conférence, Tixeo propose une solution disposant d'une certification CSPN, ainsi que d'une qualification ANSSI[5]. Elle est disponible en mode Saas, mais également « On Premise ». Elle pourrait donc permettre au-delà des conférences, la réalisation de télé-consultations en hébergement interne ou HDS. C'est à ce jour, une des rares solutions que je connaisse, proposant un véritable chiffrement de bout en bout, et comme la Statue de la Liberté, elle est 100 % française !

Au-delà des solutions commerciales, les solutions libres peuvent également venir à la rescousse !

Jitsi est une excellente solution de vidéo-conférence plébiscitée par Edward Snowden en personne[6] et notamment utilisée par la Direction Interministérielle du Numérique (DINUM)[7]. Elle fait également partie des produits recommandés depuis plus de deux ans déjà dans le SILL (Socle interministériel des logiciels libres)[8], rejointe cette année par la solution BigBlueButton orientée éducation.

Jitsi ne permet pas encore le chiffrement de bout en bout, même si cela semble être « dans les tuyaux »[9]. En revanche, il permet un chiffrement du flux via le protocole DTLSv1.2, pour lequel il est possible d'utiliser un certificat créé à l'aide d'OpenSSL ou, mieux encore, un certificat renouvelé régulièrement et reconnu par l'autorité Let's Encrypt, à l'aide de l'excellent outil Certbot[10]. Par défaut, le mécanisme d'authentification pour la mise en place d'une réunion, n'est pas activé également, ce qui peut très rapidement poser des problèmes de performances et de bande passante si tout le monde s'invite sur votre serveur. Seul point noir de la solution, la création de comptes utilisateurs et le changement de mot de passe ne peuvent être réalisés que depuis un terminal, en lignes de commandes. Des clients existent pour tous les systèmes d'exploitation, mais comme la solution repose sur le protocole WebRTC, l'utilisation d'un simple navigateur compatible WebRTC, tel que Firefox ou Chromium peut suffire.

Pour tester la solution ou pour se « dépanner » en cette période de crise, l'hébergeur français Scaleway propose gratuitement des instances Jitsi en libre-service[11].

La solution collaborative Nextcloud qui n'a rien à envier à celles proposées par les GAFAM, après une année en observation dans le SILL 2019[12], fait désormais partie des solutions recommandées[13]. Le Ministère de l'Intérieur a d'ailleurs opté pour cet excellent outil l'an passé[14]. La solution téléchargeable gratuitement (licence AGPL) peut être installée « On Premise » ou pourquoi pas sur une infrastructure HDS. Pour l'avoir essayée, j'ai été réellement bluffé par la solution. Personnalisable à souhait avec plus d'une centaine d'applications disponibles, au-delà du partage de fichiers ou de répertoires d'upload, elle permet notamment la mise en place d'une authentification à deux facteurs (mail, u2f…), chiffrement des fichiers côté serveur, affichage des checksums des fichiers, lecteur de fichiers Keepass, gestionnaire de mot de passe intégré, lecteurs intégrés d'images, de vidéos ou de sons et même lecteur DICOM, permettant de visualiser des images médicales.

Clou du spectacle, tout comme, Teams, une solution de vidéo-conférence basée sur WebRTC et s'appuyant sur Coturn (STUN/TURN) est aussi intégrée à la solution, avec l'application Talk. Contrairement à Jitsi, le

chiffrement de bout en bout est natif[15], et ce, même s'il n'est pas activé dans Coturn qui sert uniquement à la « mise en relation » entre deux terminaux.

Que ce soit avec une solution commerciale ou libre, « télétravailler » de façon souveraine n'est qu'une question de volonté.

Parution le 4 mai 2020

[1] https://www.zdnet.fr/actualites/microsoft-teams-en-panne-en-europe-39900753.htm
[2] https://www.dsih.fr/article/3710/covid-19-et-video-conference-pourquoi-zoom-n-est-pas-la-solution-ideale.html
[3] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[4] https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies
[5] https://www.ssi.gouv.fr/qualification/tixeo-server-version-11-5-2-0/
[6] https://www.wired.com/2017/02/reporters-need-edward-snowden/
[7] https://www.numerique.gouv.fr/produits-services/webconference-etat/
[8] https://www.mim-libre.fr/wp-content/uploads/2020/05/sill-2020.pdf
[9] https://jitsi.org/blog/e2ee/
[10] https://certbot.eff.org/
[11] https://ensemble.scaleway.com/
[12] https://www.mim-libre.fr/wp-content/uploads/2019/05/sill-2019-pub.pdf
[13] https://sill.etalab.gouv.fr/fr/software?q=nextcloud&year=2020
[14] https://nextcloud.com/press/pr20190827/
[15] https://nextcloud.com/talk/
https://github.com/coturn/coturn/issues/33#issuecomment-467344762

Coronavirus : la cybersécurité conjugue résilience et relance

JEAN-CHARLES LARSONNEUR
Député du Finistère

La crise sanitaire que nous traversons est inédite par sa soudaineté, son universalité et sa violence. Si elle agit comme un révélateur de nos vulnérabilités dans le domaine cyber, elle représente également un moment de prise de conscience dont nous devons collectivement nous saisir, ainsi qu'un puissant catalyseur de solutions plus sûres, plus résilientes et plus souveraines. Outre nos armées, les opérateurs d'importance vitale, les secteurs de la santé, de la grande consommation, des banques, des médias, mais aussi les particuliers ont été touchés par une recrudescence d'actes malveillants : déni de service, campagnes d'hameçonnage, diffusion de programmes espions ou fausses nouvelles. En grec ancien, la krisis renvoie à la notion de pic ou d'acmé, mais aussi à l'action de trier, de passer au crible. De cette crise, nous devons tirer les enseignements pour mieux aborder le monde d'après.

Le confinement a d'abord engendré une intensification du recours au télétravail. Les mesures de distanciation sociale et l'évolution des pratiques donnent à penser que ce phénomène sera durable. Or, les vulnérabilités que le travail à distance crée dans les systèmes d'information sont largement exploitées par les cyberattaquants. À l'évidence, nos entreprises et institutions avaient insuffisamment anticipé cette tendance et continuent parfois de sous-estimer les risques, notamment de demandes de rançon, d'escroqueries ou d'espionnage. Le recours massif à des outils comme Zoom en est une illustration. Cette application a démontré de sérieuses fragilités, poussant des États comme Taïwan à bannir son utilisation par les opérateurs publics. Au début de la crise, les première auditions à huis-clos de la commission de la Défense et des Forces armées de l'Assemblée nationale ont été organisées via ce logiciel. La mobilisation des députés et des acteurs institutionnels a permis

qu'une solution souveraine lui soit rapidement préférée (Orange Videopresence). Il existe en outre des solutions alternatives poussées par l'ANSSI comme Tixeo. Dans le domaine des messageries instantanées, on peut regretter l'utilisation de WhatsApp à des fins professionnelles quand d'autres applications offrent des communications plus sécurisées (Citadel, Signal). Les projets de cloud et de messagerie souveraine (Tchap) sont aujourd'hui plus que jamais une nécessité. En somme, ce virage digital est l'opportunité de diffuser plus largement une culture et une conscience du risque cyber, par des actions de formation, de pédagogie et de prévention en s'appuyant sur les outils existants comme la plateforme cybermalveillance.fr. Pour les entreprises, le cyber ne doit plus être perçu comme une contrainte et une charge financière mais comme un investissement au service de la performance économique.

Le deuxième enseignement que l'on peut tirer se trouve dans la vulnérabilité de certains établissements publics (hôpitaux, collectivités territoriales…). Nombre d'entre eux ont été la cible de cyber malveillances. Dans la mesure où l'on ne peut exclure de nouvelles vagues épidémiques, il serait déraisonnable de faire l'économie d'investissements importants dans la cybersécurité du parc hospitalier, sous peine de paralysie. À cet égard, je salue la constance avec laquelle les gouvernements ont soutenu l'ANSSI, responsable de la cyberprotection et de la lutte informatique défensive. Entre 2015 et 2020, les effectifs de l'ANSSI sont passés de 460 à 692 ETP. L'objectif est de les porter à 750 pour un fonctionnement optimal selon le directeur général. Les ressources budgétaires ont suivi une évolution analogue (+ 62 % en 3 ans, 49,6 millions d'euros en 2018). La crise économique ne doit pas enrayer cette montée en puissance. Le BSI (son équivalent allemand) dénombre 850 agents et dispose d'un budget d'environ 110 millions d'euros par an. Enfin, outre ce levier financier, je soutiens la mise en place de « référents cyber » au sein des établissements publics et des collectivités locales pour améliorer la prophylaxie numérique et la diffusion de bonnes pratiques, en lien avec les représentants locaux de l'ANSSI.

Par ailleurs, les fausses informations prolifèrent dans le terreau fertile que constituent les capacités de viralité offertes par les réseaux sociaux et la défiance de nos concitoyens. Certaines relèvent de la stratégie d'influence de puissances étrangères, d'autres du complotisme. Mais la frontière entre liberté

d'opinion, propagande et désinformation est ténue. L'État a trop longtemps laissé faire. Cette majorité a œuvré pour que voie le jour un dialogue renforcé avec les grandes plateformes, noué au niveau interministériel sous l'impulsion de l'Ambassadeur du Numérique. La responsabilité des réseaux sociaux et des hébergeurs est désormais engagée. Facebook a ainsi mis en place un onglet avec des informations vérifiées et référencées, Twitter ayant pour sa part censuré certains tweets du président brésilien Jair Bolsonaro.

Cette dynamique doit être activement poursuivie et entretenue.

Enfin, la loi de programmation militaire 2019-2025 prévoit la création de 1 500 postes et un montant de 1,6 milliard d'euros au profit de la cyberdéfense, par exemple sur le pôle de Bruz en Bretagne. Nous devrons, je le souhaite, aller plus loin dans le domaine de la cybersécurité maritime, en faisant fond sur les dispositifs existants, notamment à Brest (MICA Center, MSC-HOA pour la Corne de l'Afrique) ou encore à Toulon. En dépit des inévitables tensions à venir sur les budgets nationaux, je plaide pour préserver ces orientations dans l'actualisation de la loi de programmation militaire en 2021.

Vous l'aurez compris, les défis sont immenses, et la majorité présidentielle pleinement à la tâche pour les relever.

Parution le 8 mai 2020

À l'ère du télétravail, six axes pour assurer la continuité des activités métier

CHRISTOPHE AUBERGER
Directeur technique
FORTINET

Les entreprises font plus que jamais appel au télétravail, une tendance commune à nombre de secteurs d'activité. Si ce travail à distance présente des avantages concrets à court terme, les dirigeants d'entreprises doivent aussi miser sur ce télétravail et sur les technologies associées pour créer de nouvelles opportunités et évoluer à plus long terme. Le télétravail n'est pas perçu comme le moteur d'un changement radical dans la façon de concevoir les architectures de sécurité des réseaux corporate, mais plutôt comme une évolution continue susceptible de faire avancer les entreprises et leurs professionnels de la sécurité. Ainsi, les décisions de sécurité dans l'optique d'accompagner le télétravail pourraient bien contribuer à la résilience contre les futures cyberattaques.

Tirer parti des technologies existantes pour encourager le télétravail

Voici 6 axes sur lesquels les dirigeants d'entreprise sont invités à se pencher pour accompagner leurs collaborateurs, sécuriser leur activité corporate et favoriser un travail hors du traditionnel siège social d'entreprise, sans pour autant devoir investir dans de nouveaux sites.

1. Assurer la confidentialité de la connectivité
Les télétravailleurs peuvent se connecter à distance à leur entreprise via un logiciel de VPN (réseau privé virtuel). Ce logiciel, installé sur le PC de chaque collaborateur, assure la confidentialité des connexions vers les applications et données distantes des entreprises, contribuant ainsi à la protection des ressources.

2. Privilégier l'authentification à facteurs multiples
Si les télétravailleurs connaissent certaines carences au niveau des fonctions de sécurité, l'authentification à facteurs multiples (ou MFA pour Multi-Factor Authentication) s'impose pour protéger les données. Le MFA peut se déployer en associant un élément en possession de l'utilisateur (un jeton ou un smartphone) avec un élément connu par cet utilisateur (un mot de passe par exemple). Cette approche active un niveau supplémentaire de sécurité qui valide l'identité d'un collaborateur lors de sa connexion.

3. Tirer parti des points d'accès sans fil et des pare-feux
Les entreprises qui souhaitent améliorer leurs stratégies de télétravail sont invitées à tirer parti de points d'accès sans fil et de pare-feux simples à déployer sur les sites distants. Préconfigurées avant d'être expédiées, ces solutions s'installent automatiquement sur site, assurant ainsi la continuité des activités et un support pour les travailleurs distants qui ont besoin de performances et de fonctionnalités supplémentaires.

4. Renforcer l'agilité des chemins de communication
Les bureaux centralisés offrent généralement des liens de communication sécurisés au niveau de leur siège social pour accueillir les nombreux utilisateurs qui y travaillent. Avec un SD-WAN, les entreprises peuvent choisir avec agilité et sécurité le meilleur chemin de communication pour leurs utilisateurs, et ce, à tout moment. Cette stratégie accompagne l'évolution des modes de communication des télétravailleurs, ces derniers étant toujours plus nombreux.

5. Tirer le meilleur parti du cloud
Les équipes qui n'ont plus accès aux ordinateurs fixes de leur siège social peuvent déployer des applications dans le cloud, similaires à celles installées sur leur PC au bureau. L'ajout de solutions de cybersécurité, pour notamment prendre en charge les connexions SSL sécurisées de n'importe quel navigateur vers le cloud, permet aux utilisateurs d'accéder en toute sécurité à ces applications et aux données associées stockées dans le cloud, et ce, sans alimenter la complexité au niveau des utilisateurs ou de l'équipe de sécurité.

6. Améliorer ses compétences en toute autonomie
Un des avantages du télétravail est d'offrir davantage de temps supplémentaire aux collaborateurs, ces derniers n'ayant plus à se déplacer chaque jour au bureau. Comment tirer parti de ce temps ? Pourquoi ne pas en profiter pour renforcer ses compétences ? Il est par exemple possible de se former en ligne à la cybersécurité afin de garder une longueur d'avance sur les menaces. En réaffectant ce gain de temps qu'on ne gaspille plus dans des déplacements parfois interminables, les dirigeants tout comme les collaborateurs peuvent développer un savoir-faire pouvant se révéler particulièrement utile dans le futur.

Perspectives

En mettant l'accent sur ces six points, les entreprises vont pouvoir définir un modèle de télétravail efficace et sécurisé. Ces évolutions associent les infrastructures du cœur de réseau avec des solutions de connectivité tierces pour étendre la périphérie de réseau au-delà du bureau de travail classique. En optant pour une stratégie de cybersécurité pertinente couvrant la périphérie, le cœur de réseau et le cloud, les entreprises assurent la continuité de leurs activités sur leurs sites distants tout en jetant les bases des méthodes de travail et des architectures à venir.

Parution le 15 mai 2020

Le port du futur sera un port « smart » et cyber sécurisé !

JEROME BESANCENOT
Chef du Service du développement des Systèmes d'Information
HAROPA Port du Havre

Le secteur portuaire : une dépendance au numérique, une interdépendance face au risque cyber

Face à la massification du transport maritime, un facteur clé de la compétitivité des ports repose désormais sur la capacité de leurs systèmes d'information à automatiser et traiter de volumineux flux d'information liés aux marchandises, aux passagers et aux navires.

Ces traitements sont opérés au travers du système d'information portuaire communautaire appelé communément « Port Community System » (PCS) et reposent sur des échanges dématérialisés de données en EDI de type BtoB interconnectant l'ensemble des parties prenantes de la communauté portuaire. Le volume échangé représente plusieurs centaines de millions de transactions par an pour le port du Havre.

La communauté du port rassemble de nombreux professionnels des secteurs portuaires, maritimes et aussi industriels ; de par sa nature, elle se caractérise par une grande disparité de sensibilisation et de culture face au risque cyber. Chaque acteur intervient de manière synchronisée dans la chaîne d'approvisionnement logistique : l'ensemble des opérations est coordonné par le biais du PCS. Ceci induit de fortes interdépendances entre les professionnels, en matière de règle d'hygiène cyber ; il s'avère fondamental de partager les bonnes pratiques numériques pour sécuriser l'ensemble de l'écosystème.

Cette dépendance de l'activité portuaire au monde numérique s'est

considérablement accrue ces dernières années, du fait de l'automatisation qui est devenue une nécessité économique et un enjeu de performance. Le recours aux nouvelles technologies permettant de réduire les coûts, de fiabiliser le suivi des opérations portuaires et de mieux anticiper les interventions des acteurs de la logistique.

À ce titre, le concept du « SmartPort », présente un port « hyper-connecté » s'appuyant sur les technologies de l'internet des objets (IoT), sur le bigdata et sur l'intelligence artificielle (IA) qui laisse augurer une plus grande agilité due au pilotage de l'activité par la donnée numérique. Dans le même temps, l'augmentation de la surface d'exposition aux cybermenaces et du risque de leur propagation est le revers de la médaille.

Il devient donc nécessaire de s'extraire d'un fonctionnement qui reposerait uniquement sur une analyse en silo des risques de cybermalveillance, en combinant les analyses et en partageant davantage au niveau de la communauté portuaire une même stratégie globale de résilience de l'écosystème. Dans cet objectif, il convient de mettre en œuvre une véritable synergie de place afin d'amener l'ensemble des acteurs à se pencher conjointement sur ce sujet sensible, trop souvent considéré comme une affaire de spécialistes en informatique et rarement appréhendé sous sa dimension organisationnelle.
Force est de constater que le secteur portuaire n'est plus épargné par les cyberattaques et certaines d'entre elles ont récemment eu de lourdes conséquences pour plusieurs ports mondiaux majeurs, notamment sur le plan financier et la continuité d'activité.

Le Programme « SmartPortCity » de HAROPA Port du Havre : un projet innovant en matière de cybersécurité portuaire

Pour faire évoluer les lignes favorablement et pour se mobiliser de manière proactive sur ce sujet complexe, HAROPA Port du Havre a initié, au sein du programme « SmartPortCity », lauréat du TIGA-PIA3 (Territoires d'Innovation Grande Ambition - Plan d'Investissement d'Avenir), un projet d'innovation en matière de cybersécurité portuaire, maritime et industrielle avec l'ensemble des parties prenantes du territoire havrais dont la

communauté Urbaine Le Havre Seine Métropole, la communauté des professionnels portuaires de l'UMEP (Union Maritime et Portuaire), les industriels de l'association Synerzip et la SOGET leader mondial de solution PCS et éditeur de la plate-forme collaborative digitale S)One.

Le port du Havre est le premier port à conteneurs pour le commerce extérieur de la France et aussi le 1er port touché sur le range nord-européen. Il offre les meilleurs temps de transit entre l'Europe et le reste du monde et se positionne comme un corridor européen majeur. Localisé à l'embouchure de la Seine, il est relié directement aux ports de Rouen et Paris par route, fleuve et rail. Ces trois ports sont désormais regroupés sous HAROPA, portant une ambitieuse stratégie de développement et d'innovants services digitaux à l'échelle territoriale de l'axe seine. Dans ce contexte, la sûreté est une orientation clé pour HAROPA – Port du Havre qui est la première autorité portuaire européenne à avoir obtenu la certification ISO 28000 au titre de la sûreté de la chaine d'approvisionnement.

Le projet de plateforme de cybersécurité portuaire, maritime et industrielle vise à poursuivre cette stratégie de renforcement du port dans une dimension de compétitivité et d'attractivité, tout en assurant une amélioration du niveau général en matière de cybersécurité avec un enjeu double.

Le premier enjeu consiste à bâtir une démarche qui apportera de la visibilité aux clients du port sur le dispositif déployé de résilience de l'écosystème aux cybermenaces. Comme un service à valeur ajoutée au bénéfice de ses clients, le port améliorera sa compétitivité justement du fait de la prise en compte de la dimension cyber dans sa stratégie de développement. Cet enjeu est caractérisé par une image forte de construction « **du Havre : port Cyber-sûr** ». Il ne s'agit pas seulement d'identifier ce que le port pourrait « perdre » en cas de non-conformité cyber, mais plutôt de souligner ce qu'il gagne et la façon dont cet argumentaire devient un élément de décision susceptible d'apporter des trafics et de l'activité au port du Havre.

Le deuxième enjeu est d'aller au-delà de la stratégie de résilience en développant une culture d'innovation sur la cybersécurité portuaire, maritime et industrielle. Cela consiste à élargir les compétences des acteurs et à attirer de nouveaux talents sur le territoire dans cette discipline. Il s'agira

essentiellement d'impliquer les acteurs pour créer une valeur ajoutée de type filière sur la promotion des métiers de la cybersécurité et favoriser ainsi la mise en œuvre de partenariats public-privé (PPP) dans ce domaine. L'idée est de susciter auprès de différents acteurs du monde numérique et de la recherche en cybersécurité, une meilleure prise en compte de la « Security by design » dans le développement informatique des solutions portuaires, dans la certification des installations technologiques, ou encore un meilleur niveau de formation initiale et continue. Cet enjeu vise à améliorer l'attractivité du territoire et à contribuer à fixer un savoir-faire local en faisant « **du Havre le lieu d'amélioration de la cybersécurité** » de ses entreprises.

La cybersécurité, un facteur de compétitivité pour HAROPA Port du Havre et pour l'écosystème portuaire français

Le calendrier du projet a été défini pour établir en première priorité la gouvernance cyber de la plateforme en déclinant de manière opérationnelle des mesures pragmatiques, adaptées aux besoins du port et répondant à une gestion raisonnée des vulnérabilités : le piège d'une potentielle distorsion de concurrence avec d'autres ports devra être écarté, en s'assurant en permanence que les mesures adoptées ne soient pas disproportionnées ou trop difficiles à porter. Chaque entreprise, quelle que soit sa structure ou son organisation, deviendra alors un acteur essentiel de cette gouvernance et participera à son animation. Dans cette perspective, les évènements organisés depuis 2018 au Havre, en partenariat avec le CyberCercle, en faveur de la sûreté portuaire et la sécurité numérique, ont permis avec succès de sensibiliser l'ensemble des acteurs de la place portuaire sur des thématiques de réglementation, de sensibilisation, de gouvernance ainsi que d'innovation.

En parallèle, un échéancier pour les trois ans à venir, sur la base de cette gouvernance, va établir une feuille de route de création d'un portefeuille de services mutualisés d'assistance aux entreprises comprenant de la sensibilisation, de la formation, de l'analyse et des audits de risque, de la gestion de crise, de la recherche et innovation, un SOC portuaire (Security Operation Center) et une place de marché pour faciliter l'accès aux offres techniques de sociétés cyber-spécialisées reconnues.
La clé du succès du projet repose ainsi principalement sur la capacité collective

à valoriser véritablement cette initiative sous l'angle du progrès, en dépassant le stade simpliste où elle ne serait perçue que selon son principe d'obligation réglementaire. La cybersécurité peut alors être appréhendée comme une opportunité permettant au port d'améliorer sa compétitivité en combinant l'accélération de la transformation digitale et sa sécurisation numérique. Elle devient alors un critère positif, et donc, un argument commercial garantissant la « compliance » de l'écosystème portuaire havrais. Cette « compliance » va pouvoir se valoriser auprès des entreprises de la place, en termes d'attractivité auprès des clients du port, permettre potentiellement de conquérir des parts de marché ou plus pragmatiquement par exemple, de réduire les primes d'assurances des entreprises du territoire.

Ce projet ambitieux revêt aussi une dimension d'intérêt général, car il est essentiel que le modèle défini et mis en place puisse être dupliqué sur d'autres territoires au niveau national comme à l'international. Il devra notamment pouvoir s'adapter aux différents contextes, en se déclinant aux besoins des ports plus petits où les moyens d'action font face à des contraintes fortes de moyens. Il s'inscrira aussi dans la politique nationale et européenne en matière de cybersécurité maritime en étroite collaboration avec le Secrétariat Général de la Mer (SGMer) où l'interopérabilité de la plateforme de cybersécurité portuaire, maritime et industrielle avec le futur M-CERT (Maritime - Computer Emergency Response Team) national est un enjeu clé du dispositif.

En résumé, HAROPA Port du Havre au travers d'une inédite démarche d'innovation s'engage sur un processus de progrès pour renforcer sa politique en matière de cybersécurité portuaire, maritime et industrielle, faisant de cette discipline un vecteur essentiel du développement de l'activité du port et de sa résilience. Cette initiative permettra aussi à l'État d'affermir sa souveraineté nationale en intégrant le « Port Cyber sécurisé » dans son dispositif global de cybersécurité maritime, contribuant ainsi à sécuriser le commerce international sur le moyen et long terme.

Parution le 22 mai 2020

La cybersécurité post-covid rimera-t-elle vraiment avec souveraineté ?

RAPHAEL MARICHEZ
Expert cybersécurité
Services du Premier ministre

Le milieu de la cybersécurité s'inquiète à juste titre des conséquences de la crise du coronavirus sur la soutenabilité des budgets de sécurité. Mais au-delà des quantités, c'est la mutation du métier même de la cybersécurité qui se trouve brutalement accélérée.

Pour redynamiser son activité, l'entreprise devra démontrer la robustesse de son outil de production et la fiabilité de ses produits et services : la cybersécurité fait partie de l'équation.

Le retour allégué de la souveraineté permettrait-il de répondre positivement aux enjeux de cybersécurité de l'entreprise ?

La mutation de la cybersécurité dans la transformation numérique

Depuis plusieurs années, les DSI ont déjà largement entamé un virage structurant vers une **externalisation accrue** des activités de haute technicité et aux coûts d'investissements élevés (hébergements, clouds…). Selon les contenus des fiches de postes de RSSI ou CISO correspondantes, il serait attendu des responsables cybersécurité qu'ils délaissent leur expertise technique en architectures et conceptions de sécurité, au profit de connaissances sur la configuration des services des principaux fournisseurs de services cloud (CSP, Cloud Service Providers).

Le RSSI d'une entreprise recourant au cloud computing deviendrait garant de **la conformité des configurations des services de cloud à une politique**

adossée aux référentiels du CSP. C'est à mon avis une voie de garage avec peu de valeur métier.

La cybersécurité de l'entreprise ne créera demain de la valeur ni en se concentrant sur l'informatique traditionnelle détenue en propre par les DSI que les métiers délaissent, ni en étant l'opérateur humain des interfaces de gestion des CSP.

Le potentiel du responsable cybersécurité réside dans son aptitude à piloter les risques en appui des métiers et en exploitant des outils facilitateurs évitant la répétition de tâches à faible valeur.

Vers le directeur de la cybersécurité, plus proche des métiers, du risque opérationnel, et de la gestion de crise[1].

L'entreprise moderne crée sa richesse par l'utilisation du numérique. Celles qui montrent les plus fortes croissances sont les entreprises construites autour d'un socle numérique, « digital-native » (Doctolib, Blablacar, Uber, AirBnb…). A l'extrême, la création de valeur part d'un produit numérique simple auquel on ajoute, par itérations, des fonctionnalités. Même dans le monde de l'industrie traditionnelle comme l'automobile, l'innovation par le numérique permet la création de valeur et la capacité à se distinguer sur un marché mondialisé.

Dans les entreprises qui innovent et réussissent, **les métiers deviennent leur propre direction du numérique**. En sous-traitant massivement par commodité et pour éviter des investissements humains et financiers déraisonnables, ils entraînent **la fragmentation de leur outil numérique de production** (hébergement, réseau, devops, supervision, exploitation applicative, y compris la sécurité opérationnelle…), parfois sans avoir conscience de la cascade de sous-traitance derrière le prestataire qui joue le rôle d'intégrateur de solutions.

La **concentration des acteurs numériques** est particulièrement prononcée dans le « bas » de la chaîne de valeur qui constitue le socle de l'outil de production : outils de communication, stockage, calcul en ligne, sécurité opérationnelle de ces services. Et, ce qui n'est pas anecdotique, l' « **effet**

réseau » incite à opter pour la même solution que son partenaire, client ou fournisseur, pour des raisons de coopération et de facilité de prise en main.

Le coronavirus aura été le game changer de la transformation numérique

En quelques jours 8 millions de travailleurs français ont été placés en télétravail, souvent dans l'urgence. Les métiers ont adopté comme jamais une utilisation décomplexée de l'informatique vue comme un consommable facilement accessible : réseaux, stockage, serveurs, sécurité opérationnelle.

Les plans de continuité d'activité pré-établis ont pu amortir le choc de sidération des premiers jours sur les moyens préexistants des DSI et pour une partie réduite de l'activité et un nombre limité de salariés. Le redémarrage au maximum du possible de l'activité nominale via le numérique a fait voler en éclat les principes de précautions managériaux, sécuritaires voire budgétaires. Les souscriptions aux services de cloud computing ont explosé.

À court terme, la crise sanitaire aura favorisé l'utilisation massive d'outils numériques parmi un faible nombre d'acteurs, rarement français ou européens, ainsi que la fragmentation des outils numériques de production auprès d'une cascade de sous-traitants.

Perte des frontières ?

Le principe de colocalisation du lieu de travail avec le lieu de production, qui survivait encore par inertie ou habitude, a été totalement balayé, bien sûr à l'exception des activités industrielles traditionnelles nécessitant une présence humaine.

L'industrie traditionnelle adhère par essence aux territoires dans lesquels elle produit et verse des salaires. Ce n'est pas le cas pour l'industrie des services et encore moins pour le numérique. La « dé-territorialisation » du travailleur, qui promet d'être durable, appelle à la poursuite de la transition vers le cloud, la fragmentation de la chaîne de production, et l'abandon du critère géographique dans la localisation des ressources numériques.

Le responsable cybersécurité doit englober, dans sa gestion de risque, l'activité extra-périmétrique, portée par le salarié hors sol, et portée par les outils de production hors sol. Deux facettes d'une même tendance, et qui emportent chacune des évolutions de risques différentes que le responsable cybersécurité doit intégrer - ou accepter d'être relégué aux archives.

Perte de souveraineté ?

Alors que revient le discours de la souveraineté sous l'angle de l'autonomie de production, l'absence de maîtrise de maillons nécessaires à l'outil de production doit évidemment interpeller. L'argument simpliste de la nationalité ou de l'autonomie de toute la capacité de production mérite une contre analyse.

Le risque de disruption de l'activité de l'entreprise trouve sa source dans l'intégration, au sein de la chaîne de production, d'acteurs non facilement substituables et placés dans un rapport de force largement asymétrique et défavorable au client : ce dernier n'est pas en mesure d'imposer ses propres conditions. En matière numérique et davantage encore en cybersécurité, nous sommes très loin de l'objectif !

Pour autant, la souveraineté de l'entreprise n'est pas un vain concept. Elle est la condition de l'exercice de son libre arbitre dans le cadre du marché, et notamment la liberté de choisir ses fournisseurs selon leurs caractéristiques. Or, l'informatique devient un consommable (réseau, stockage, opérations), au même titre que l'énergie (électricité, fuel…). Le moyen de parvenir à la liberté de choisir repose ainsi sur trois nécessités :

- connaître les caractéristiques du service auquel on souscrit (auditabilité, standards) ;
- évaluer en quoi ces caractéristiques répondent aux besoins métiers (expertise, lien avec le métier) ;
- pouvoir changer de fournisseur en cas de besoin (réversibilité, diversité des fournisseurs).

Les responsables cybersécurité, dans la chaîne de création de valeur, doivent accompagner le mouvement naturel des métiers vers les solutions externalisées et notamment basées sur le *cloud computing*. Il s'agit notamment

d'intervenir sur les services de stockage, les réseaux orchestrés par logiciel, les environnements d'intégration et de déploiement continus, et les outils de sécurité opérationnelle.

Analyser sérieusement la sécurité des outils

Il ne s'agit plus de durcir un système d'information aux frontières définies (RSSI : « responsable de la sécurité des *systèmes d'information* »). Il s'agit de garantir une activité de production durablement optimisée face aux multiples *risques numériques* (sécurité numérique), ou face aux risques informationnels (*chief information security officer*). Les solutions pour y parvenir ne seront pas uniformes. Elles dépendent : des cas d'usages (une moto va plus loin qu'un tank) ; des expertises et ressources humaines disponibles (le chiffrement sans bonne gestion des secrets et des terminaux présente un intérêt réel mais limité) ; enfin de ce qu'offre le marché (réinventer la roue donne rarement un meilleur produit que l'original).

Sur l'exemple classique de la visioconférence parmi d'autres, les nombreux outils disponibles se distinguent par facilité et type d'usage (conférences, réunions, ateliers, entretiens), passage à l'échelle, disponibilité, confidentialité des flux et/ou des données d'annuaire, intégration avec d'autres outils collaboratifs, fonctionnement embarqué dans les navigateurs, facilité d'installation, fonctionnalités ou protections supplémentaires accessibles selon le type de licence acquise... Les choix de Zoom, Webex, Teams, Tixeo, Jitsi, et consort, peuvent tous se justifier selon le cas, le contexte d'usage et les options souscrites.

L'analyse factuelle des risques introduits par l'utilisation d'outils tiers sur l'information et l'activité de l'entreprise entre pleinement dans le mandat du responsable cybersécurité. Malheureusement, la reprise virale de messages simplistes et sensationnalistes est plus rapide et invite à sensibiliser les dirigeants. Ces messages relayés de proche en proche mélangent des faiblesses d'implémentation réelles mais corrigeables, des utilisations dangereuses (sciemment ou non) de la part d'utilisateurs non habitués, ou des facilités d'usage intrinsèques et assumées du service fourni.

Il convient ainsi de faire le tri et d'apporter aux utilisateurs les informations

simples et nécessaires sur les conditions d'utilisation des outils.

« Ce qui est simple est toujours faux. Ce qui ne l'est pas est inutilisable. » (Valéry)

On attend bien du responsable cybersécurité qu'il se livre à une analyse fouillée, vérifiée, au-delà des synthèses globalisées et recopiées sans analyse, des **caractéristiques précises des différents outils** du marché au regard des besoins de l'entreprise qui ne sont pas les besoins d'une autre. Il s'appuiera sur des consultants, sur des études comparatives étayées et sourcées (par exemple NSA[2], Orange Cyberdéfense[3], ou experts indépendants), sur des organismes reconnus (MITRE), sur la documentation technique voire le code source.

Pour que la sécurité soit rendue simple pour l'utilisateur, le responsable cybersécurité ne peut pas faire l'économie d'un questionnement propre à l'entreprise, et d'une réflexion amont solide dans une matière complexe mêlant technique et stratégie. Sécurité, patriotisme, maîtrise du tiers, continuité d'activité, constituent différents critères de choix tous vertueux mais qui ne sont pas alignés. Il n'existe pas de recommandation d'un outil idéal dans l'absolu, car chaque usage est différent : tant mieux pour la concurrence, l'innovation et pour la résilience de l'activité.

Sécuriser le volet numérique de l'activité

La fragmentation des composantes numériques de la chaîne de production rend celle-ci vulnérable à des disruptions soudaines affectant certains maillons, disruptions dont la fréquence d'apparition devrait augmenter[4]. Or il n'est pas objectivement évident que la relocalisation nationale[5] amène, à fonctionnalités similaires, une meilleure sécurité de fonctionnement, une économie et/ou une meilleure efficacité. Parce qu'il existe des dispositifs de sécurité et de contrôles, la France s'accommode très bien de ne produire aucun disque dur ni aucun disque SSD sur son territoire, alors que ces supports indispensables de nos données embarquent de l'électronique et du logiciel de haute technologie[6].

Plutôt que de miser sur des fournisseurs monopolistiques, l'entreprise

pourrait s'inspirer du concept de **résilience productive**[7], afin de reconquérir la maîtrise de sa chaîne de production comprise comme un écosystème :

- Distribution, redondance : Recours à des plateformes, ou des hub, qui permettent de distribuer la charge de travail sur plusieurs fournisseurs tout en maintenant un standard d'interopérabilité entre les éléments amonts et aval de la chaîne de production
- Agilité, diversité : aptitude à intégrer et s'interfacer rapidement avec des technologies et des fournisseurs divers pour réduire les risques spécifiques à certains fournisseurs, pays ou technologies.
- synergies locales : tirer localement profit d'opportunités de mutualisation, de partage, de partenariats, de regroupements de compétences, de services ou d'infrastructures.

La responsabilité sociétale des entreprises mondialisées.

La souveraineté à l'échelle nationale dans le domaine de la cybersécurité passe par le maintien de capacités de création de valeur dans nos territoires, entraînant emploi, versement des salaires et pouvoir d'achat.

Or l'outil de production numérique, pour l'entreprise comme pour les CSP, est déconnecté du territoire géographique. La création de valeur en cybersécurité se fera au sein des métiers intellectuels non remplaçables par des algorithmes. Dans un nouveau cadre de travail à distance, s'ouvrent des perspectives enthousiasmantes de dynamisation de territoires éloignés des grandes métropoles, mais aussi des perspectives de concurrence acerbe entre territoires y compris à l'étranger. La concentration accrue de fonctions productives essentielles au sein d'acteurs numériques multinationaux présente alors un danger pour la stabilité de nos sociétés-nations, avec le risque de délocalisation totale de la création de valeur.

Une évolution des politiques de responsabilité sociétale et environnementale (RSE) des entreprises pourrait prendre en considération la dynamisation de nos territoires dans les choix de recrutements mais aussi... de sous-traitance !

Ainsi, la souveraineté dans le contexte cybersécurité reposerait sur deux objectif distincts : d'une part, une volonté de sécuriser l'outil de production ; d'autre part, le maintien ou la création dans nos territoires de capacités

productives intellectuelles. Bien loin d'une vision simpliste d'un souverainisme isolationniste, ces deux objectifs n'ignorent pas la mondialisation et la concentration du marché de la cybersécurité.

Recommandations

La cybersécurité des entreprises devrait progressivement intégrer ou intensifier les activités suivantes :

- **se rapprocher des métiers** dans leurs objectifs de création de valeur et de continuité d'activité, notamment en accompagnant les transitions vers le *cloud computing* et le DevOps de manière sécurisée et pérenne ;

- rattraper le **backlog** de la crise, réviser la **gestion du risque** et sécuriser **le « nouveau normal »**, notamment en (re)construisant si nécessaire les principes et architectures permettant la sécurisation des services de *cloud computing* et du travail à distance pérenne.

- maîtriser les risques numériques de **défaillances des chaînes de production** en recourant à **la diversification** des solutions, à **l'agilité** face aux événements imprévus, et à **l'automatisation** des tâches à faible valeur ;

- organiser l'analyse des risques numériques par **activités métier** et par **flux de services consommés**, plutôt que par systèmes d'information physiques et périmétriques ;

- **questionner, auditer et analyser en profondeur les caractéristiques** des outils et services numériques du marché, en particulier ceux fournissant le socle de l'outil de production, en vue d'assurer la **cohérence de la gestion des risques de l'entreprise** ;

- intégrer, pourquoi pas, un **objectif de responsabilité sociétale** conduisant à maintenir une activité numérique intellectuelle productive, incluant la sous-traitance, sur le territoire (région, pays, continent), sans méconnaître l'écosystème environnant.

L'entreprise peut donc aisément conjuguer sa propre souveraineté et sa cybersécurité, cette dernière éclairant la direction sur les choix stratégiques contribuant à la robustesse de l'appareil productif. Sans méconnaître la réalité du marché mondialisé des services numériques, la cybersécurité pourra trouver un terrain de coopération favorable avec la souveraineté comme enjeu de politique publique par le vecteur de la responsabilité sociétale et environnementale de l'entreprise, prolongeant ainsi dans le domaine de l'entreprise le volontarisme naturel des administrations publiques.

Parution le 29 mai 2020

[1] CESIN « directeur cybersécurité » Le Directeur Cybersécurité décrypté - CESIN
[2] https://www.nextgov.com/cybersecurity/2020/04/zoom-or-not-nsa-offers-agencies-guidance-choosing-videoconference-tools/164953/
[3] https://orangecyberdefense.com/global/blog/covid-19/video-killed-the-conferencing-star/
[4] https://theconversation.com/apprivoiser-les-cygnes-noirs-enseignements-de-la-crise-du-coronavirus-135481
[5] sabelle Méjean "La relocalisation est une fausse bonne idée" dans Le Monde publié le 24 mai.
[6] Relire Softwar (1984, Thierry Breton et Denis Beneich)
[7] https://www.utopies.com/publications/covid-19-une-question-de-resilience-productive/

D'une pandémie l'autre…

CHRISTIAN DAVIOT
Ancien conseiller stratégie
du directeur général de l'ANSSI

L'on objectera que comparaison n'est pas raison, qu'il est encore trop tôt pour tirer des enseignements de la période que nous traversons. Il reste que l'expérience vécue lors du traitement par la France de la pandémie Covid-19 permet d'envisager l'impact de l'inévitable pandémie virale numérique qui nous touchera avant cinq ans. Et de s'y préparer.

Oser un tel parallèle est d'autant plus opportun que cette pandémie a accéléré la transition numérique de notre pays. Plus de numérique, c'est plus d'opportunité pour tous, y compris pour les acteurs malveillants, États ou criminels. Le développement à venir des usages permis par la 5G et la perspective de « territoires intelligents » augmentent d'autant la surface d'attaque de nos sociétés.

Prenons quelques-uns des éléments qui ont caractérisé les semaines écoulées.

L'origine de la pandémie

Avant que l'origine géographique et accidentelle de la pandémie fasse consensus pour les scientifiques, certains États ont tenté d'attribuer au gouvernement du pays concerné la responsabilité de la diffusion du virus. En perspective sans doute, les traces dans la mémoire collective des cinquante millions de morts causés par un virus importé d'un autre continent en Europe, mais toujours attribués cent ans après à une grippe « espagnole » ! Censure hier, propagande aujourd'hui…

Si l'origine d'une pandémie dans le monde matériel est discutée, dans

l'univers numérique, il est question d'attribution. Certains États pratiquent le « naming and shaming » : une attaque informatique réelle, souvent à des fins d'espionnage, est publiquement dénoncée et des présumés coupables désignés[1], sans qu'aucune preuve définitive ne soit apportée. Il est vrai que révéler des preuves, lorsqu'elles existent, serait dévoiler ses propres pratiques et capacités… d'espionnage ! Malgré les pressions de gouvernements étrangers et la volonté de certains ministères, la France a jusqu'ici refusé cette pratique et intelligemment choisit le dialogue bilatéral, notamment parce que l'attribution d'une attaque informatique est un choix politique plus qu'une certitude technique. Il nous faudra nous le rappeler si demain la pandémie numérique touche nos intérêts vitaux.

Les victimes de la pandémie

À ce jour, la pandémie a fait près de trente mille morts en France. Les commissions d'enquête parlementaires établiront peut-être s'il aurait pu en être autrement. Les mesures économiques prises par le gouvernement permettront d'éviter une hécatombe économique, même si la pérennité de l'activité de plusieurs dizaines de milliers d'artisans, commerçants, indépendants, petites et moyennes entreprises est remise en question.

Si des victimes humaines seront sans doute à déplorer, la pandémie numérique qui vient n'endeuillera heureusement pas autant de familles. Ses conséquences économiques seront, en revanche, potentiellement plus graves. Un virus informatique chiffrant et/ou destructeur[2] se diffusant largement et rapidement[3], pourrait stopper net l'activité de centaines de milliers d'entreprises de toutes tailles, de la multinationale au boulanger. Éventuellement sans possibilité de reprise. La France se remettrait difficilement d'une telle mise à terre.

Le système de santé

Alors qu'ils dénonçaient il a quelques mois leurs conditions de travail, le management par la restriction budgétaire et l'état de l'hôpital public, les hommes et les femmes du « personnel soignant » ont été capables par leurs compétences et dévouement de faire face aux effets de la pandémie, parfois au péril de leur vie, en inventant des solutions leur permettant de compenser toutes sortes de pénuries.

La France n'est pas (encore) prête à faire face à une pandémie numérique, pas plus qu'une autre nation. Le choix effectué il y a dix ans d'un modèle interministériel de cybersécurité plutôt que d'en confier la mise en place à la Défense ou aux services de renseignement a cependant permis de nous doter, au travers de l'ANSSI[4], de capacités de traitement opérationnel des attaques informatiques parmi les meilleures au monde. Mais bien que les gouvernements successifs aient donné les moyens budgétaires et humains nécessaires à son développement, et malgré leurs compétences et dévouement, ralentis par un accompagnement administratif plus que perfectible, les 650 agents de l'ANSSI ne pourraient faire face seuls à une pandémie numérique touchant des milliers d'acteurs répartis sur le territoire national. La stratégie nationale pour la sécurité du numérique portée par le Premier ministre en 2015 a d'ailleurs pris en compte cet enjeu en décidant de la création d'un organisme[5] dédié à la sensibilisation des particuliers, entreprises et collectivités territoriales et au traitement des attaques informatiques dont ils sont victimes par une mise en relation avec des prestataires privés de proximité. Cette plateforme, cybermalveillance.gouv.fr, est un succès à la fois technique et pédagogique qui a montré toute sa pertinence pendant la crise du Covid-19 et mériterait d'ailleurs d'être davantage soutenue aujourd'hui par l'État, les collectivités et les entreprises.

Pendant la pandémie Covid-19, et même si elles sont légitimes, les réquisitions par des préfets de masques de protection initialement commandés par des présidents de Région pour la protection de leurs administrés ont manifesté qu'en cas de crise des intérêts concurrents pouvaient exister entre l'État et les Régions. Il en irait de même en cas de pandémie numérique. L'ANSSI serait concentrée sur les opérateurs d'importance vitale, les administrations et les orientations que lui fixera le gouvernement. Ainsi, il appartient aux Régions de se préparer à la future pandémie numérique. Certaines Régions ont déjà pris conscience des enjeux liés à la sécurité du numérique, mais leurs ressources et compétences numériques sont souvent saturées par l'obligation de répondre à des contraintes réglementaires déjà lourdes et à la bureaucratie sous-jacente.

L'appui sur des experts

En complément de l'organisation administrative existante, la création d'un conseil scientifique a permis depuis le début de la pandémie d'éclairer une décision politique qui a su prendre en compte d'autres sources d'information et expertises de terrain, au moins partiellement.

L'expertise française en matière de cybersécurité est d'excellent niveau. Des universitaires ont notamment mis en place une approche interdisciplinaire de ce sujet et l'envisagent sous les angles national, européen et international. Pourtant, en raison d'une conception propriétaire, datée et exiguë de la sécurité du numérique, l'administration répugne généralement à consulter ces universitaires dont certains ont pourtant acquis une renommée internationale. Cette faiblesse retarde l'organisation de notre résilience à la future pandémie numérique.

Le rôle des acteurs privés

L'engagement des entreprises dans la lutte contre la pandémie est également un fait marquant. À côté des initiatives prises par de nombreuses PME, associations ou particuliers, de grandes entreprises comme LVMH se sont mobilisées, non seulement en exploitant leurs capacités industrielles pour fournir du gel hydroalcoolique par exemple, mais également en mobilisant leur réseau international pour trouver et fournir les équipements manquants.

On assiste à la même mobilisation de grandes entreprises en faveur de la sécurité du numérique dans une sorte d'inversion des rôles. Tandis que les États s'affrontent - malgré les conventions signées - dans ce qu'ils considèrent comme un nouveau domaine de combat, au risque d'entraîner des dysfonctionnements graves de nos sociétés et de provoquer la pandémie numérique qui les affaiblirait, des acteurs privés s'engagent en faveur de la paix et de la sécurité dans le numérique. Il en va ainsi du Tech accord de Microsoft ou de la Charter of trust de Siemens. En France, l'adhésion de nombreuses entreprises de l'écosystème au projet de Campus Cyber souhaité par le Président de la République relève du même engagement.

De même qu'un éventuel vaccin ne viendra que d'un effort conjoint entre

États et entreprises, la sécurité du numérique ne se fera pas sans un engagement et une écoute des acteurs privés sans qui le numérique n'existerait pas.

Confinement et déconfinement

Visant à garantir la « distanciation sociale » - cette expression a valeur d'aveu - le confinement a, au contraire, souvent rapproché les personnes et suscité innovations et solidarités de proximité. Le traitement d'une pandémie numérique se fera dans la proximité et devra bénéficier, comme le déconfinement, de l'appui des Régions.

Des chantiers majeurs à lancer

L'analogie entre pandémie Covid-19 et pandémie numérique serait à poursuivre au travers des gestes barrières, du rôle des ministères des Armées et de l'Intérieur, de la place du Conseil de défense, etc.

Des scientifiques avaient anticipé la pandémie qui nous touche. Les administrations « compétentes » ont proposé au politique des décisions qui priorisaient d'autres critères que ceux à prendre en compte en matière de santé publique.

La période qui s'ouvre va être propice à une réflexion large - pas seulement économique - sur ce que nous voulons pour la France, l'Europe et les relations internationales dans les dix ans qui viennent. Au-delà des discours généraux qui émergent sur la souveraineté, périodiquement avancée par le politique, périodiquement enterrée par les administrations, il nous appartiendra de décliner à la sécurité du numérique certaines avancées présentées comme des solutions aux pandémies comme celle (super tabou dans l'administration) de « souveraineté européenne » ou de « bien public mondial ».

Portées à propos du numérique par le Président de la République, notamment dans ses discours annuels aux ambassadeurs, ces notions mériteraient l'attention et le travail des administrations, le soutien des universitaires et l'association des entreprises et des ONG. Associées à un engagement multilatéral conforme à nos valeurs et pas seulement pavlovien,

à une vraie réflexion stratégique qui enterrerait la pathétique « Revue stratégique de cyberdéfense » de 2018, ces notions sont de nature à préparer la résilience qu'il nous reste à construire avec les Régions face à la pandémie numérique à venir.

Mais ces sujets feront l'objet d'autres développements.

Parution le 5 juin 2020

[1] Le lecteur identifiera aisément les quatre États généralement cités.
[2] De type Shamoon (2012) ou NotPetya (2016) par exemple.
[3] De type Conficker (2008).
[4] Agence nationale de la sécurité des systèmes d'information.
[5] Le groupement d'intérêt public ACYMA, cybermalveillance.gouv.fr

Application #STOPCOVID : quels impacts sur nos données personnelles ?

NACIRA SALVAN
Présidente
CEFCYS

Depuis l'annonce du développement de cette application, beaucoup de questions entourent sa mise en place : Comment ça marche ? Quelles informations personnelles seront utilisées ? Comment seront utilisées les données ? Y a-t-il un risque d'atteinte à la vie privée ? Qui aura accès à ces données ? Les expertes du CEFCYS vous livrent des clés d'analyse (article collectif).

La pandémie de coronavirus a déclenché une crise sanitaire mondiale sans précédent, obligeant toutes les populations à modifier leurs comportements et le gouvernement à opter pour des mesures drastiques de confinement afin de limiter la propagation du virus. Les chercheurs examinent les déplacements des personnes malades pour comprendre comment le coronavirus se propage à très grande vitesse (la chaîne de transmission). Le but est de permettre un déconfinement sans une deuxième vague tant redoutée.

Plusieurs pays, dont la Corée du Sud, Singapour, Taïwan et Israël, se sont tournés vers le digital pour assouplir le déconfinement et tracer la chaîne de transmission. À travers une application, les personnes testées positives au Covid-19 sont identifiées et les personnes qui rentrent en contact avec elles reçoivent une alerte sur leur téléphone.

Dans le même esprit, l'Union européenne a lancé le programme « Pan-European Privacy-Preserving Proximity Tracing » (PEPP-PT). L'objectif affiché est de développer une application de traçage via Bluetooth, avec enregistrement sur la base du volontariat.

Pour la France, l'application se nomme « Stop COVID » et est rentrée en effet le 2 juin avec déjà 1,5 million d'utilisateurs.

Éléments d'analyse

Ce sujet a fait l'objet de nombreuses discussions au sein de notre association, le CEFCYS (Cercle des Femmes dans la Cybersécurité), et nous étions également largement sollicitées par notre entourage. À travers cet article collégial, notre but est de fournir aux lecteurs des informations claires et vérifiées pour soutenir leur décision, et non de prendre parti pour ou contre l'application.

Nous avons fait le choix de rassembler les informations sous la forme d'un SWOT[1], qui est une présentation factuelle.

	Positif (Pour atteindre l'objectif)	**Négatif** (Pour atteindre l'objectif)
Origine Interne (Organisationnelle)	**S** **Forces** 1. Implications d'entreprises performantes 2. Implications d'institutions reconnues 3. Implémentation de la « Privacy by design » 4. Utilisation d'un traçage de proximité	**W** **Faiblesses** 1. Utilisation du protocole Bluetooth 2. Applicabilité de la RGPD (minimisation, anonymisation, limite dans le temps) 3. Publicité pour les partenaires : impact long terme ? 4. Application limitée aux portables
Origine Externe (Environnement)	**O** **Opportunités** 1. Utilisation du digital pour permettre un déconfinement sans deuxième vague 2. Complément du dispositif par un accès aux tests et aux gestes barrières (masques) 3. Inscription sur la base du volontariat 4. Communication transparente sur la solution mise en œuvre 5. Opportunité européenne sur la RGPD	**T** **Menaces** 1. Inscription sur la base du volontariat : difficulté à atteindre le pourcentage requis de participants pour être efficace 2. Volonté des personnes alertés de se faire tester et de se confiner 3. Défiance vis-à-vis du gouvernement 4. Souveraineté numérique 5. Applicabilité de la RGPD (Accès aux données, consentement, sous-traitants, information en cas de fuite) 6. Création d'applications « Pirates » 7. Limitation de l'application à la France

Forces (Strengths)

L'implication d'acteurs majeurs de la Sécurité des Systèmes d'Information (avec notamment l'Inria, ANSSI, Capgemini, Dassault Systèmes, Inserm,

Lunabee Studio, Orange, Santé Publique France et Withings) se veut rassurant car c'est l'association d'entreprises performantes et d'institutions reconnues, comme l'Inria qui coordonne le projet. La CNIL[2] a également appuyé ces travaux et est consultée à chaque étape clé du projet.

Il est annoncé que cette application sera respectueuse du RGPD en suivant le principe de « PrivacyByDesign ». « L'application utilisera des pseudonymes et ne permettra pas de remontée de listes de personnes contaminées », explique Marie-Laure Denis, la présidente de la CNIL dans son avis rendu le 24 avril 2020.
Le secrétaire d'État en charge du numérique, Cédric O, sur BFM TV rassure sur les points suivants :
• L'identité de l'utilisateur ne sera jamais dévoilée.
• La collecte, l'identification et la durée de conservation seront limitées.
• La minimisation et dé-identification de l'application sont prônées.

Dès le début, le gouvernement insiste sur le fait que cette application ne sera pas du « tracking », mais un système de « traçage de proximité » et ce « contact tracing » utilisera la technologie « bluetooth » pour être moins intrusive. L'identification sera anonymisée dès la racine de la donnée et sa détention sera éphémère. De plus, le gouvernement a fait le choix de soumettre le code de l'application à des hackers éthiques, à travers la plateforme de Bug Bounty YESWEHACK.

D'après son article sur l'application, le Journal des femmes indique qu'une fois installée sur le smartphone, l'application préviendra les personnes qui ont été en contact avec un malade testé positif au coronavirus. La personne alertée pourra alors se faire dépister et être prise en charge au plus tôt, ou se confiner afin de briser les chaînes de transmission du virus, même si elle ne développe aucun symptôme. Cette alerte suppose que la personne testée positive au Covid-19 se déclare comme telle et accepte de diffuser cette information aux utilisateurs de l'application qu'elle croiserait dans la rue, les magasins… Cette application sera combinée au répertoire des données.
Deux nouvelles solutions numériques de lutte contre le virus sont en train d'être discutées : Sidep et Contact Covid, qui accompagneront les fameuses « brigades de cas contact » aussi appelées Brigades sanitaires[3].

Faiblesses (Weaknesses)

Tous ces points évoqués sont des forces pour cette application en devenir, mais face à cela de nombreuses faiblesses sont mises en lumière.
Les freins techniques sont pointés du doigt par plusieurs experts en cyber sécurité car la technologie Bluetooth est très critiquée à cause de l'inexactitude des informations Bluetooth et leur qualité.

Au-delà des limites technologiques, il est clair que cette application suscite beaucoup d'interrogations principalement liées à la gestion des données personnelles utilisées et la mise en œuvre réelle des principes de la RGPD :

- Minimisation : est-ce que seules les données nécessaires et suffisantes seront récoltées ? Il y a déjà des exemples en Chine et Corée du Sud de traçage des trajets.
- Anonymisation : l'identité de la personne malade ne doit pas être connue ou induite par les informations disponibles.
- Limitation de conservation dans le temps : Y aura-t-il une transparence sur le cycle de vie intégrale de nos données ?
- Implémentation de toutes les mesures de sécurité informatique nécessaires à la protection de ces données sensibles.

Les entreprises qui participent aux travaux communiquent déjà en disant qu'elles font un geste à titre gracieux, mais l'impact publicitaire est colossal.
Le gouvernement parle déjà d'autres possibilités pour tracer les contacts : boîtier ou bracelet connectés, mais leur élaboration est plus longue et plus coûteuse que l'application pour smartphone.

L'audition de Guillaume Poupard[4] (Directeur de l'ANSSI) est à écouter, car il met en lumière les risques des dérives et d'espionnage, l'impossibilité d'anonymisation totale et les choix politiques d'une telle solution.

Opportunités (Opportunities)

Dans ce contexte de pandémie Covid-19, tous les moyens sont louables pour sortir de cette crise mondiale. L'objectif du développement de l'application a été clairement expliqué par le gouvernement : #STOPCOVID, une application pour smartphone permettra d'aider à limiter la propagation du

coronavirus et se fera sur la base du volontariat. Elle sera un complément aux mesures déjà en cours pour munir la population de masques et tester un maximum de personnes pour connaître la sérologie positive ou négative d'un maximum d'individus sur le territoire français.

Le Premier ministre, lors de son audition à l'Assemblée nationale, a insisté sur la nécessité de casser les chaînes de transmission, en identifiant au plus vite les personnes ayant été au contact des personnes infectées. Des brigades sanitaires, d'environ 20 000 à 30 000 personnes, seront chargées de remonter la liste de cas contacts, pour les inviter à se faire tester.

Dans l'article du 6 mai[5], le Secrétaire d'État chargé du Numérique, Cédric O, sur BFMTV le mardi 5 mai, détaillant la feuille de route, assurait que les conditions sont très encadrées et proportionnées. La solution numérique serait même fortement utile selon lui « dans les centres urbains [...], les transports en commun, les lieux publics ou les commerces », où les moyens humains ne permettront pas de reconstituer les chaînes de transmission aussi efficacement que le traitement de données.
L'inscription se fera sur la base du volontariat, il n'y a donc pas d'obligation à l'utiliser.
Les travaux d'élaboration de l'application #STOPCOVID se veulent transparents, le gouvernement communique depuis le début en expliquant qui participera activement au projet. La CNIL a donné son aval et veille au bon déroulé du dispositif en demandant une transparence intégrale au gouvernement, ce qui rassure les experts du RGPD.

Les mesures d'application de ces enquêtes seront précisées par un décret[6] en Conseil d'État, pris après avis de la CNIL, et par ordonnances. L'application de traçage de proximité STOPCOVID pourra être mise en place par ces ordonnances, mais le Premier ministre a promis un débat et un vote spécifique, quand sa mise en œuvre aura avancé.

Pour cela, l'article 6 du décret de la loi soumise, va créer une base de données pour ces enquêtes épidémiologiques. Ce fichier (dont la durée sera de 3 mois, d'après les dernières annonces) pourra contenir des données de santé et d'identification sur les personnes infectées et celles ayant été en contact avec elles, le cas échéant sans leur consentement. Il pourra également être nourri

des données de Santé publique France, de l'assurance maladie et des agences régionales de santé. Seuls les services de santé et les laboratoires autorisés à réaliser les tests pourront avoir accès aux données de ce fichier pour les enquêtes épidémiologiques.

Étant donné que les travaux continuent, les informations sont communiquées assez régulièrement et cela montre le bel élan positif ainsi que la force légale du RGPD en France et en Europe. L'opportunité d'harmoniser le RGPD à l'échelle européenne est forte, les pays de l'union ont pu travailler ensemble à travers cet exercice inédit. La tendance du RGPD en France est une valeur indéniable, c'est le « fer de lance » de la France d'après le commissaire européen Thierry Breton, chargé de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace. L'objectif est de mener à bien ce projet d'utilité publique pour sortir de la crise sanitaire.

Menaces (Threats)

Cette influence positive du RGPD est souvent éclipsée par les menaces immédiates perçues par la population française, les détracteurs ne manquent pas de souligner les nuisances d'une telle application, les mauvais exemples dans certains pays étrangers et les obstacles à son bon fonctionnement.

La première menace à la bonne efficacité de l'application est l'inscription sur la base du volontariat : le volontariat doit être de minimum 60 % de la population pour faire reculer la maladie Covid-19. De plus, les personnes ayant été malades doivent s'identifier comme telles et avoir confiance dans le système pour fournir cette information.

Ensuite, il est impératif que les personnes qui reçoivent une alerte suivent le protocole, se fassent tester et se confinent. Si ce protocole n'est pas suivi, le virus continuera de se propager.

Malgré les garanties apportées pour minimiser les risques sur la vie privée et les libertés individuelles, persiste le caractère menaçant des moyens technologiques assimilés, par une frange de la population, à des procédés de suivi de masse. L'application fait débat et les détracteurs ne manquent pas de souligner le caractère liberticide d'une telle application. Ainsi, en fonction

du degré de confiance en notre système démocratique, déjà secoué par des vents contestataires depuis plusieurs années, l'application peut être perçue comme les prémisses de dérives totalitaires.

Loin des enjeux géopolitiques visant à maintenir une souveraineté numérique face aux acteurs privés disposant de moyens technologiques équivalents - GAFAM, cette défiance vis-à-vis de l'autorité publique se fait omniprésente alors même que l'usage de ces mêmes moyens par ces firmes privées suscitent une adhésion quasi généralisée depuis plusieurs années. Les données personnelles et la vie privée pourraient donc être détenues par des firmes privées sans que cela ne soit perçu comme un risque majeur par les individus alors même qu'une application visant à juguler les risques de propagation d'un virus mortel suscite une levée de boucliers.

La réelle application de la RGPD est au cœur de nombreuses craintes :

- Nous sommes en droit de nous demander où iront nos données ? De plus, les risques de perte et de fuite ne sont pas faibles, quelles seront les conséquences, les dommages et les accès inappropriés ?
- Au-delà d'un usage et une exploitation commerciale non souhaités de ces données, nous ne sommes pas à l'abri d'une exploitation malveillante, est-ce que les mesures de protections et de sécurité sont correctement implémentées ?
- Les exigences métiers sont-elles respectées pour toute personne ayant accès à ces données ?
- La politique de contrôle n'est-elle pas ambigüe au vu du contexte de pandémie (exemple : inscription des utilisateurs parfois compromis avec une violation de l'inscription) ? Les restrictions et les mécanismes sont-ils respectueux en termes de limitation et d'accord ? Les sous-traitants pourraient éventuellement faire fuiter des DCP sensibles avec une grande pluralité des acteurs, seront-ils tous bien identifiés ?
- Quid du Fichier de collecte de données de santé : l'assurance maladie recense déjà nos données de santé et le fichier est créé par ce biais, mais qui d'autre pourra accéder à ces informations ? (politique de développement sécurisé, protection des données de test, visibilité dans un volet du Dossier Médical Partagé en ligne?)
- En cas de violation des données à caractère personnel sensibles, y aura-t-il un bon suivi : enregistrement des incidents ?

- Nous sommes en droit de nous demander s'il sera vraiment possible de retirer son consentement comme l'exige le RGPD : si on télécharge l'application, peut-on tout de même s'opposer au traitement de nos données ? Pourra-t-on se rétracter, et sous quel délai ? (Quid d'une demande légitime de Demande D'accès Aux Données Nominatives Collectées).

- Quelles sont les mesures de transmissions des Données à Caractère Personnel (fuites vers d'autres pays, attention au transfert entre juridictions) Comment pouvons-nous garantir que les données de santé d'une personne contaminée puissent transiter en toute sécurité vers un système standardisé équivalent au nôtre, au sein de la zone Europe ?

La question de la souveraineté numérique se pose également. Où seront hébergées ces données ? Pouvons-nous avoir confiance alors que tant de données sensibles seront en jeu ? Certains pays (hors UE) sont moins scrupuleux à l'utilisation des données personnelles et de grosses dérives de surveillance de masse sont craintes[7].

Les acteurs privés et les puissances étrangères n'ont pas attendu pour déployer des arsenaux technologiques qui risquent d'impacter, à terme, notre souveraineté numérique.
Pire, de nombreux Français ont déjà téléchargé une application développée par la Géorgie : de nombreuses applications « Copycat » fleurissent et n'offrent aucune garantie sur la protection des données ou la réelle efficacité de l'application. Le risque est grand pour un usager de télécharger la mauvaise application.

Pour le moment, l'application sera faite pour la France, ce qui ne répond pas au besoin de nombreux frontaliers. Chaque pays de l'UE est en train de développer et tester sa propre application et ne prend donc pas encore en considération les personnes qui dans le cadre de leur travail effectuent quotidiennement des trajets hors France.

Pistes d'amélioration

Plusieurs pistes d'amélioration sont possibles pour permettre un plein succès de l'application STOPCOVID :

1. Renforcement du Bluetooth par le protocole ROBERT. Pour être crédible au niveau européen le consortium PEPP-PT (Pan-European Privacy Preserving Proximity Tracing) a créé le protocole ROBERT[8]. L'inria en France et Frauhofer en Allemagne sont à l'origine de ce protocole pour équiper plusieurs pays du continent.
2. Certification ISO27701 de l'application pour garantir une mise en œuvre totale et transparente du RGPD au sein de l'application.
3. Mise en place d'une application unique à l'échelle européenne pour répondre au besoin des frontaliers, et montrer un succès européen dans la gestion de cette crise sanitaire.
4. Création de bracelets ou autres objets connectés pour ouvrir l'utilisation de l'application aux seniors, les plus sensibles au virus, mais les moins équipés en téléphone portable.

L'influence de l'ISO 27701 tombe à point nommé, car cette norme internationale reflète les exigences RGPD, le code de bonne pratique et le cadre de la protection de la vie privée. Ce cadre permet de mieux comprendre dans quelles mesures nos données personnelles peuvent être collectées de manière respectueuse. L'objectif est d'atténuer les risques de ce traitement massif de données en prouvant la transparence à travers des informations claires, précises, simples et concises pour le public ciblé.

Parmi les exigences de l'ISO27701, notons les points suivants :
- Protection des Données externes à caractère personnel : l'entreprise doit documenter tout stockage de Données à Caractère Personnel (supports/dispositifs/chiffrement/procédures/mesures compensatoires).
- PIMS RGPD (Système de gestion des données personnelles) : clarifient les exigences liées aux Sous-Traitants et aux Responsables de Traitement.
- La Sécurité physique et environnementale doit être assurée : zone, emplacement, protection, sorties des actifs, procédures, gestion des changements, sauvegarde des informations.

Cette application fait partie d'un ensemble de mesures qui permettra de reprendre l'activité économique rapidement et en toute sécurité. L'application n'est qu'un maillon de la chaine de protection. L'humain et sa santé sont des priorités qu'il faut pérenniser et protéger.

Le sujet de l'application STOPCOVID est particulièrement épineux dans la mesure où il pose le débat de la proportionnalité des moyens nécessaires à la maitrise de risques de surmortalité liés à la pandémie actuelle. Qui dit situation exceptionnelle, dit moyens exceptionnels.

Les démocraties sont-elles prêtes à accueillir, sans renier leurs principes fondamentaux, les nouvelles vagues technologiques qui fournissent des moyens de plus en plus puissants pour collecter et traiter les données des populations ? C'est tout l'enjeu politique autour de l'application STOPCOVID.

Parution le 12 juin 2020

[1] https://fr.wikipedia.org/wiki/SWOT_(m%C3%A9thode_d%27analyse)
[2] https://linc.cnil.fr/fr/coronoptiques-34-des-modeles-epidemiologiques-au-contact-tracing-rendre-visible-la-contagion
https://www.cnil.fr/fr/deconfinement-lavis-de-la-cnil-sur-le-projet-de-decret-encadrant-les-systemes-dinformation-mis-en
[3] https://www.dataz.fr/
[4] http://videos.senat.fr/video.1608918_5ebaa04d6b8cd.audition-de-m-guillaume-poupard-directeur-general-de-l-agence-nationale-de-la-securite-des-systeme
[5] https://www.linternaute.com/
[6] Dalloz actualité, 29 avr. 2020, art. P. Januel
[7] https://www.lemonde.fr/idees/article/2020/05/14/l-europe-doit-tracer-le-covid-19-sans-les-gafam_6039656_3232.html
https://www.zdnet.fr/blogs/50-nuances-d-internet/la-vie-privee-ou-la-sante-telle-n-est-pas-la-question-39903763.htm
DCP : Données à Caractère Personnel
[8] https://siecledigital.fr/
PROTOCOLE ROBERT pour Robust and privacy-presERving proximity Tracing protocol

Vous avez dit souveraineté ?

ALAIN BOUILLE
Expert Cybersécurité

Les propos de cet article reflètent l'opinion de son auteur et n'ont aucunement vocation à représenter la position de quel qu'organisme ou quel que groupe de travail que ce soit dans lesquels l'auteur est par ailleurs impliqué.

Le sujet de la souveraineté en matière de numérique devient une sorte de marronnier qui s'apparente à une mauvaise série où à la fin de chaque épisode, on a l'impression que c'est toujours le même qui gagne ou plutôt le même qui perd à savoir notre souveraineté numérique !

Les batailles perdues du 20ème siècle

L'histoire hoquète depuis 40 ans où toutes les batailles (mais au fait s'est-on vraiment battus ?) ont été perdues ou presque. Ce fut d'abord le cas du hardware remporté de main de maître par les Américains qui font depuis longtemps travailler les Chinois pour la fabrication de leurs matériels. Puis, ce fut le software également gagné par les Américains avec cependant quelques poches de résistance dont SAP reste sans doute la plus notable en Europe. Entre temps, il n'est pas besoin de s'appesantir sur l'épisode Minitel / Internet, l'histoire a mille fois été contée.

L'émergence des GAFAM et… des premiers Clouds Souverains

À l'avènement du Cloud Computing au début des années 2000, l'Europe est restée coi et s'est laissée submerger par ceux qui n'étaient pas encore les géants de la Californie et que l'on n'appelait pas encore les GAFAM ! Sans

doute piquée par l'hégémonie de ces derniers qui se répandaient comme une traînée de poudre dans les entreprises françaises et dans le reste du monde, la France sort de sa torpeur 12 ans plus tard, autrement dit un siècle à la vitesse du numérique et lance avec panache le cloud souverain à la française sous l'impulsion du Président Sarkozy ! Comme on ne pouvait pas faire simple, deux sociétés voient le jour, Cloudwatt et Numergy avec un investissement initial de 150 millions d'euros qu'il a fallu partager en deux soit 75 millions d'euros chacune. Ce montant peut sembler trop élevé quand on connait la fin de l'histoire, mais représente une infime goutte d'eau comparée aux milliards de dollars investis de l'autre côté de l'Atlantique par les géants californiens parfois en pure perte. Mais en France on ne supporte pas l'échec et les détracteurs de la souveraineté se délectent dès qu'ils le peuvent de ces « débâcles » pour justifier qu'il vaut mieux aller en Californie chercher les solutions à nos besoins numériques.

La Data et le RGPD

Du coup, lorsque les datas ont commencé à jaillir dans les années 2010 tel l'or noir au 19ème siècle, on s'est dit que là peut-être quelqu'un allait se réveiller pour faire en sorte que nos gisements de données ne traversent pas l'Atlantique par les pipelines de l'Internet. C'est alors qu'on a sorti l'arme absolue, à savoir le RGPD qui devait mettre au pas, entre autres, les grands acteurs du cloud qui commençaient à malmener les données privées des usagers en toute impunité. Les GAFAM n'ont pas tremblé longtemps, car ce fut eux paradoxalement qui ont affiché d'insolentes conformités au RGPD avant tout le monde tandis que les entreprises françaises ramaient pour être « compliant » à la date fatidique du 25 mai 2018.

Certes le RGPD représente une avancée indéniable en matière de protection des données à caractère personnel, mais n'aide aucunement les RSSI à protéger les données critiques de l'entreprise qui ne sont justement pas « à caractère personnel » ! Ce règlement a aussi contribué à ce que les GAFAM construisent des data centers en France pour éviter des flux de données trop problématiques vers les USA ou l'Irlande ou encore les Pays-Bas, mais on s'est bien gardé d'imposer dans le règlement une quelconque étanchéité de ces données pourtant stockées en France, aux lois extraterritoriales américaines (Patriot Act, Cloud Act…). On rencontre encore pourtant

quelques naïfs ou pire des incompétents qui ne voient pas le problème et qui s'imaginent que parce que les données sont en France, tout baigne !

Les ravages des solutions collaboratives pour la protection du patrimoine informationnel

Là où la situation a commencé à devenir ingérable pour les données des entreprises, c'est lorsqu'on a commencé à s'équiper d'outils dits collaboratifs et que l'on a externalisé les messageries des entreprises et tant qu'on y était les répertoires bureautiques avec, trop contents de se débarrasser de ces boulets qui encombraient les datacenters des entreprises avec un niveau de service de plus en plus décrié. Que celui qui ne s'est pas retrouvé un beau matin obligé de « nettoyer » sa boîte aux lettres pour envoyer le message archiurgent à son chef, mais qui ne pouvait partir parce que la boîte aux lettres était pleine lève le doigt ! Alors évidemment quand on annonce une boîte aux lettres de taille quasi illimitée à ces utilisateurs, ils demandent tout de suite la date de la migration !

Lorsqu'on externalise dans le Cloud un service, une base de données, une application métier, bref des données connues et maîtrisées, les RSSI sont suffisamment outillés pour effectuer une analyse de risques appropriée, pointer les données critiques et mettre en œuvre les outils de protection adaptés… et il y en a pléthore ! Seulement lorsqu'il s'agit de migrer son environnement bureautique, effectuer cette analyse relève d'une mission impossible, car on ne sait jamais in fine ce que contiennent les milliers de boîtes aux lettres d'une entreprise et les milliards de fichiers bureautiques stockés parfois depuis des décennies ! Lorsqu'on est suffisamment kamikaze (j'en connais au moins un !) pour se lancer dans une analyse de ces contenus, on y découvre un énorme foutoir où on y croise un peu de tout : des données RH en pagaille, des notes stratégiques, des plans à 5 ans, des rapports d'audit, des prévisions d'investissement… avec des données certes correctement protégées dans les applications qui les gèrent, mais mises au clair dès qu'elles se retrouvent stockées dans des espaces bureautiques et en pièce jointe de mails.

Alors que deviennent toutes ces données ? Eh bien la plupart du temps, elles sont ni plus ni moins « bennées » dans les Clouds telles quelles, et la plupart

du temps sans protection particulière ! Bon débarras et en plus il n'y a que des vieux trucs ! Ben voyons.

La supercherie des solutions hybrides et des systèmes de protection

Hybridation : au début de ces projets collaboratifs, les entreprises se sont lancées dans des analyses de risques plus ou moins sérieuses, plus ou moins complaisantes selon la pression exercée par le porteur du projet (en général le DSI) sur celui chargé de cette analyse (en général le RSSI aux ordres du DSI, cherchez l'erreur !). Il y a même des cas où il n'y a pas eu d'analyse de risques du tout. En général, la grande trouvaille pour les données sensibles a été de considérer que seuls les VIP en manipulaient, donc il suffisait de garder un mini service de messagerie « on premises » pour ces utilisateurs sensibles et le reste pouvait être externalisé en toute quiétude. Comme si les VIP n'écrivaient jamais à l'étage d'en dessous et n'échangeaient jamais des pièces jointes sensibles avec leurs collaborateurs et comme si les données les plus sensibles n'étaient pas manipulées par des salariés en bas de l'organigramme ? Mais cette option rassurait les COMEX, on leur épargnait une décision douloureuse en les chouchoutant ainsi ! Ces solutions dites hybrides ont très vite fait long feu du fait de la porosité des deux mondes et surtout du coût qu'elles généraient.

Protection : d'aucuns ont pu se lancer dans des solutions de chiffrement pour protéger leurs données sensibles. Trois écueils à cette option :

- D'abord comme on ne peut pas tout chiffrer, on demande à l'utilisateur de faire le tri en classifiant ses fichiers et ses mails. Mais comment peut-on être certains que l'utilisateur joue le jeu s'il sait qu'une classification élevée est synonyme de dégradation de la fameuse « expérience utilisateur » ?
- Ensuite on a le choix d'utiliser la solution de chiffrement proposée par l'hébergeur qui est parfaitement intégrée à l'ergonomie de la solution… mais qui ne sert à rien, en tous cas pas à se protéger de l'hébergeur, puisque ce dernier garde la clé de chiffrement.
- Vient enfin l'option d'utiliser ses propres clés, mais à ce moment-là le service n'a en effet plus accès aux données et l'expérience utilisateur est dégradée, car ses mails ne sont plus indexés et il est obligé de les classer à la main comme au bon vieux temps !

La dernière possibilité reste l'aiguillage des mails sensibles vers une solution dite de confiance, mais toujours avec l'écueil que cet aiguillage reste à la main de l'utilisateur en fonction de la classification. De telles solutions sont actuellement en développement chez certains offreurs de confiance… à suivre.

La non-réversibilité des solutions, l'enfermement des clients et le verrouillage de la concurrence

Au début de ce nirvana du Cloud, les ROI étaient flamboyants. Bien sûr on pouvait se débarasser de toutes ces machines, de ces coûteux data centers et des informaticiens qui allaient avec ! Enfin pas tous, car il a fallu très vite s'occuper de ces solutions Cloud dont la complexité est la marque de fabrique sans parler des contrats où des armées de juristes doivent être recrutées pour les comprendre et les suivre.

Mais il a fallu très vite déchanter. On a vu des premiers renouvellements de contrat s'accompagner d'une « petite » rallonge de 35 % avec une totale impossibilité de revenir en arrière. On n'avait déjà pas assez de serveurs pour héberger des boîtes aux lettres de taille limitée, alors des boîtes aux lettres de taille illimitées 3 ans après les premières migrations, il faudrait en racheter des serveurs ! Allez à la concurrence ? Chez Monsieur Google ? Alors oui l'irréversibilité (l'enfermement devrait-on dire) est un problème, car cela veut dire qu'aujourd'hui les clients sont pieds et poings liés avec ces fournisseurs et qu'ils ne se gênent plus pour augmenter les tarifs de manière indécente. Il y a belle lurette que les gros clients n'osent plus parler de ROI pour justifier leur basculement dans le Cloud. Il reste bien sûr l'immense richesse de ces offres qui, il faut bien le reconnaître, n'ont pas d'égal à date.

On l'a vu avec la crise COVID, dépendre d'un seul pays, en l'occurrence la Chine, pour la fourniture de tonnes de choses très utiles en cette période de crise était une très mauvaise idée et que rééquilibrer (un peu !) nos capacités de production nationale serait sans doute une bonne idée. Faudra-t-il une crise similaire, les morts en moins il faut l'espérer, pour que la France et l'Europe réalisent que de dépendre que d'une seule nation étrangère pour la fourniture de 80 % de ses services informatiques devenus essentiels pour la bonne marche de l'économie, n'est pas non plus une bonne idée ?

Optimisation ou… fraude fiscale ?

Chacun sait que les GAFAM ne payent pas les impôts qu'ils devraient payer en Europe, la faute à une fiscalité avantageuse organisée par… l'Europe elle-même. Comment alors jouer à égalité quand les offreurs de Cloud français ne font pas signer leurs contrats en droit irlandais à leur client ? Ce sujet est un problème complexe qui semble insoluble, mais qui du coup aggrave la situation qui, si on n'y remédie pas, sera toujours au détriment du cloud souverain.

Les parlementaires s'intéressent au sujet

D'excellents rapports ont été produits par les parlementaires sur le sujet de la souveraineté les années passées. Les deux derniers en date « Le devoir de souveraineté numérique » du Sénat sous l'égide de Gérard Longuet et celui de l'Assemblée nationale sous l'égide du député Raphaël Gauvain « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » abordent ces questions et donnent des pistes intéressantes en matière de légifération. Le rapport Gauvain en particulier établit la liste de ce qu'il faut faire spécifiquement dans ce domaine… on ne pourra pas dire, je ne savais pas ! Alors qu'attend-on ?

La fausse bonne idée des données sensibles

Quand on parle de Cloud Souverain, automatiquement l'auditoire associe cette notion aux seules informations sensibles. Je ne sais pas d'où vient cette fâcheuse habitude que de ne s'intéresser qu'aux données sensibles quand on parle de Cloud Souverain mais à l'ère du Big Data et de la Data Science, où l'on sait désormais faire « parler » les données qui, individuellement, ne présentent aucun intérêt, mais agglomérées dans des data lakes, représentent souvent une grande richesse à exploiter, il serait temps de reconsidérer cette restriction. Les offreurs de Cloud Souverain seraient donc condamnés à ne ramasser que les miettes laissés par les GAFAM ou du moins les données que les entreprises même les plus aventureuses n'ont pas encore osé externaliser ? Le Cloud Souverain doit aussi s'ouvrir aux données hautement valorisables.

Les bras d'honneur à la souveraineté

Il y a certes des circonstances atténuantes pour les entreprises qui n'ont pas le choix quand il s'agit d'externaliser leur service de messagerie. Car seules deux offres sérieuses sont disponibles sur le marché : Microsoft, leader en la matière, et Google. Et on ne peut tout de même pas leur en vouloir de proposer des solutions performantes !

En revanche, quand des solutions souveraines sont disponibles et concurrentes des GAFAM pour l'hébergement des données de santé par exemple, pourquoi diantre laisser fabriquer un process d'agrément qui ne barre pas la route aux entreprises assujetties à des lois extraterritoriales ? La dernière décision en date où le gouvernement français a pris la décision d'héberger les informations de santé de millions de Français (Cf. projet Health Data Hub) sur les serveurs de Microsoft, au détriment d'OVH, une société française, s'apparente à un bras d'honneur à tous les travaux en cours pour tenter de sauver ce qui peut encore l'être en matière de souveraineté.

GAIA-X une solution souveraine ?

Cette décision malheureuse pour la souveraineté concernant le Health Data Hub tombe au pire moment. Celui où l'Allemagne et la France annoncent la création de GAIA-X, censé offrir une alternative aux solutions de Google, Amazon et Microsoft. On peut résumer que GAIA-X est une sorte de catalogue de services numériques portés par des fournisseurs qui se seront préalablement engagés sur des standards supposés renforcer la confiance de leurs clients en matière de sécurité des données, mais aussi de transparence des contrats et enfin d'interopérabilités des technologies d'un hébergeur à l'autre. Mais on apprend que GAIA-X ne sera pas fermé aux GAFAM qui pourront proposer leurs services à condition de respecter le cahier des charges. Je ne suis pas spécialiste juridique, mais cette hypothétique adhésion à GAIA-X ne les rendra pas hermétiques aux lois extraterritoriales de leur pays d'origine, dans ce cas pourquoi mettre GAIA-X au crédit des offres souveraines ?

En conclusion, personne ne peut le nier, les résultats ne sont pas à la hauteur des attentes. Le sujet pourrait sembler éculé, car les projets de souveraineté

numérique sont évoqués depuis plusieurs décennies, et pourtant la situation de dépendance ne fait qu'empirer. Et si nous nous y prenions mal ?

J'insisterai cependant sur quelques mesures :

- Légiférer sur la protection des données sensibles des entreprises qui ne sont pas soumises au RGPD et qui devraient n'être éligibles qu'à des clouds de confiance.
- S'intéresser aux données hautement valorisables qui devraient aussi être candidates au cloud de confiance.
- Soutenir la filière pas seulement par des investissements massifs, mais par des commandes à commencer par l'État qui n'a pas donné l'exemple ces derniers mois.
- Changer le mode de pensée qui implique que l'herbe est plus verte de l'autre côté de l'Atlantique. Les solutions françaises et européennes sont là et ne demandent qu'à se développer.
- Trouver les moyens sans protectionnisme exacerbé pour donner une préférence française/européenne comme le font les américains chez eux pour leurs propres fournisseurs, un « Patriot » (au sens premier du mot) Act européen en quelque sorte .
- Mettre les solutions européennes et non-européennes sur un pied d'égalité fiscale.

Parution le 18 juin 2020

Sensibiliser à la sécurité numérique au plus près des acteurs sur les territoires : un enjeu majeur

JEROME NOTIN
Directeur général
Cybermalveillance.gouv.fr

Le dispositif Cybermalveillance.gouv.fr a été partenaire du Tour de France de la Cybersécurité pour la 2ème année en 2019.

Chaque étape du TDFCyber a été une occasion de présenter aux participants en plénière le dispositif et ses missions de sensibilisation aux risques numériques, d'assistance aux victimes d'actes de cybermalveillance, et d'observation de la menace cyber, ainsi que la plateforme et les typologies de victimes et de modes opératoires de cyberattaques traités sur Cybermalveillance.gouv.fr.

Lors de plusieurs étapes du Tour de France de la Cybersécurité, un atelier a été organisé pour aider les participants à comprendre les étapes méthodologiques d'une démarche de sensibilisation interne, en entreprise ou dans une collectivité. Cet atelier a été construit comme une mise en situation concrète des participants et a été l'objet de réflexions et retours très constructifs et encourageants.

Globalement, la participation de Cybermalveillance.gouv.fr au TDFCyber est l'occasion pour le dispositif d'aller à la rencontre de ses publics sur les territoires, de faire connaître ses missions et les contenus de sensibilisation, mais aussi d'apprendre, de la part des participants du TDFCyber, de nombreuses remontées de terrain et enseignements sur les pratiques de sensibilisation et d'assistance.

La richesse des interventions et des publics, ainsi que la qualité des conditions d'accueil et des intervenants, fait du TDFCyber un événement auquel le

dispositif Cybermalveillance.gouv.fr est fier de contribuer.

Article atelier de sensibilisation

Lors du Tour de France de la Cybersécurité 2019, le dispositif Cybermalveillance.gouv.fr a organisé sur plusieurs étapes un atelier de sensibilisation appelé « Construire une démarche interne de sensibilisation aux enjeux de cybersécurité, un enjeu majeur pour les entreprises et les collectivités ».

Cet atelier a été imaginé pour répondre à un besoin de méthodologie et de réflexion sur la manière dont on peut élaborer des stratégies de sensibilisation, et pas uniquement utiliser des contenus de sensibilisation déjà préparés.

Pour Cybermalveillance.gouv.fr, cet atelier a été également une manière de recueillir, auprès des participants, leurs retours d'expériences permettant de nourrir les contenus et stratégies de sensibilisation et de recommandations de bonnes pratiques du dispositif.

L'atelier a été proposé pour 12 à 15 participants maximum à chaque fois.

Ceux-ci ont été partagés en deux groupes qui ont reçu chacun une situation concrète à mettre en place :
- un groupe recevant la simulation d'une stratégie de sensibilisation pour les agents d'une collectivité territoriale de 5 000 habitants ;
- l'autre groupe recevant la simulation d'une stratégie de sensibilisation pour une PME de 35 salariés travaillant comme sous-traitante dans le secteur automobile.

Ces deux scénarii font alors l'objet d'une réflexion, par petits groupes, cadrée par une trame écrite qui permet aux participants de balayer petit à petit les différentes phases de construction d'une méthode de sensibilisation.

Au bout de 45 minutes environ, les deux groupes se réunissent et vont présenter chacun le fruit de leur réflexion. L'animateur-trice de l'atelier va alors enrichir cette restitution, si besoin, avec des bonnes pratiques déjà éprouvées, mais aussi noter et recueillir des pratiques qui seraient intéressantes à faire remonter.

Les participants sont tout d'abord invités à une première phase d'identification et d'analyse des informations et données qui sont à protéger dans l'entité : cela permet, avant d'entamer la démarche de sensibilisation proprement dite, de prendre conscience de l'application concrète et du périmètre qu'elle va devoir prendre. Il faut identifier les informations sensibles, qui y a accès, et comment.

Ensuite, les participants vont relever quelles sont les menaces qui peuvent viser l'entité qu'ils ont mission de protéger, quelles sont les mesures de sécurité déjà existantes, et faire un état des lieux de la maturité et de la formation des personnels.

À partir de là, ils vont pouvoir donner des objectifs précis à leur démarche de sensibilisation : définir les sujets à traiter, établir un calendrier, prioriser les actions et les publics.

Enfin, ils commencent une réflexion sur la mise en œuvre concrète, à court et moyen terme, de la démarche de sensibilisation aux risques cyber adaptée à leur entité.

Cette démarche partant de la situation de l'organisation est l'occasion de faire un état des lieux et une première réflexion d'analyse des risques en prenant en compte la réalité de la vie d'une entreprise ou d'une collectivité. Les participants à l'atelier doivent se mettre dans la peau du responsable de cette mission de sensibilisation (DSI ou autre) et aller chercher dans l'ensemble des activités et des personnels de l'entité le périmètre et les ressources qui vont ensuite être au cœur de l'activité de sensibilisation.

En mettant l'accent sur les besoins et la démarche à long terme de sensibilisation, cet atelier permet aux participants de s'identifier et donc de pouvoir réfléchir aux propres démarches mises en œuvre dans leur organisation d'origine. Cela permet également, par la suite, de choisir ou de créer des contenus de sensibilisation qui vont être particulièrement adaptés à la démarche choisie, plutôt que de construire une démarche a posteriori en fonction des ressources disponibles.

Les retours des participants, et l'enthousiasme qu'ils ont mis durant les

différents ateliers, montrent que cet exercice est utile et intéressant à mettre en œuvre. Après une phase de démarrage qui prend quelques minutes d'explication, le temps que chacun comprenne bien le cadre de réflexion et ce qui est attendu, les groupes se prennent au jeu et vont permettre une mise en commun d'avis et de retours d'expériences qui alimentent la construction de la démarche de sensibilisation.

La restriction de l'atelier à deux petits groupes de 5 à 6 personnes, si possible en situation de management dans leur entité (publique ou privée), permet un réel échange d'idées et d'informations, en laissant à chacun la place de s'exprimer.

L'animateur-trice de l'atelier doit avoir à cœur de ne pas laisser un groupe s'enliser dans une réflexion stérile ou un monopole de parole par un intervenant, afin de s'assurer que chaque groupe ait pu avancer au maximum pendant le temps imparti.

La phase de restitution finale est très importante et il faut y consacrer un temps significatif, d'abord pour que chaque groupe puisse restituer sa réflexion, mais aussi pour permettre l'échange entre chaque groupe (pourquoi tel choix, qu'est-ce qu'il y a derrière comme réflexion), et l'enrichissement par l'animateur-trice avec des idées, des pratiques, des suggestions qui n'auraient pas été identifiées par les groupes. Lors des ateliers organisés avec le Tour de France de la Cybersécurité en 2019, cette phase de restitution durait entre 30 et 45 minutes.

L'intérêt de ce type d'atelier de sensibilisation réside non pas dans la somme de connaissances qui va être apportée de façon descendante vers les participants, mais bien dans la discussion collective qui a lieu et qui invite chaque participant à la réflexion. Cette réflexion est ancrée dans des situations réelles et guidée par une fiche de progression qui permet aux groupes d'avancer concrètement de l'analyse d'une situation initiale aux solutions pratiques.

À l'heure où les contenus et solutions clés en main de sensibilisation foisonnent, cette démarche de réflexion collective et d'adaptation à son environnement de terrain est proposée pour aider les personnes en situation

de responsabilité à exercer leur faculté de choix et de décision avec une méthodologie progressive.

Il serait bien entendu intéressant de pratiquer en situation réelle, et sur un temps plus complet, cette démarche auprès d'une entité publique ou privée de taille moyenne comme il est question dans cet atelier, afin de pouvoir faire un retour d'expérience plus complet et précis sur ce type de méthodologie.

Parution le 26 juin 2020

Identités numériques

DR MICHEL DUBOIS
Chef du Pôle Expertise
Direction de la cybersécurité, Groupe La Poste

Du latin « identitas » signifiant « le même », l'identité présente de multiples définitions en fonction du domaine d'étude. Ainsi, le psychologue allemand Erik Erikson, dans son ouvrage « Enfance et société », définit l'identité comme « le sentiment subjectif et tonique d'une unité personnelle et d'une continuité temporelle ». Pour la philosophe Anne-Marie Drouin-Hans, l'identité sépare le soi du non-soi. Le sociologue Erving Goffman explique, dans son ouvrage « Stigmate », que l'identité d'un individu s'élabore par le jeu de l'interaction et résulte de l'opposition entre une identité définie par autrui et une identité pour soi. Dans le domaine juridique, l'identité correspond à « la personnalité civile d'un individu, légalement reconnue ou constatée, établie par différents éléments d'état civil et par son signalement ».

Comme nous pouvons le voir, définir la notion d'identité, est un problème difficile, dépendant du domaine d'étude et évolutif dans le temps.

Malgré tout, il nous faut définir la notion d'identité dans le domaine du numérique.

Dans son rapport « Identités numériques - Clés de voûte de la citoyenneté numérique », le Conseil national du numérique définit l'identité numérique sous deux angles :

- l'identité numérique peut faire référence à l'identifiant d'accès à un service, choisi pour ou par le détenteur. Dans ce cas, l'identité numérique peut être déclarative ou imposée par le service, en rapport avec l'état civil ou non. Il existe alors une multiplicité d'identités numériques propres aux pratiques numériques de chaque individu ;

- l'identité numérique peut aussi être perçue comme le reflet des comportements en ligne des individus, c'est-à-dire l'ensemble des traces qu'un individu peut laisser en surfant sur Internet, et qui permettront de définir une cartographie de ces comportements et de faire entrer celui-ci dans une typologie.

Le deuxième angle est celui utilisé dans le marketing. Il permet de catégoriser un internaute en fonction de son comportement sur les sites Web qu'il visite. Nous allons nous focaliser sur le premier angle de définition de l'identité numérique : celui basé sur un identifiant que nous appelons couramment login, adresse email ou pseudo en fonction du contexte.

La problématique de l'identité numérique réside dans la conception d'Internet. En effet, Internet a été construit sans qu'il soit possible de savoir à qui et à quoi on se connecte. Comme cette capacité essentielle fait défaut, des solutions de rechange ont dû être trouvées afin d'identifier qui accède à quoi. La conséquence directe de cet état de fait est qu'Internet, en l'absence d'une couche d'identité native, est basé sur un patchwork d'identités ponctuelles et multiples.

C'est ainsi que l'internaute moderne s'est habitué à saisir ses identifiants sans avoir la certitude de l'authenticité des sites Web qu'il visite, ou si des informations privées sont divulguées à des parties illégitimes à son insu. Les cybercriminels ont bien compris cette situation et ont développé des attaques spécifiques comme le phishing, le spear phishing, la fraude 4-1-9, l'arnaque au président, le pharming et le credential stuffing. Cette dernière attaque étant directement liée à la multiplicité des identités numériques ce qui entraîne une réutilisation des éléments d'authentification.

Avec le temps, des protocoles spécifiques ont été élaborés comme « Transport Layer Security » (TLS). TLS est un protocole de sécurisation des échanges sur un réseau informatique et donc sur Internet. Ce standard permet d'authentifier le serveur et l'utilisateur ainsi que de garantir l'intégrité et la confidentialité des échanges. Concrètement, TLS est le « S » de HTTPS dans les adresses des sites Web. Sur le plan technique, des réponses ont été apportées, cependant elles ne sont pas universellement déployées. En outre, elles ne concernent que le monde des réseaux informatiques et ne résolvent

pas le problème des identités multiples.

Il est donc primordial de disposer d'une plateforme permettant d'agréger les différentes identités numériques d'un individu.

Pour être adoptée massivement par les utilisateurs, une telle plateforme devrait répondre à un certain nombre de principes :

- Contrôle et consentement de l'utilisateur. L'utilisateur doit pouvoir faire confiance à la plateforme de gestion de son identité. Pour gagner cette confiance, la plateforme doit être conçue de manière à ce que l'utilisateur puisse contrôler les identités numériques utilisées et les informations divulguées. La plateforme doit également protéger l'utilisateur contre la fraude, en vérifiant l'identité de toute partie qui demande des informations. Enfin, la plateforme doit permettre à l'utilisateur de connaître les raisons pour lesquelles les informations sont recueillies ;
- Collecte restreinte du nombre d'identifiants. La plateforme doit être conçue en tenant compte du risque de compromission de son annuaire interne. À ce titre, elle ne doit collecter que le minimum d'éléments d'identification pour chaque individu ;
- Ségrégation des identités. La plateforme garantit la ségrégation des identifiants destinés aux entités publiques, administratives, professionnelles ou privées. L'utilisateur doit pouvoir faire en sorte que l'identité numérique utilisée à titre privé ne soit pas connue de son employeur ou de l'administration ;
- Centralisation sur l'humain. Dans un processus d'identification on distingue le consommateur, qui offre un service, et les contextes de données d'identification. En fonction du consommateur, l'individu doit pouvoir choisir quel contexte de données d'identification utiliser. Ainsi, l'utilisateur pourra s'identifier sur un service médical avec des éléments identifiants différents de ceux utilisés pour un service assurantiel ;
- Compatibilité multi protocole. La plateforme doit permettre l'interfaçage avec les différentes technologies et normes de gestion des identités et d'authentification ;
- Expérience utilisateur. La plateforme doit garantir à ses utilisateurs une expérience simple et cohérente tout en permettant la séparation des contextes. Indépendamment du contexte, les procédures d'identification et d'authentification doivent être identiques et simples à utiliser.

Il existe de multiples plateformes d'agrégation d'identité permettant, au travers d'une identité pivot, d'accéder à des services divers et variés. Cependant, ces plateformes sont opérées par les grands noms d'Internet : Google, Apple, Facebook, Amazon et Microsoft. De ce fait, elles ne répondent pas aux critères précédemment énoncés.

En 2014, la France s'est dotée d'un dispositif répondant aux principes que nous avons détaillés.

Mise en œuvre par la Direction interministérielle du numérique, la plateforme FranceConnect est la solution proposée par l'État pour sécuriser et simplifier la connexion à plus de 700 services en ligne.

Reposant sur le protocole OpenID connect, son objectif est de mettre en relation des fournisseurs d'identité et des fournisseurs de service. Ainsi, lorsqu'un utilisateur souhaite effectuer une démarche en ligne, il lui suffit de cliquer sur le bouton « FranceConnect » et de choisir un compte sur l'un des fournisseurs d'identité référencés. La plateforme FranceConnect le redirige alors sur la page d'authentification. Une fois les opérations d'identification et d'authentification réalisées, l'utilisateur peut accéder au service désiré.

La plateforme FranceConnect est cependant limitée au seul usage de la relation entre un citoyen et l'administration. Il manque donc un équivalent de FranceConnect regroupant l'ensemble des besoins de support de l'identité du citoyen : vis-à-vis de l'administration, mais aussi, dans le cadre de sa vie privée et professionnelle.

L'idéal serait que notre pays dispose d'une plateforme sur laquelle chaque citoyen puisse gérer, en fonction du contexte, une identité pivot regroupant ses différentes identités numériques. En attendant ce jour, il reste d'autres difficultés, liées à l'identité numérique, à prendre en compte comme, par exemple, la suppression des mots de passe.

Parution le 3 juillet 2020

Impact des recherches en cybersécurité sur la stratégie nationale en matière de souveraineté numérique

LAURENT OLMEDO
Directeur du programme Sécurité globale
Direction des applications militaires, CEA
et
BRUNO CHARRAT
Responsable du programme cybersécurité
Direction de la recherche technologique, CEA

Renforcer notre souveraineté numérique au plan national revêt un double enjeu, à savoir conserver notre liberté d'appréciation, de décision et d'action en cas de cyberattaque et préserver nos domaines de souveraineté traditionnels au regard des cybermenaces. Ceci passe par la disponibilité d'une filière industrielle nationale, voire européenne, forte et compétitive dans le domaine des produits et services de cybersécurité ainsi que d'une recherche d'excellence afin de préparer à l'avance les futurs outils de cybersécurité.

La crise sanitaire que notre pays traverse a pour conséquence indirecte de montrer l'importance des technologies digitales pour apporter une forme de résilience au plan de la continuité d'activité. Elle souligne également combien les vulnérabilités en matière de cybersécurité pouvaient surajouter du risque à la menace sanitaire. Ce premier retour d'expérience démontre qu'il est urgent de concrétiser les ambitions de la France en cybersécurité avec la mise en place d'une réelle capacité prenant en compte nos enjeux de souveraineté.

De nombreuses initiatives nationales

Le Président de la République a lancé depuis près d'un an la démarche du pacte productif qui vise à dynamiser l'économie française. L'un des volets

de cette initiative consiste à identifier les marchés clés prioritaires qui sont à soutenir et accélérer, afin d'en exploiter tout le potentiel économique. La cybersécurité a été identifiée comme l'un de ces secteurs clés, notamment afin de contribuer à garantir notre souveraineté numérique.

En complément, un rapport intitulé « Faire de la France une économie de rupture technologique[1] » a été remis par un collège d'experts aux ministres de l'Économie et de L'Enseignement supérieur, de la Recherche et de l'Innovation mi-février. Ce document retient également la cybersécurité comme l'un des 10 marchés clés (cf. p.54 du rapport), ce qui signifie en pratique que la cybersécurité sera identifiée comme l'une des priorités claires du futur Programme d'investissements d'avenir (PIA 4).

Ce rapport demande pour ces secteurs clés une concentration des moyens de l'État, une meilleure coordination des initiatives de l'Administration, une intervention des pouvoirs publics sous forme notamment de « stratégies d'accélération » visant à soutenir les technologies diffusantes.

De façon plus large, l'État a déjà lancé plusieurs initiatives structurantes depuis 2018. Elles visent à accélérer autant que possible les stratégies en cours, définies en concertation avec les industriels, en particulier :

- La structuration d'une politique industrielle en matière numérique reposant sur la maîtrise de « technologies clés » qui est l'une des recommandations de la revue stratégique de cyberdéfense conduite par le SGDSN en février 2018, pour assurer la souveraineté numérique de la France ;
- L'action du Ministère des Armées, avec la publication en juillet 2019 du document d'orientation de l'innovation de défense (DOID) par l'Agence d'innovation de défense (AID) dans lequel l'objectif des travaux de recherche en cybersécurité répond au « double enjeu de défense des infrastructures critiques souveraines de l'État et de préservation de l'efficacité opérationnelle de nos forces » ;
- Le Comité stratégique de filière (CSF) « Industries de sécurité », dont le contrat a été signé le 29 janvier 2020, et son projet structurant « Cybersécurité et sécurité de l'IoT » ;

- La mission de préfiguration d'un campus cyber confiée à Michel Van Den Berghe, dont le rapport a été rendu public le 29 janvier 2020, et qui rentre dans sa phase d'opérationnalisation avec un objectif d'ouverture du campus au premier semestre 2021 ;
- Le lancement d'un Grand défi Automatisation de la cybersécurité dans le cadre du Conseil de l'Innovation.

Ce contexte général rend encore plus impérieux la nécessité de maintenir l'excellence de la recherche Française, à même de s'impliquer dans cette dynamique nationale et de répondre au besoin constant de disposer de nouveaux outils et technologies.

En effet, le domaine de la sécurité numérique est à la fois en forte croissance et face à un potentiel de crise majeure résultant de la professionnalisation et de la sophistication des attaques. Les **solutions technologiques matérielles et logicielles existantes ne suffisent parfois plus** à endiguer le flot des **fuites de données et des prises de contrôle de systèmes**, allant du bénin (pages personnelles) au **souverain** (infrastructures d'importance vitale, identité). Contrer ces menaces requiert de sécuriser l'ensemble des systèmes d'information qui supportent la souveraineté nationale et permettent la sécurité du citoyen. L'enjeu est de taille, et le succès d'une telle démarche permettra de créer les conditions pour une **confiance des citoyens dans le numérique, grâce à des filières industrielles et de services**.

Face à ce défi, les acteurs nationaux de la recherche sont rassemblés au sein de l'alliance des sciences et technologies du numérique Allistene qui regroupe en tant que membres fondateurs la CDEFI, le CEA, le CNRS, la CPU, Inria et l'Institut Mines-Télécom.

Le CEA, un acteur singulier de la recherche en cybersécurité

De par ses activités dans le nucléaire, le Commissariat à l'Énergie atomique et aux énergies alternatives (CEA) est fortement concerné par ce sujet de la cybersécurité. D'une part, le CEA a des **problématiques propres de cybersécurité opérationnelle**, l'obligeant à exploiter ses systèmes

d'information (SI) et opérer ses systèmes industriels (ICS), en cohérence avec le référentiel réglementaire édicté par l'ANSSI en ce qui concerne les activités civiles du CEA et par le Ministère des Armées pour les activités de défense.

Le CEA doit ainsi organiser **la protection au quotidien de 30 000 postes de travail, plus de 500 services ouverts sur internet avec 3 accès à très haut débit**. Cette cyberprotection du CEA sur l'ensemble de ses activités dans un périmètre étendu avec des systèmes d'information très diversifiés et une menace constante a nécessité de se doter **d'une très grande expertise opérationnelle**, afin de protéger des activités critiques telles que les infrastructures nucléaires, de calcul intensif, ou les activités en science du vivant.

D'autre part le CEA s'est doté d'une capacité de recherche technologique pour répondre à ses besoins propres et à ceux de ses partenaires en focalisant son action sur les deux grands axes d'activités suivants :

- **Recherche et développement de nouvelles technologies pour la sécurisation des systèmes** et leur transfert à des acteurs industriels. Selon les cas, le terme système peut recouvrir un circuit intégré, un système électronique – logiciels – réseaux – services connectés dans le cyberspace tels que des véhicules, équipements industriels, dispositifs médicaux…) ;

- **Recherche et développement de nouvelles méthodes de caractérisation et d'outils d'évaluation** de systèmes commerciaux ou en cours de développement par les industriels, afin d'en détecter les vulnérabilités.

Le CEA mène ses programmes d'innovation et de transfert technologique avec pour objectif d'accompagner le développement de la filière industrielle et de donner les moyens techniques aux services de l'État et à l'industrie d'assurer leur cyberprotection. Pour cela, **le CEA travaille en étroite collaboration avec ses partenaires de l'Alliance Allistene** avec pour objectif de créer des technologies et des **outils innovants**, et de fournir des preuves de concept concrètes, opérationnelles permettant aux industriels d'expérimenter et évaluer les briques technologiques. Ces

activités d'intégration mobilisent donc de nombreuses compétences transverses (microélectronique, numérique), essentielles à la réalisation de ces démonstrateurs :

- **Une expertise reconnue internationalement :** sur certains sujets (par exemple la recherche de vulnérabilités), le CEA conduit des recherches au meilleur niveau national et international. En témoignent les travaux fondateurs conduits depuis 2015 avec **l'ANSSI**, sur l'utilisation de l'intelligence artificielle (IA) en attaque de composants électroniques ou encore la mise en open source d'outils logiciels de référence comme Frama-C (qualification de la sécurité des logiciels) ou Miasm (reverse engineering de codes malveillants) ;

- **La montée en maturité technique grâce à des plateformes technologiques :** maillon indispensable des recherches en cybersécurité le CEA a investi dans des plateformes qui permettent d'aller jusqu'à une démarche de prototypage. Certaines de ces plateformes constituent des moyens uniques au plan national.

Avec sa singularité, le CEA est reconnu par ses partenaires académiques, industriels et institutionnels comme un acteur de confiance de la filière cybersécurité française et européenne. Ainsi, dès 1999, le CEA a mis en place à la demande des pouvoirs publics, **un Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI)**, afin de répondre aux besoins des industriels français. Ce CESTI, agréé par l'ANSSI, fait ainsi partie du **schéma Français de certification des composants sécurisés et de micrologiciels.** Le CEA est également fortement sollicité par ses partenaires pour assurer la coordination globale d'actions collaboratives nationales et Européennes. C'est en particulier le cas du projet européen **SPARTA** qui est l'un des quatre pilotes retenus pour créer un « Réseau de compétences en cybersécurité » financé par la Commission Européenne. Son objectif est de ré-imaginer la manière dont la recherche, l'innovation et la formation se pratiquent et se coordonnent au sein de l'Union européenne afin de participer au renforcement de l'autonomie stratégique européenne par la mutualisation des expertises. Ses travaux alimenteront également les réflexions préalables à l'établissement d'un centre de compétences européen en cybersécurité.

Enfin, le CEA s'est doté d'un programme spécifique de recherche en **Sécurité globale** qui a permis de créer une interaction forte avec les pouvoirs publics (DGA, ANSSI, Ministères des Armées et de l'Intérieur) en apportant une expertise scientifique et technique et en positionnant les projets de recherche dans une dimension régalienne. Cette capacité a également démontré son utilité dans la crise liée au CoVID-19.

Quelles actions à engager pour renforcer la souveraineté numérique de la France ?

Le propos liminaire du DOID[2] dresse ce constat : « Innover est plus que jamais une nécessité opérationnelle et stratégique, c'est même un enjeu de souveraineté nationale ». Toutefois, cette démarche se doit d'être faite dans un cadre structurant et fédérateur des initiatives afin d'en tirer le meilleur bénéfice au plan national.

Pour réussir, il est indispensable, comme le dit l'ANSSI dans son manifeste 2020, de structurer « l'écosystème de cybersécurité ». À ce titre, l'initiative du Campus cyber Parisien devrait devenir une pierre angulaire au plan national dans sa capacité à rassembler des acteurs, en vue de la création de « communs en cybersécurité » et à faire émerger d'autres campus sur le territoire national, fonctionnant en réseau, afin de tirer parti au mieux des expertises disponibles localement.

Cette démarche bénéficiera d'un contexte où la cybersécurité est l'archétype des recherches dites « duales », tant du point de vue de l'irrigation conjointe et respective des deux domaines civil et défense, que de celui des forts enjeux de criticité (parfois différents) qui y sont associés pour chacun d'entre eux.

À ce titre, l'initiative du Ministère des Armées avec la création récente du Cyberdéfense factory au sein du pôle Rennais est un bon exemple de création d'outils innovants indispensables permettant de renforcer les interactions entre les différents acteurs.

L'autre enjeu sera de renforcer la coordination des actions de recherche et

innovation afin d'éviter tout risque de travail en silo et d'éparpillement des moyens. Le développement de nouveaux outils de cybersécurité est en effet intrinsèquement interdisciplinaire (hardware, software, mathématiques, sciences sociales…) et il est indispensable de pouvoir faire travailler ensemble des experts d'horizons divers, sur des plateformes technologiques à l'état de l'art et en étroite interaction avec les acteurs industriels et étatiques, afin de garantir la performance, la pertinence et la légalité des outils. Des initiatives comme le Grenoble Alpes Cybersecurity Institute, fondé en 2018 et rassemblant des experts de 16 laboratoires pour conduire des travaux interdisciplinaires sont des exemples à suivre et répliquer.

Il ne peut en effet y avoir de projets de recherche structurants sans connexion avec une analyse fine de la menace actuelle et de sa projection dans un futur court et moyen terme. Il ne peut y avoir également de projets de recherche à visée stratégique sans une analyse fine des enjeux liés aux grandes évolutions en cours ou à venir, comme en témoigne le domaine de la cryptographie post-quantique.

Dans cette perspective, on peut souligner le travail effectué par le SGDSN dans sa revue stratégique en matière d'identification de technologies critiques destinées à assurer notre souveraineté numérique.

Il reste désormais à construire la feuille de route nationale en matière de projets de recherche, dans une dimension interdisciplinaire qui tire le meilleur des technologies numériques pour développer de nouveaux composants de confiance ou encore de nouveaux outils d'analyse de la sécurité en soutien des analystes.

Tout le succès des programmes de recherche qui vont se mettre en place reposera en définitive sur une démarche « coordonnée » : connaissance partagée des enjeux, des réalités de chaque acteur, ainsi que sur la construction de feuilles de route conjointes. Les initiatives lancées au plan national ne trouveront pleinement leur sens que dans cette logique et pourront alors renforcer la souveraineté numérique de la France et sa place dans un espace européen et international fortement compétitif.

Au plan européen, beaucoup reste encore à faire pour que se concrétisent les objectifs que se donne également la nouvelle Commission européenne au plan de la souveraineté numérique. L'importance de cette dimension européenne a conduit le CSF « Industries de sécurité » à l'inscrire dans sa feuille de route.

Tout semble réuni pour que notre pays tire pleinement parti des capacités existantes pour renforcer sa souveraineté numérique. Le CEA a de son côté l'intention d'apporter sa contribution à cet effort national, notamment en participant au Campus cyber, et en poursuivant son engagement européen dans la coordination de réseaux d'acteurs à l'instar de ce qui a déjà été engagé avec SPARTA et son implication dans ECSO.

Parution le 10 juillet 2020

[1] https://cache.media.enseignementsup-recherche.gouv.fr/file/Mediatheque/41/1/Rapport_college_experts_06_02-2_1242411.pdf
[2] Document d'Orientation de l'Innovation de Défense. Lien : https://www.defense.gouv.fr/aid/actualites/le-document-d-orientation-de-l-innovation-de-defense-doid

La ResNumerique : de la sécurité des systèmes d'information vers un numérique de confiance, il est temps d'agir.

STEPHANE MEYNET
Président
CERTitude NUMERIQUE

Bien définir la « chose »

Sécurité numérique, cybersécurité, sécurité des systèmes d'information… autant de termes que nous mélangeons tous allégrement pour désigner au final ce qui tendrait à rendre l'usage de nos moyens numériques le plus robuste possible. Aïe ! Encore des termes ambigus - moyens numériques et robustes - qui sans définition partagée laissent libre cours à l'imagination et l'interprétation, source de complications et d'échecs.

Pour traiter correctement et sérieusement d'un sujet, il faut d'abord bien le définir et s'assurer que l'on parle tous de la même chose. C'est ce que l'on m'a toujours appris. Et que je n'ai pas toujours mis en application : pourquoi définir ce qui est évident ? Erreur, car le diable se cache souvent dans les détails.

Derrière ce préambule quelque peu provocateur, l'idée est de simplement souligner que cette difficulté de langage, de définition, non résolue à ce jour, cache une réalité très concrète : le champ d'action que confère chacune des appellations citées ci-dessus varie. C'est pourquoi il est important de définir clairement « la chose », l'objet sur lequel nous devons concentrer nos efforts pour construire une politique efficace adaptée aux enjeux d'aujourd'hui en termes de confiance numérique.

Un périmètre qui évolue et se transforme

Si l'on parle de sécurité des systèmes d'information (SSI), l'objet important

au final est l'information et donc sa sécurité, quel que soit son support. Ce support, historiquement le papier, devient aujourd'hui majoritairement numérique, à tel point d'ailleurs que l'État s'est fortement engagé dans la dématérialisation pour de nombreux services.

Donc, logiquement, la sécurité des systèmes d'information se transforme en sécurité des systèmes numériques qui, au-delà d'être bientôt le principal support à l'information, recouvre également d'autres systèmes : les systèmes de production de nos usines, les systèmes pilotant nos infrastructures vitales, nos infrastructures sur les territoires… jusqu'à nos équipements médicaux « implantés » chez les patients.

Mais cette transformation vers le numérique met à l'écart une partie du champ d'action historique de la sécurité des systèmes d'information : la sécurité des supports d'information autres que numériques. Et si l'on parle de sécurité de l'information, qui a priori englobe la sécurité des systèmes d'information, le champ s'élargit encore pour traiter d'un tout autre sujet ô combien important et régulièrement mis à « l'honneur » ces derniers temps : celui de la désinformation, des fakenews et de l'influence.

Cette longue introduction montre combien une réflexion de fond sur la clarification et la gouvernance de ces sujets devient aujourd'hui nécessaire.

Laissons de côté le sujet de la sécurité de l'information dans son sens noble et large[1] pour revenir à la sécurité des systèmes numériques voire la sécurité (du) numérique.

Confiance et sécurité numériques : la « ResNumerique »

Tout d'abord, ne perdons pas de vue que la sécurité numérique n'est pas une fin en soi et qu'elle est inutile si elle ne sert pas une « chose » plus large. Petite provocation encore, car nous savons tous que la sécurité numérique est indispensable. Faut-il le rappeler, elle contribue à renforcer la confiance dans nos systèmes numériques essentiels à notre quotidien, à nos métiers, à notre développement, à notre protection… et à notre souveraineté.

En France, la question de la sécurité numérique est traitée au travers d'une organisation spécifique intégrant notamment l'Agence Nationale de la Sécurité des Systèmes d'Information et les ministères disposant chacun d'une chaîne fonctionnelle et opérationnelle dédiée. Elle a fait l'objet d'une réglementation abondante, dont la désormais très célèbre et première du genre Loi de Programmation Militaire 2014-2019 et son article 22 à destination d'une catégorie spécifique d'organisations, à savoir les Opérateurs d'Importance Vitale. Une réglementation qui depuis 2014 n'a cessé de s'enrichir, sous l'impulsion notamment de l'Union Européenne qui s'est saisie pleinement de ce champ depuis la Stratégie de Cybersécurité européenne de 2012.

La France dispose également d'un écosystème fort en matière de sécurité numérique comprenant des acteurs de renommée internationale et de nombreuses start-up, ce qui mérite d'être souligné, car insuffisamment mis en valeur par le passé.

Mais qu'en est-il du « simple » numérique indispensable à nos entreprises, nos territoires, nos collectivités et notre souveraineté ? L'écosystème de ce simple numérique, celui des outils numériques, que tous nous employons quotidiennement, est fortement extra-national voire extra-européen. Comment construire alors un numérique de confiance avec, certes, un écosystème fort sur la sécurité numérique, mais faible, tout du moins en apparence, sur le numérique, brique pourtant essentielle ? Bien évidemment, la filière sécurité numérique peut renforcer la sécurité de solutions numériques que nous ne maîtrisons pas et assurer la protection, dans le sens de la confidentialité, de l'information. Mais elle est totalement impuissante dès lors qu'il s'agit d'assurer la résilience (encore un terme à définir) des solutions numériques. La disponibilité de nos outils numériques est bien souvent, pour l'utilisateur que nous sommes, plus importante que la confidentialité des données.

Le choix des solutions numériques : un dilemme ?

La crise sanitaire a renforcé notre dépendance au numérique et le besoin de disponibilité des solutions, tout le monde en est désormais convaincu. Le

recours aux outils de visioconférence par exemple a été pour beaucoup une bouée de sauvetage, que ce soit dans la sphère professionnelle ou personnelle, et le seul moyen d'assurer la continuité d'activité et le lien social avec nos proches.

Dans ce contexte, bien évidemment particulier, le volet sécurité numérique a clairement été relégué au second plan. Mais finalement ne l'était-il pas déjà auparavant ? Dans le cadre de la transformation numérique de notre société, le recours au numérique relève ni plus ni moins que de la compétitivité des organisations. Face à ce constat et cette nécessité d'évoluer rapidement, la question à résoudre pour beaucoup est en premier lieu celle du choix des outils numériques. Pour faire court, ce choix se résume aux critères suivants : « on veut que ça marche, que ce soit simple à utiliser et que ça ne coûte pas trop ». Et la sécurité ? La réponse est que la sécurité est nécessairement intégrée lorsque l'on choisit des solutions comme celles de Microsoft, Amazon, Google et les autres. En pratique, il faut bien reconnaître que ces entreprises investissent lourdement dans la sécurité numérique, en plus de répondre aux autres critères recherchés par les utilisateurs. Donc pour une PME, une ETI, une association ou une collectivité locale le choix est évident, d'autant plus que les alternatives, lorsqu'elles existent, ne sont pas ou peu connues. Pas de dilemme !

Le devoir de souveraineté numérique

Le Sénat a publié en octobre 2019 un rapport d'information fort intéressant sur le devoir de souveraineté numérique[2]. Ce rapport propose un ensemble de pistes, dont celle de la souveraineté numérique à travers une véritable politique industrielle soutenant le développement des technologies clés. Néanmoins, les besoins numériques, rappelés lors de la crise du Covid-19, ne relèvent pas nécessairement de technologies clés, tout du moins pas dans le sens où on l'entend habituellement dans « la communauté cyber » (IA, big data, blockchain, supercalculateur, 6G par exemple).

Où sont alors les solutions numériques de confiance pour les entreprises, les collectivités, les associations et les particuliers ?

Quels sont les acteurs publics et privés en France qui traitent de la

« ResNumérique », cette chose fondamentale pour notre société ? Quels sont les acteurs qui adressent ce marché ?

Un constat d'échec

Le rapport du Sénat souligne un point crucial en rappelant, pour illustrer le propos, l'échec du projet de cloud souverain : « L'État a investi dans deux projets rivaux, CloudWatt et Numergy, au début des années 2010 en choisissant de ne pas inclure OVH, acteur pourtant déjà très développé dans le cloud. Ce projet a été poursuivi par les gouvernements successifs jusqu'à son échec en 2016. Les raisons officielles de cet échec : pas d'adhésion du marché. Au final, Orange a annoncé officiellement la fermeture de CloudWatt en début d'année et l'État, selon la presse aurait perdu 56 millions d'euros dans l'histoire. ». Le chiffre de 150 millions de pertes pour l'État a parfois même été avancé[3].

Une décision politique complexe

Faut-il effectivement pour l'État impulser la création de solutions (sous-entendu souveraines) venant concurrencer celles proposées par les GAFAM qui ont aujourd'hui l'adhésion du marché ?

La réponse des pouvoirs publics actuels tend à renvoyer vers les acteurs privés et leur capacité d'investissement, mais aussi sur les lois du marché.

En effet, pourquoi faudrait-il s'acharner à dépenser de l'argent public à hauteur de ce qu'investissent, si toutefois cela est possible, les GAFAM si au final les utilisateurs préfèrent ces solutions ? Nous ne pouvons que partager cette analyse.

Faut-il alors contraindre, par la réglementation, certains utilisateurs à utiliser des solutions alternatives aux GAFAM lorsqu'elles existent ou existeront, et s'affranchir ainsi des lois du marché ?

Sur ce sujet, les États-Unis ont récemment signé un décret présidentiel interdisant l'achat d'équipements fabriqués à l'étranger par les acteurs du réseau de production et de transport d'électricité, secteur d'importance vitale.

Voilà qui donne à réfléchir ! Pour rappel, notre article 22 de la LPM n'impose rien de tel. La « seule » contrainte pour les Opérateurs d'Importance Vitale en termes de choix de solutions concerne les sondes de détection pour laquelle la loi précise que les Opérateurs doivent mettre en œuvre des sondes qualifiées. Si cela limite aujourd'hui le choix (seulement deux sondes qualifiées), cela n'exclut pas pour autant des solutions étrangères à l'avenir.

Faut-il alors être plus contraignant et imposer des solutions nationales ou européennes, à l'image du récent décret américain, et engager une politique industrielle pour construire ou renforcer ces solutions ?

Cette question délicate se pose en ce moment même en ce qui concerne le choix des équipements pour la 5G.

Le temps de l'action

Une véritable réflexion doit donc être menée quant à notre politique publique pour un numérique de confiance. Le rapport du Sénat préconise de mener une revue précise de nos avantages et de nos faiblesses dans l'économie numérique. 200 % d'accord !

Il ressortirait peut-être que :
- la France dispose de créateurs de talents qui peinent parfois à réunir des fonds pour développer des solutions numériques utiles et qui contribueraient à repositionner la France sur les rails de la souveraineté numérique ;
- lorsque les start-up développent des solutions innovantes, parfois avec le soutien et des fonds publics, elles peinent, pour ne pas dire échouent, à franchir la marche conduisant à l'industrialisation et sont rachetées par des entreprises étrangères (« StartNoUp ») : notre pays ne serait-il qu'un pays de « start », mais « up » pour les autres ?
- le marché numérique pour les PME/TPE et collectivités semble à l'abandon et manque de solutions simples et de confiance (cf. supra) ;
- la France dispose d'un fort écosystème numérique, mais il n'est pas ou peu soutenu et n'est que trop peu visible, surtout pour les petits acteurs ;
- l'éducation nationale, les universités et les organismes de recherche pourraient, voire même devraient, être des lieux de (re)développement de

la souveraineté numérique et montrer l'exemple à nos futures générations. La crise Covid-19 a révélé les lacunes dans le domaine du numérique pour certains de ces acteurs : n'y aurait-il pas là une opportunité à saisir ?

- la commande publique est plus souvent un frein qu'une aide pour développer une souveraineté numérique. Ce sujet a été mainte et mainte fois évoqué ;
- la normalisation dans le domaine numérique est un secteur insuffisamment investi par la France, alors qu'il permettrait d'appuyer le développement d'une politique pour un numérique de confiance ;

- les territoires, en particulier les Régions, peuvent réunir les conditions favorables pour développer un numérique de confiance. La Région Auvergne-Rhône-Alpes par exemple a lancé le projet de campus numérique, sans oublier d'intégrer le volet sécurité numérique.

Pour résumer, les idées et les énergies ne manquent pas pour développer un numérique de confiance. À nous maintenant et sans tarder « d'agir efficacement ensemble » en commençant peut-être par cette proposition du Sénat en complément d'une réflexion sur notre gouvernance nationale en matière de confiance numérique[4]. De nombreux experts annoncent l'arrivée d'une crise numérique à court terme : ne reproduisons pas, en attendant qu'elle arrive, le slogan « on n'a pas de pétrole, mais on a des idées » scandé durant la crise énergétique des années 70.

Il est temps d'avoir de vraies politiques publiques, réalistes et adaptées aux enjeux pour nos organisations et nos territoires sur cette chose qu'est le numérique.

Parution le 17 juillet 2020

[1] Les lecteurs pourront consulter l'étude du Sénat : « désinformation, cyberattaque et cybermalveillance : l'autre guerre du Covid-19 » (avril 2020) qui aborde très concrètement le sujet.
[2] « le devoir de souveraineté numérique » rapport du Sénat (octobre 2019)
[3] https://www.solutions-numeriques.com/securite/arret-de-cloudwatt-fin-de-partie-pour-le-cloud-souverain-finance-par-letat/
[4] Des propositions comme la création d'un ministère du numérique, d'un ministre d'État ou d'un haut-commissaire en charge du numérique pour renforcer la vocation interministérielle ont été avancées à plusieurs reprises.

Innovation de rupture et cybersécurité

WILLIAM LECAT
Directeur de Programme Grand Défi automatisation de la cybersécurité
Secrétariat Général pour l'Investissement

La rupture

Il est important de bien distinguer les notions de rupture technologique et d'innovation de rupture. La première nous offre de nouvelles possibilités, alors que la deuxième amène de nouvelles applications. En effet, l'innovation de rupture au sens où on l'entend en général est centrée sur la modification des usages. Néanmoins, le lien entre les deux reste étroit et bidirectionnel dans la mesure où de nouveaux usages stimulent des ruptures technologiques pour mieux y répondre et où les ruptures technologiques ouvrent de nouvelles possibilités pour l'innovation d'usage.

On retrouve principalement trois types d'innovation de rupture. Celui qui vient le plus facilement à l'esprit concerne la « rupture de marché ». Il s'agit à la fois d'un nouvel usage et d'un nouveau marché. C'est par exemple le cas d'AirBnB qui amène un nouvel usage de location de logements de particuliers dans le cadre d'une plateforme en ligne grand public. Le deuxième type correspond à la « rupture de sens ». Ici, un nouvel usage est poussé sur un marché existant. L'illustration typique est l'apparition de l'iPhone qui révolutionne l'usage du téléphone portable. Enfin, le dernier type correspond à une « rupture par le bas » rendant accessible au plus grand nombre un usage existant (par exemple, la Ford T ou les vols low cost).

Par définition, une technologie de rupture est (le plus souvent) une technologie naissante. Il arrive donc fréquemment qu'elle sous-performe par rapport à l'existant, à sa création. Ce n'est qu'avec une certaine maturité que cette nouveauté pourra supplanter les technologies devenues obsolètes. Ce

processus peut parfois donner l'impression qu'anticiper ce type de rupture est plus aisé en identifiant des technologies prometteuses parmi celles en cours de maturation. Il n'en reste pas moins que l'anticipation de la rupture elle-même, c'est-à-dire de la création et non de la maturation de la technologie, est très ardue, voire impossible.

De même, l'innovation de rupture peut troubler par son apparente simplicité à la fois du nouvel usage et, souvent même plus, de la technologie sous-jacente. Trop souvent, les innovations de rupture sont considérées comme ne reposant pas sur des ruptures technologiques, or c'est assez fréquemment le cas. Si la coïncidence (voire la précédence) temporelle de la rupture d'usage avec la rupture technologique est assez rare, il n'en reste pas moins que, pour reprendre les exemples précédents, AirBnB a été rendu possible par la démocratisation d'Internet à la suite de l'arrivée de l'ADSL puis de la 3G et de la 4G ; que l'iPhone s'est appuyé à sa création sur les technologies tactiles et sur la 3G, etc.

Déterminer lequel des deux, de l'usage et de la technologie, est le premier correspond souvent au problème de l'œuf et de la poule, les deux étant parties prenantes dans un cycle. En effet, les nouvelles technologies en maturation amènent de nouvelles possibilités engendrant de nouveaux usages, appelant de nouvelles technologies. La richesse de l'innovation d'un domaine est donc particulièrement dépendante de la vitesse de révolution de ce cycle et de son intrication avec les cycles des domaines connexes.

En réalité, l'absence de ruptures technologiques rend l'innovation de rupture plus difficile. De plus, la maîtrise de ces technologies de rupture est un prérequis minimal pour pouvoir les appliquer.

Il n'en reste pas moins que l'arrivée d'une rupture technologique est très rarement couplée à une innovation de rupture. Il semble que pour impulser de nouveaux usages, ces technologies doivent être en mesure d'atteindre certains niveaux de maturité. C'est d'ailleurs logique puisque les innovations de rupture sont le plus souvent des innovations d'usage, elles s'appuient donc sur des usages. Il est donc fondamental que ces technologies sous-jacentes soient prêtes pour une application industrialisée.

La cybersécurité

Dans ce contexte, le cas de la cybersécurité est très spécifique. En effet, la cybersécurité existe pour les besoins d'un autre marché : le numérique. Ce dernier est bien souvent un catalyseur vis-à-vis d'autres domaines (industrie, médical, transport, etc.). Le dynamisme de la cybersécurité est ainsi largement favorisé par ses multiples applications, chaque nouveauté dans un domaine d'application pouvant stimuler une innovation en cybersécurité. Cette effervescence est renforcée par la rapide évolution des technologies (parfois de ruptures) et leurs applications galopantes à tous les domaines ouvrant ainsi la porte à de nombreuses innovations de rupture. Tous ces éléments contribuent à expliquer les évolutions rapides sur des cycles très courts dans ce secteur.

La cybersécurité est donc naturellement exposée à de nombreuses ruptures technologiques ou d'usage dans le secteur en lui-même (par exemple, l'application de l'intelligence artificielle pour la détection de menaces), mais aussi dans ses domaines d'application (objets connectés, 5G, etc.). Il y a ainsi une distinction à faire entre de nouveaux usages de cybersécurité et la cybersécurité des nouveaux usages. Ce dernier aspect est souvent considéré comme une menace ou un problème du point de vue de la sécurité. En effet, les ruptures d'usage arrivant de plus en plus vite et se diffusant tout aussi rapidement, l'adaptation de la sécurité pour les prendre en compte est souvent en retard et dans tous les cas, confinée à une position réactive. La réponse à ce problème a été trouvée depuis longtemps déjà : il faut être sécurisé « by design » et non pas a posteriori. Il est d'ailleurs essentiel que la cybersécurité ne soit pas un frein à ces nouveaux usages pour faciliter son adoption rapide et la plus large possible. C'est bien sûr ce vers quoi il faut tendre, grâce aux prises de conscience des utilisateurs et des fournisseurs, et par la réglementation dans certains cas. Néanmoins la route est encore longue. Malgré tout, même dans une configuration idéale, certaines problématiques subsistent dans la mesure où l'impact et l'évolution de ces nouveaux usages sont difficilement prédictibles et dès lors que la sécurité peut être affectée de manière inattendue.

À l'opposé, du point de vue de l'innovation, les évolutions constantes dans les domaines d'application de la cybersécurité représentent des opportunités.

Innover constamment est donc nécessaire que ce soit en adressant de nouveaux usages (nécessitant parfois des ruptures technologiques en cybersécurité) ou en proposant des ruptures (d'usage) dans la manière d'approcher la sécurité. L'innovation est d'autant plus favorisée par la forte proportion de solutions logicielles pouvant être apportées aux problématiques de cybersécurité. Le développement logiciel présentant moins de barrières à l'entrée que d'autres domaines (nécessitant de grosses infrastructures par exemple), de nouveaux acteurs apparaissent en permanence.

Face à cette marche forcée de l'innovation, les acteurs économiques fournisseurs de cybersécurité sont tiraillés entre une recherche de stabilité, la conquête de nouveaux marchés et la concurrence toujours plus diverse. S'il est bien clair pour de tels acteurs qu'une innovation permanente est un prérequis, les démarches d'anticipation restent variées. Or, il apparaît qu'anticiper de nouveaux besoins correspond plus à être proactif sur les innovations incrémentales dans les domaines d'applications alors que l'arrivée de nouveaux usages (innovation de rupture) n'est que rarement anticipée (sinon, la rupture serait moindre, les usages pouvant s'adapter progressivement) à part par ceux qui les poussent, et encore.

Grand Défi cyber

Les cycles courts et les évolutions rapides de la cybersécurité imposent une maturation rapide des technologies afin de resserrer le lien entre les usages et les technologies. C'est exactement dans ce cadre que s'inscrit le Grand Défi cyber, l'objectif étant de financer des technologies pouvant faire émerger une rupture tout en poussant de nouveaux usages. Ainsi, pour tous les projets soutenus, on cherchera à établir un partenariat avec un industriel qui amènera sa problématique et qui pourra bénéficier des nouvelles approches permises par les technologies et les produits développés. L'idée est de pouvoir procéder à des expérimentations en boucles courtes pendant le développement pour arriver le plus rapidement possible à un produit utilisable, basé sur de nouvelles technologies.

Le découpage de la sélection et de la réalisation des projets reflète cette démarche. En effet, une première phase du Grand Défi devrait débuter la semaine prochaine (avec l'ouverture des candidatures) et s'achèvera de

manière simultanée pour tous les projets en janvier 2022. On prévoit donc entre 12 et 15 mois de réalisation. À l'issue, une seconde sélection aura lieu pour accélérer les projets les plus prometteurs, qui auront amené des ruptures technologiques et d'usage, sur une période de 11 mois jusqu'à fin 2022 constituant la seconde phase.

Sur ces deux phases, environ 25 millions d'euros provenant du Grand Défi, principalement sous forme de subvention à un taux pouvant aller jusqu'à 50 %, seront dédiés au financement des projets pour lever des verrous technologiques et développer des technologies de rupture. Il s'agira donc d'un co-investissement (public/privé) d'au moins 50 millions d'euros.

Les projets sélectionnés seront centrés sur les trois axes verticaux de la feuille de route du Grand Défi : l'impact des nouveaux usages sur les réseaux, les objets connectés et la protection des petites structures.

Cette démarche devra préfigurer des initiatives de plus grande ampleur pouvant prendre le relais et permettant à la France de devenir un leader mondial dans le domaine de la cybersécurité.

Parution le 24 juillet 2020

Dérive du modèle français de cybersécurité : origines, conséquences, remèdes

CHRISTIAN DAVIOT
Ancien conseiller stratégie
du directeur général de l'ANSSI

Introduction

L'analyse froide et désincarnée des textes administratifs qui étayent le modèle français de cybersécurité viendra en son temps, dans des manuels qui tomberont de la main des lecteurs tant l'amphigouri de certains de ces textes reflète peu les circonstances exceptionnelles et les débats passionnés qui les ont générés. Il est vrai que ces textes n'ont pas été rédigés pour rappeler une évidence : les gouvernements, administrations, parlements, entreprises et organisations non gouvernementales français et étrangers qui ont contribué directement ou indirectement à imaginer, développer et… fragiliser la cybersécurité française sont animés par des êtres humains aux cultures, niveaux de compréhensions, visions, motivations professionnelles ou personnelles pour le moins diverses.

La responsabilité de la dérive est collective. 2020 est probablement une année charnière pour le modèle français de cybersécurité. Il semble donc utile de rappeler succinctement ce qui en a fait la force, en fait la faiblesse aujourd'hui et les conséquences qu'engendrerait une dérive trop prononcée de ce modèle. Et de proposer quelques pistes.

2007 – 2017 : la construction

Si aucune allusion n'y est faite dans la lettre de mission[1] confiée en août 2007 à un ancien secrétaire général de la défense nationale, l'attaque informatique subie par l'Estonie quelques mois plus tôt est dans les esprits et dans les débats des membres de la commission de préparation du Livre blanc

sur la défense et la sécurité nationale.

Préfacé - donc endossé - par le Président de la République et publié en juin 2008, le Livre blanc[2] institue un « Conseil de défense et de sécurité nationale », annonce la mise en place d'une capacité de lutte informatique offensive et la création d'une agence chargée de la sécurité des systèmes d'information relevant du Premier ministre et de la tutelle de ce qui devient le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN).

Les fondamentaux du modèle français de cybersécurité sont ainsi posés. La sécurité des systèmes d'information est un sujet interministériel, les capacités offensives relèvent quant à elles du ministère de la défense. Ce choix contraste avec ceux des états alors les plus actifs dans le domaine, qui ont confié défensif et offensif à leurs services de renseignement.

Durant les mois qui suivent la publication du Livre blanc, la combinaison parfaite du Secrétaire général de la défense et de la sécurité nationale - conseiller d'État - et d'un de ses conseillers - X-télécoms - pour appréhender le sujet avec la hauteur de vue nécessaire et la compréhension technique indispensable, permet la préfiguration de la future agence sur la base d'une des directions du SGDSN. L'Agence Nationale de la Sécurité des Systèmes d'Information, l'ANSSI, naît le 7 juillet 2009. Le décret[3] de création de l'agence la rattache au Secrétaire général de la défense et de la sécurité nationale et n'en fait pas une simple direction du SGDSN. Il l'installe comme service à compétence nationale - elle peut intervenir sur l'ensemble du territoire -, et comme « autorité nationale en matière de sécurité des systèmes d'information » chargée de multiples missions dont celle de coordonner les travaux interministériels dans son champ de compétence. L'agence compte alors moins d'une centaine de personnes, essentiellement des ingénieurs civils et des militaires.

Le Parlement vient alors de voter la loi « Création et Internet » qui envisage l'installation d'un mouchard[4] sur les ordinateurs soupçonnés de télécharger illégalement, via internet, des œuvres protégées. Cette mesure technique, faille de sécurité potentielle, a bien été identifiée par les promoteurs de l'agence qui ont choisi de ne pas intervenir auprès des cabinets ministériels lors de l'élaboration du projet de loi ou auprès des députés au cours des débats

parlementaires : trop d'incompréhension technique des sujets.

Dès l'automne 2009, l'ANSSI entame l'élaboration d'une stratégie. Adoptée début 2010 par le comité stratégique de la sécurité des systèmes d'information prévu par le décret de création de l'agence, la stratégie de la France en matière de défense et sécurité des systèmes d'information répertorie une quarantaine d'actions regroupées en quatre objectifs et sept axes de travail. Elle sera le seul leg du comité, organe à caractère consultatif qui ne trouvera pas son équilibre de fonctionnement, notamment en raison de la présence intermittente d'intervenants de la direction de la modernisation de l'État alors attachée à Bercy. Le comité sera supprimé en 2015.

La stratégie, dont la version publique[5] ne sera publiée qu'en mai 2011, adopte une terminologie simple : la cybersécurité, état recherché, 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.

Fin 2010, l'ANSSI identifie une attaque informatique à des fins d'espionnage menée contre Bercy. Les informations recherchées et régulièrement collectées par l'attaquant ne laissent guère de doute quant à son origine géographique. À cette occasion, l'agence élabore une méthodologie de traitement des attaques informatiques. Associée au développement de capacités de détection des attaques informatiques initié simultanément, cette méthodologie en constante évolution depuis cette date permet aux experts de la « sous-direction opérations » de l'agence d'être sans conteste parmi les meilleurs au monde en matière de traitement de crise informatique.

Un incident significatif interviendra durant les trois mois que prendra le traitement de l'attaque : un des experts de l'ANSSI constate que l'attaquant est en ligne et qu'il est en mesure d'accéder à sa machine, ce qui permettrait vraisemblablement de l'identifier. L'officier de police judiciaire qui accompagne l'ANSSI le lui interdit au motif que cela constituerait une atteinte à un système de traitement automatisé de données relevant du code pénal… Cet incident sera le début d'une réflexion de l'agence sur l'aménagement du droit national, afin de permettre une réponse proportionnée aux attaques subies.

L'attaque informatique contre Bercy, que le ministère a bien voulu rendre publique à des fins pédagogiques, est l'occasion pour l'ANSSI d'élaborer une série de mesures destinées à renforcer la sécurité des systèmes d'information des administrations et, grâce au soutien sans faille des cabinets militaires du Président de la République et du Premier ministre, de les proposer à l'arbitrage, accompagnées d'un plan de développement de l'agence. Mesures et plan sont présentés lors d'un conseil des ministres[6] en mai 2011.

Juillet 2012. Les attaques contre les systèmes d'information, d'origine étatiques ou non, appartiennent aux sujets d'étude que le Président de la République souhaite voir étudiés dans la lettre de mission[7] adressée au conseiller-maître de la Cour des comptes juste revenu de sa mission à l'ONU, en vue de l'élaboration d'un nouveau Livre blanc.

Identifiant l'opportunité offerte par les travaux pour l'élaboration du Livre blanc, le directeur général de l'ANSSI, qui a constaté que les entreprises comme les administrations peinent à intégrer dans leurs priorités la sécurité de leurs systèmes d'information, décide d'utiliser la loi pour contraindre les plus sensibles d'entre elles à mettre en œuvre les politiques nécessaires. L'ANSSI participera donc très activement aux travaux de la commission du Livre blanc, notamment par une solide contribution écrite en lien avec les ministères de la Défense et de l'Intérieur et communiquée à chaque membre de la commission.

Parallèlement, pour prévenir une action de lobbying contre son projet, le directeur général ira au-devant des grandes entreprises et de leurs associations représentatives afin de leur expliquer les raisons du recours à la réglementation.

La question se pose alors de l'établissement de la liste des entreprises qui seront visées par la loi. Pour éviter tout obstacle européen, le choix est fait de retenir la liste des entreprises appartenant aux secteurs d'activité d'importance vitale, déjà visés par une réglementation acceptée par Bruxelles. Un choix imparfait, notamment parce que la liste est protégée par le secret de la défense nationale - et qu'il est difficile de mobiliser des personnels lorsqu'on ne peut pas leur en expliquer les raisons - et que la réglementation est alourdie par des textes anciens peu adaptés au développement du numérique.

Les propositions de l'ANSSI seront retenues et insérées dans le Livre blanc[8] rendu public en avril 2013.

En référence à l'incident intervenu pendant le traitement de l'attaque informatique contre Bercy, l'ANSSI proposera une disposition législative supplémentaire permettant d'accéder au système d'information d'un attaquant dans certaines conditions, afin de caractériser l'attaque et d'en neutraliser les effets (pas les causes…). Les articles 21 à 25[9] de la loi de programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale seront votés à l'unanimité sur la base de l'étude d'impact rédigée par l'ANSSI.

Deux points sont à noter concernant cette législation[10] :

- Portée par l'ANSSI au niveau européen, elle servira de base à la future directive européenne « Network and Information System Security (NIS) » qui sera adopté en 2016.
- L'article 22 de la loi impose pour certains systèmes l'utilisation de sondes de détection d'attaques informatiques maîtrisées[11], exploitées sur le territoire national par des personnes habilitées. Cette disposition, très contraignante, sera difficile à mettre en œuvre. Il aura d'abord fallu convaincre les industriels français de développer un produit, éventuellement associé à un service, pour un marché national réduit. Les spécificités techniques et fonctionnelles souhaitées étaient également un obstacle qu'un grand industriel a renoncé à franchir. Au final, une startup a, la première, relevé ce défi, suivie par l'autre grand industriel du secteur.

En cette même année 2013, la révélation de documents issus des services de renseignement américains et des révélations relatives à des attaques informatiques spectaculaires (Stuxnet, Shamoon) montrent que des états pratiquent non seulement l'espionnage de manière massive - l'espionnage n'est pas interdit en droit international, excepté lorsqu'il vise certaines pratiques diplomatiques - mais aussi le sabotage via les réseaux informatiques, par l'insertion dans les réseaux de bombes logiques appelés « implants » dans le jargon.
Prenant en compte la progression du numérique dans tous les secteurs de la société, les nouveaux usages et l'évolution de l'environnement international, le nouveau directeur général de l'ANSSI décide à l'été 2014 d'engager une

démarche interministérielle destinée à élaborer une stratégie nationale. Un séminaire de lancement a lieu en présence de toutes les administrations concernées et de Corinne ERHEL, députée des Côtes-d'Armor, auteur, avec Laure DE LA RAUDIÈRE, députée d'Eure-et-Loir, d'un rapport sur le développement numérique de l'économie française. Des groupes de travail sont constitués, pilotés par différents ministères. Après plusieurs mois de travail, les conclusions des groupes de travail sont entérinées lors d'un séminaire de conclusion réuni autour d'Axelle LEMAIRE, Secrétaire d'État chargée du Numérique qui soutient activement la démarche et avec le cabinet de laquelle l'ANSSI a des réunions très régulières.

La stratégie nationale pour la sécurité du numérique[12] est présentée en octobre 2015 par le Premier ministre[13] et Axelle LEMAIRE devant 800 personnes réunies à Paris.

En 2016, les Etats-Unis veulent généraliser le *hack back* qui permettrait à une entreprise de répondre à une attaque informatique par une attaque informatique. Ce principe correspond à la stratégie de cybersécurité des Etats-Unis[14] fondée, comme plus largement le modèle de sécurité américain, sur la domination technologique et l'emploi de la force. Or, un tel principe est une aberration technique : l'attaquant informatique apparent n'est pas nécessairement l'attaquant réel. Mis en œuvre, le *hack back* serait un danger majeur pour le modèle français de cybersécurité, empêchant de fait l'ANSSI de remplir sa mission et serait un risque pour la survie même du numérique.

Face au lobbying américain sur ce sujet via des *think tanks* qui font la tournée des gouvernements européens, l'ANSSI convainc le SGDSN d'organiser une conférence internationale destinée à amener spécialistes du droit international, entreprises et gouvernements à se prononcer contre des actions offensives dans le numérique en temps de paix[15]. D'abord pensée en petit comité à la demande du Secrétaire Général, l'organisation de la conférence s'effectue ensuite sur une base plus large, associant le ministère des Affaires étrangères et celui de la Défense. Appuyée par une étude réalisée par des professeurs de droit international[16] de l'Université Grenoble-Alpes, « Construire la paix et la sécurité internationales de la société numérique[17] » cette conférence a lieu début avril 2017 à l'UNESCO. Elle réunit des représentants de gouvernements, d'entreprises, d'ONG et des universitaires

des cinq continents. Cette conférence sera également l'occasion d'un premier contact entre l'ANSSI et son homologue de la Cyberspace administration of China.

Le consensus sera général parmi les participants pour repousser le principe du hack back systématique.

Sauf rebond à venir, cette conférence aura constitué le climax du modèle français de cybersécurité.

2018 : la dérive

Début 2017, une « note blanche » est élaborée afin de nourrir les débats sur le numérique dans le cadre de la campagne des élections présidentielles. Elle met en avant les trois leviers pour le numérique et la cybersécurité que sont l'identité numérique de niveau élevé (au sens eIDAS), les villes et territoires intelligents, la 5G.

Mai 2017. Tout juste élu, le Président de la République évoque[18] la cybersécurité avec un scientifique candidat aux législatives. La réponse du Président est éclairante : il considère que la France est en retard. Ses modèles sont israéliens et états-uniens, mais il estime qu'il faut désenclaver la cybersécurité du seul domaine militaire et que ce sujet a une dimension européenne. Il évoque la nécessité de renforcer le partenariat franco-allemand sur ce thème. Le Président termine en ajoutant qu'il compte donner les moyens budgétaires nécessaires au développement de la cybersécurité en les incluant dans les 2 % du budget qu'il souhaite voir attribué à la Défense.

À cette date, le Président ne connaît donc pas l'organisation française en matière de cybersécurité. Il ignore également que le modèle français, essentiellement civil, a servi de base à la réflexion et à l'organisation européenne ou que le partenariat avec le Royaume-Uni est particulièrement riche.

Quelques semaines plus tard, dans un discours[19] à l'Hôtel de Brienne qui restera dans les mémoires pour d'autres raisons, le Président de la République demande à la ministre des Armées d'engager une revue stratégique de défense

et de sécurité nationale en amont d'une future loi de programmation militaire. En osmose avec les textes et la pratique, il rappelle ensuite que « des opérateurs des armées contribuent, sous la coordination générale du Premier ministre et en soutien de l'ANSSI, à la détection et à l'attribution des attaques et donc à la cybersécurité nationale », et demande au Premier ministre l'élaboration d'une revue stratégique de la cyberdéfense. L'échéance de ces deux revues est fixée à la fin de l'année.

Le député européen mandaté par la ministre des Armées pour présider le comité de rédaction remet la revue stratégique de défense et de sécurité nationale courant décembre.

En parallèle, le Secrétaire Général de la Défense et de la Sécurité Nationale qui s'est vu confié la revue stratégique de cyberdéfense a engagé des travaux interministériels auxquels les administrations contribuent abondamment. Devant la qualité de la revue stratégie de défense et de sécurité nationale qui prend parfaitement en compte les enjeux de souveraineté numérique, consigne est glissée d'élaborer un document plus volumineux et foisonnant. Rapporteur et administrations sont finalement court-circuités au profit d'un exercice qui aboutira à une revue stratégique de cyberdéfense[20] dont le principal mérite est d'être pédagogique pour le néophyte quant à l'analyse de la menace.

Il faudra revenir plus longuement sur ce document qui sera publié par l'ex-secrétaire général après son départ sous le titre de « Stratégie nationale de cyberdéfense[21] ».

Point nodale du texte, quatre chaînes opérationnelles sont mises en place. Une chaîne « protection » confiée à l'ANSSI, une chaîne « action militaire » qui relève du ministère des Armées, une chaîne « renseignement » menée par les services et une chaîne « investigation judiciaire » suivie par les ministres de l'Intérieur et de la Justice. Une comitologie est également instaurée qui entérine le fait que les grandes décisions concernant la cybersécurité sont prises en conseil de défense et de sécurité nationale.

Si le processus décisionnel est formalisé, la création de quatre chaînes opérationnelles signe la fin de la singularité du modèle français de

cybersécurité par l'éclatement des responsabilités et le déséquilibre des arbitrages pour la défense et contre l'économie.

2020 : le déclin ou le rebond

S'il faut rester optimiste par nécessité, les discours donnés et les actes engagés depuis trois ans sont contradictoires et finalement peu rassurants. À l'issue d'une période où l'activité de la France ne s'est pas tout à fait arrêtée grâce au numérique, constats et réflexions sur le modèle français de cybersécurité sont tenus par la prise en compte du numérique dans son ensemble.

Faire du modèle français de cybersécurité un avantage concurrentiel[22] pour la France est une responsabilité collective. L'action du gouvernement est évidemment clé, comme l'est l'audace des administrations, comme le sont les choix des entreprises, l'analyse transverse du Parlement, la stimulation apportée par les ONG. Mais c'est en premier lieu de vertus dont nous devons faire preuve. D'humilité, de volonté et de courage.

L'humilité comme point de départ
Il nous faut reconnaître que nous ne donnons pas au numérique la priorité qu'il mérite. Norbert WIENER avait anticipé la capacité du numérique à absorber le reste du monde. « La sociologie et l'anthropologie sont avant tout des sciences de la communication, et relèvent en tant que telles de la cybernétique en général. Cette branche particulière de la sociologie qu'est l'économie, qui s'en distingue en ce qu'elle possède de meilleures mesures numériques de ses valeurs que le reste de la sociologie, est une branche de la cybernétique en vertu du caractère cybernétique de la sociologie elle-même. », écrivait l'inventeur de la cybernétique, en 1956[23] ! Du quotidien des PME à celui des états, de la conduite de la guerre à la transition écologique, des échanges familiaux aux délires transhumanistes, rien ne peut s'envisager désormais sans le numérique et sa cohorte de sujets liés. Pas de retour en arrière possible.

Or, il faut remonter jusqu'au siècle dernier pour trouver un ministre en charge du seul portefeuille du numérique[24]. Si le secrétaire d'État en charge du numérique dans le premier gouvernement de ce quinquennat était placé auprès du Premier ministre - comme la cybersécurité, le numérique est

interministériel par nature - il était vingt-deuxième et dernier dans l'ordre protocolaire. Son successeur, exilé à Bercy, se retrouve trente-et-unième sur trente-cinq et a perdu l'autorité sur la direction interministérielle du numérique. Aujourd'hui, le secrétaire d'État chargé de la transition numérique et des communications électroniques, partagé entre Bercy et la cohésion des territoires, est trente-huitième sur quarante-deux membres du gouvernement. Sans importance réelle pour le grand public, ordre protocolaire et décrets d'attribution sont regardés de près par les administrations qui jugent ainsi de l'importance du sujet aux yeux du Président de la République - leur seule référence utile.

Pour les administrations et les entreprises, elles aussi attentives, le numérique n'est donc pas une priorité du gouvernement. Ce sujet a d'ailleurs été le grand absent des discours de politique générale des deux Premiers ministres du quinquennat. Dans ces conditions, comment s'étonner que la France ne soit que dans la moyenne des pays européens en matière de numérique[25] et, à vrai dire, en retard par rapport aux pays avec lesquels elle prétend se mesurer ?

Il nous faut reconnaître que nous devons à nos choix successifs la situation délicate dans laquelle se trouve notre pays. « *Nos vrais ennemis sont en nous-mêmes* »[26]. Dans les années 1990, celles de la fin de l'Histoire et du capitalisme mondialisé triomphant, les énarques de Bercy se gaussent des travaux[27] du rapporteur général du budget au Sénat qui prophétise que les délocalisations des usines vers les pays à bas coût de main d'œuvre entraineront le départ des laboratoires de recherche et à terme une perte de souveraineté. Au tournant des années 2000 c'est un ingénieur diplômé d'une grande école française, aux commandes d'un équipementier français d'envergure mondiale des télécoms qui eut cette idée folle d'imaginer un groupe industriel sans usine. Dans le numérique comme dans d'autres secteurs, nous payons aujourd'hui les conséquences de la faillite de la pensée d'une part des élites françaises.

Il nous faut reconnaître que, centrés sur nous-mêmes, nous ne voyons que tardivement l'évolution rapide de notre environnement économique et politique. En 2024 selon le World Economic Forum[28], l'économie française passera de la sixième à la dixième place des économies mondiales. La Chine devancera les Etats-Unis et quatre pays asiatiques seront dans les cinq

premières places, la Russie arrivera en sixième position. Le contexte de guerre froide Etats-Unis vs Union soviétique, dans lequel ont été formés, raisonnent et agissent aujourd'hui encore les fonctionnaires occupant les plus hauts postes de responsabilité, est dépassé. Pour se préparer à vivre dans un monde différent il faudrait s'appuyer sur les connaissances et les expériences des universitaires et des entrepreneurs habitués aux cultures, usages et marchés de ces pays.

Or « *L'idée est l'ennemie capitale des souverains*[29] ». Pour l'administration qui a fait sienne cette maxime impériale, il ne faut pas sortir du confort de la reproduction.

Les études et rapports d'experts, les rapports parlementaires ne sont ainsi généralement pas lus à la hauteur de ce qu'ils pourraient apporter comme idées, et surtout comme actions. Les administrations préfèrent généralement ruminer des idées déjà digérées dans le silo voisin de ministères « compétents ».

Les personnes porteuses d'idées ou de pratiques nouvelles sont rarement tolérées dans le temps. Ainsi, le départ du premier secrétaire d'État chargé du numérique, officiellement pour des raisons de campagne électorale, s'est parallèlement accompagné de l'exfiltration de la seule personne en mesure de mener à son terme la transition numérique des administrations en favorisant l'expérimentation et le développement agile. Jugé trop remuant et trop créatif, il a été remplacé à la tête de la direction interministérielle du numérique par un profil plus conforme au feutre administratif. Son départ a été suivi d'une hémorragie des compétences de la DINUM.

Les organismes censés accompagner l'évolution de la société sont eux-mêmes victimes de la recherche d'économies lorsqu'ils ne sont pas soutenus. Ainsi le gouvernement a décidé en 2019 de la suppression de l'Institut national des hautes études de justice et de sécurité qui, sous la conduite d'Hélène CAZAUD-CHARLES avait pourtant mis en place, parmi d'autres sujets, un cycle de formation aux enjeux de la cybersécurité d'excellente qualité.

L'ANSSI n'est pas à l'abri de ces enfermements. Ainsi, il aura fallu sept ans et la détermination de ses deux directeurs généraux successifs pour que les

experts de l'agence se dotent d'un conseil scientifique.

Longtemps le cloud computing n'a été considéré par l'agence que comme un simple retour du client-serveur. Il aura fallu plusieurs réunions avec un équipementier télécoms non européen qui demandait à l'ANSSI ce qu'il faudrait ajouter aux standards en discussion finale pour améliorer la cybersécurité de la 5G pour que l'agence s'investisse sur ce nouveau protocole.

Les premiers actes et le style adopté par le nouveau Premier ministre, la nomination au poste clé de Secrétaire Générale du Gouvernement de Claire LANDAIS qui a suivi l'activité de l'ANSSI ces deux dernières années, sont un signe que l'humilité succède à l'arrogance.

La volonté ensuite

Une fois la prise de conscience effectuée, l'arrogance tempérée par un peu d'humilité, forts des capacités françaises en matière de recherche et des grands acteurs du secteur - opérateurs télécoms, sociétés de service, startups et licornes potentielles - il est possible de doter la France d'une stratégie en matière de numérique, au-delà des stratégies de niche actuelles. Les idées existent, les acteurs du secteur en proposent régulièrement[30], de multiples rapports parlementaires en développent, notamment sur les trois leviers communs au numérique et à la cybersécurité que sont l'identité numérique[31] - des arbitrages sur ce sujet étaient déjà prêts en 2016 -, la ville et les territoires intelligents[32] - les collectivités sont livrées à elles-mêmes sur ce sujet pour lequel se posent pourtant des questions de souveraineté, d'égalité, de libertés et de protection des données.

Pour la 5G, levier essentiel, le gouvernement ayant choisi dans les faits d'écarter les équipementiers non européens de la construction des futurs réseaux 5G, l'optimisme pousse à croire qu'existe déjà, partagée avec d'autres membres de l'Union, une stratégie de soutien des équipementiers européens qui procure une alternative d'équipements maîtrisés de même niveau technique et permette d'envisager les générations suivantes.

L'élaboration et le suivi d'une telle stratégie du numérique pourrait être confiée au Commissariat destiné à remplacer le Commissariat général à la stratégie et à la prospective créé en 2013[33], « France-Stratégie », dont les

travaux n'ont pas été de nature à inspirer administrations et décideurs politiques. Il appartiendra au nouveau Haut-Commissaire de veiller à ce que cette stratégie survive aux gouvernements. En matière de cybersécurité comme dans d'autres domaines, la Nouvelle France Industrielle du précédent quinquennat comportait des « feuilles de route » qui auraient mérité un peu de continuité. La quête d'éléments de communication susceptibles de montrer que les gouvernements agissent d'une part et l'appétence de quelques grandes entreprises pour les subventions qui accompagnent les programmes repeints d'autre part ont généralement raison de la continuité des politiques.

Enfin une stratégie du numérique devrait adopter une ambition claire et les moyens nécessaires, à l'instar de nos voisins allemands. En juin dernier, le gouvernement allemand a en effet décidé d'investir 9 des 130 milliards d'euros de leur plan de relance dans la filière hydrogène afin de devenir le numéro un mondial dans dix ans[34]. En 2018, le plan hydrogène de la France était doté de 100 millions d'euros, près de cent fois moins. Le plan de relance annoncé cet automne fixera sans doute une perspective plus réaliste.

Le courage enfin

À l'international, être fidèle à ce que nous sommes. En choisissant un modèle de cybersécurité interministériel, dans lequel les pratiques défensives et offensives ne sont pas confiées aux mêmes acteurs, même s'ils travaillent ensemble, la France a choisi le seul choix qui permette le développement d'un numérique durable. Sous l'impulsion de la France, l'Union européenne a choisi une approche similaire. Un peu de courage pourrait peut-être aider à limiter les actions offensives néfastes de certains états dans le numérique. Lancé en 2018, l'« Appel de Paris pour la confiance et la sécurité dans le cyberespace[35] », conçu à l'origine par le Quai d'Orsay pour reprendre la main après la conférence organisée par le SGDSN à l'Unesco et répondre aux initiatives privées[36], a permis, grâce aux talents des diplomates, d'engager sur un même document près de 80 états dont certains s'opposent sur ces sujets dans les instances multilatérales et 650 entreprises. Devant l'impasse dans laquelle se trouvent les discussions du groupe d'experts de l'ONU face aux deux résolutions présentées par deux blocs d'états, l'Appel de Paris pourrait être enrichi, par exemple par la recherche des éléments communs à toutes les initiatives, et mieux exploité pour favoriser le désarmement dans l'espace numérique.

De la même manière, la décision récente de la Cour de Justice Européenne à propos du *privacy shield*, la volonté de l'ONU d'élaborer un texte sur la cybercriminalité, le projet de loi américain Earn it[37] sont autant de sujets sur lesquels la France pourrait s'exprimer et peser avec ses alliés européens pour conforter ses choix et promouvoir ses valeurs.

Certaines organisations internationales[38] évoquent la cybersécurité comme un droit humain : la marge de manœuvre à l'international est donc importante.

En France, adopter des voies nouvelles. Vouloir que des startups innovantes deviennent des licornes au rayonnement mondial implique de s'exposer aux marchés et aux capitaux. Limiter les investissements étrangers dans les startups revient à les condamner au marché français ou, au mieux, européen.

Certains leviers restent à notre disposition. Celui de la commande publique par exemple qui représente 90 milliards d'euros annuels[39]. Une potentielle licorne française qui a décidé d'attaquer le marché américain a vu son principal concurrent local bénéficier d'un contrat public de 50 millions de dollars, lui procurant ainsi un avantage concurrentiel et la certitude d'une valorisation conséquente. En France, « *L'innovation reste un ovni, mal appréhendé dans la communauté de la commande publique*[40]». Pourtant, un décret de décembre 2018, sous-utilisé, autorise la conclusion de marchés sans mise en concurrence pour des achats innovants en dessous de 100 000 euros (un début !). De la même manière, on pourrait dans certains cas exclure de certains marchés publics les entreprises dépendantes d'un droit extra-européen.

À plusieurs reprises, le Président de la République a proposé des idées qui pourraient favoriser le développement du numérique et conforter le modèle français[41]. Ainsi en est-il du projet de Campus Cyber voulu par le Président de la République, inspiré des modèles israélien, américain, russe ou chinois mais fondé sur la création de communs opérationnels.

Confié au seul entrepreneur capable de réunir tous les acteurs utiles, ce projet pourrait faire passer un cap d'efficacité à la cybersécurité française pour peu

qu'administrations compétentes - dont l'ANSSI - aient le courage d'y investir des équipes opérationnelles en effectifs suffisants.

Conclusion

« *La barbarie d'aujourd'hui discourt et pose. Elle est vision du monde autant que pulsion. Elle érige sa violence en justice, sa vision du monde en vérité, son idéologie en absolu, l'irruption du réel en subversion. Elle précipite le lien pour le réduire à une relation univoque : dominer ou être dominé, appartenir à la race des seigneurs ou mériter sa place d'esclave. Au niveau des Etats, elle réactive la menace de la guerre.* »[42]

Dans tous les pays où il s'est développé, le numérique est rendu possible par la recherche et l'investissement essentiellement portés par le secteur privé. De leur côté les états fondent sur le numérique une part de plus en plus importante de leur croissance, de leur fonctionnement et de celui de la société.

Pourtant, ce sont les pratiques des états donnant la priorité à l'offensif qui mettent en danger un numérique qui soutient désormais l'essentiel des services critiques fournis à leurs populations. Il y a un peu plus de dix ans, un gouvernement français a choisi à contre-courant un modèle de cybersécurité privilégiant la prévention et la défense, seul moyen d'éviter l'escalade de l'affrontement entre états dans le numérique et la guerre dans le monde matériel.

Dans un cyberespace où les armes se retournent contre leurs créateurs et ou les preuves se fabriquent en quelques clics, des voix se font entendre qui déforment les positions françaises et en appellent à l'intervention de l'armée pour protéger les réseaux civils[43]. Si des sanctions à l'encontre d'entités étrangères comme celles prises sur la base de preuves par l'Union européenne ce 30 juillet sont proportionnées, si la caractérisation de la menace et la neutralisation des effets doit être élargie à la pose d'implants comme l'ont proposé des députés au printemps dernier[44], les discours autour d'une mal nommée « cyberdissuasion » doivent être tenus avec circonspection.
Dans le numérique, « Si vis pacem, para pacem ».

Par son histoire, sa culture, ses valeurs et ses choix, la France a une responsabilité dans le devenir du numérique. Avec de l'humilité, de la volonté et du courage, notamment de la part du gouvernement et des administrations, elle pourra, comme par le passé, peser en faveur d'une approche favorable au développement du numérique et respectueuse de la souveraineté des états pour peu qu'elle conserve l'approche pluridisciplinaire déjà identifiée comme une nécessité il y a soixante-dix ans : « *Il ne serait peut-être pas mauvais que les équipes présentement créatrices de la cybernétique adjoignent à leurs techniciens venus de tous les horizons de la science quelques anthropologues sérieux et peut-être un philosophe curieux de ces matières*[45]. »

Parution le 31 juillet 2020

[1] http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/Lettre_mission_JCMallet.pdf
[2] http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html
[3] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212&categorieLien=id
[4] Cf. article 5 de la LOI n° 2009-669 du 12 juin 2009. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id
[5] https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf
[6] http://archives.gouvernement.fr/fillon_version2/gouvernement/la-politique-de-securite-des-systemes-d-information.html
[7] http://www.livreblancdefenseetsecurite.gouv.fr/pdf/2012-07-13-lettre-de-mission-pr-livre-blanc.pdf
[8] https://www.vie-publique.fr/rapport/33131-livre-blanc-sur-la-defense-et-la-securite-nationale-2013
[9] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id#JORFSCTA000028338829
[10] Des années de travail seront nécessaires aux agents de l'ANSSI pour la mise en œuvre de ces dispositions législatives, en collaboration et transparence avec les opérateurs.
[11] Pour détecter une attaque informatique menée par les Martiens, il ne faut pas utiliser des équipements vendus par les Martiens…
[12] https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/

[13] https://www.gouvernement.fr/strategie-nationale-pour-la-securite-du-numerique-un-bon-equilibre-entre-prise-en-compte-de-la-3075
[14] Cf. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/
https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[15] L'espionnage, qui n'est pris en compte dans le droit international que dans des circonstances particulières n'est pas comprise dans ces pratiques offensives.
[16] "Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés" Karine BANNELIER, Théodore CHRISTAKIS, 2017
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2957795
[17] http://www.sgdsn.gouv.fr/evenement/conference-internationale-je-suis-internet/
[18] https://www.sciencesetavenir.fr/politique/video-quand-cedric-villani-et-emmanuel-macron-parlent-de-science-pour-sciences-et-avenir_112884
[19] https://www.elysee.fr/emmanuel-macron/2017/07/13/discours-d-emmanuel-macron-a-l-hotel-de-brienne
[20] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
[21] https://www.economica.fr/livre-strategie-nationale-de-la-cyberdefense-sgdsn,fr,4,9782717869941.cfm
[22] Michael PORTER, "L'Avantage concurrentiel des nations", Dunod, 1993
[23] N. WIENER, I Am a Mathematician, Cambridge (Ma), MIT Press, 1956, p. 327.
[24] François FILLON, ministre des Technologies de l'information et de La Poste dans le premier gouvernement d'Alain JUPPE en 1995.
[25] Indice relatif à l'économie et à la société numériques (DESI, France, 2019). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59990
[26] Jacques-Bénigne BOSSUET. Oraison funèbre de Marie-Thérèse d'Autriche, reine de France.
[27] https://www.senat.fr/rapports-senateur/arthuis_jean83011j1992.html
[28] https://www.weforum.org/agenda/2020/07/largest-global-economies-1992-2008-2024
[29] Maximes et pensées de Napoléon". Honoré DE BALZAC
[30] Par exemple les idées synthétisées par Syntec numérique en mai dernier https://syntec-numerique.fr/actu-informatique/75-propositions-secteur-numerique-pour-relance-economique
[31] Rapport des députés Marietta KARAMANLI, Christine HENNION et Jean-Michel MIS http://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information
[32] Rapport du député en mission Luc BELOT (2017) https://www.vie-publique.fr/rapport/36551-de-la-smart-city-au-territoire-dintelligences-lavenir-de-la-smart
[33] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027343503&categorieLien=id
[34] https://www.lemonde.fr/economie/article/2020/06/13/l-allemagne-veut-devenir-le-pays-de-l-hydrogene_6042722_3234.html
[35] https://pariscall.international/fr/
[36] Comme celle du techaccord initié par Microsoft https://cybertechaccord.org
[37] https://www.congress.gov/bill/116th-congress/senate-bill/3398/text
[38] https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue
[39] 31 milliards pour les achats de l'Etat, 16 milliards pour les achats de défense et de sécurité, 23 milliards pour les hôpitaux publics, 20 milliards pour les collectivités territoriales.
[40] Samira BOUSSETTA, "Appuyons la transformation sur l'achat public !"in acteurs publics n°141, septembre 2019
[41] Notamment à l'occasion du discours annuel prononcé lors de la conférence des ambassadeurs.
[42] Céline PINA, "Nous nous vivions puissance, nous nous sommes réveillés nus… et barbares." in Front Populaire, n°1, Juin 2020.
[43] Dans l'actuel code de la défense, il n'est pas question de riposte face à une attaque informatique mais de caractérisation de la menace et de neutralisation de ses effets.
https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html
[44] http://www.assemblee-nationale.fr/dyn/15/textes/l15b2778_proposition-loi
[45] Père Dominique DUBARLE, à propos de la publication de "Cybernetics, or control and communication in the animal and the machine," de Norbert WIENER, journal Le Monde, 28 décembre 1948.

La conformité au RGPD est devenue une évidence, au service des collectivités et des citoyens

FRANÇOIS COUPEZ
Avocat associé
Implid Legal

Il ne se passe pas quelques semaines, même pendant la période du mois d'août, sans que l'on ne parle d'une nouvelle décision d'un régulateur ou d'une cour de justice concernant l'application des règles en matière de protection des données personnelles (notamment le Règlement europeén n°2016/679, dit « reg̀lement geńeŕal sur la protection des donneés » ou encore RGPD) :

- invalidation du Privacy Shield par la Cour de Justice de l'Union Européenne (prévisible, mais trop longtemps attendue) ;
- mise en cause plus largement du régime juridique de protection des données personnelles aux USA rendant problématique l'encadrement juridique de ces données entre l'Espace Economique Européen et les USA (idem) ;
- mise en cause par la CNIL de l'utilisation du reCAPTCHA de Google par les sites internet et application (elle aussi prévisible et trop longtemps attendue) - cf. décision MED-2020-015 de la CNIL d'audit de l'application StopCOVID ;
- ou encore mises en demeure par la CNIL en ce mois d'août 2020 de quatre communes du fait de la collecte et du traitement de photographies des véhicules, notamment en vue rapprochée de la plaque d'immatriculation, pour l'exercice du pouvoir de police par les communes (en lien avec la tranquillité publique ou la salubrité publique). La CNIL rappelle en effet que le traitement de ces photographies n'est pas autorisé en l'état actuel de la réglementation (notamment l'arrêté du 14 avril 2009 et son article 6).

Pourtant, tout comme la cybersécurité, la conformité RGPD n'est pas toujours prise au sérieux dans l'ensemble de ses composantes.

La réglementation française en matière de protection des données a beau avoir fêté ses 42 printemps et s'être renforcée au fil des années, notamment avec le RGPD depuis le 25 mai 2018, trop souvent encore, certaines collectivités en restent à la nomination d'un DPO mutualisé disposant de peu de moyens et sans que la gestion des données soit considérée comme devant réordonner la façon même dont la « relation citoyen » doit être fondée. L'e-administration (simplification administrative) est pourtant un axe important de modernisation de l'action publique et répond à une demande effective des citoyens dans le cadre de l'e-démocratie, le respect des règles de protection des données à caractère personnel par les collectivités étant un facteur de transparence et de confiance à l'égard des usagers, mais aussi du personnel qui y travaille.

Au-delà d'un renforcement de la sécurité des systèmes d'information, pierre angulaire de la conformité en matière de protection des données personnelles, la conformité en la matière suppose également l'adoption de mesures organisationnelles, sans oublier les nécessaires analyses juridiques préalables. Ainsi, le fait que la fiche « l'impact du RGPD sur le droit de la commande publique » émanant de la Direction des affaires juridiques (DAJ) du ministère de l'économie[1] ne mentionne que l'hypothèse d'un fournisseur forcément « sous-traitant » au sens du RGPD est révélateur du travail qui reste encore à parcourir sur le sujet. De plus en plus, nous constatons en pratique dans les dossiers dans lesquels nous intervenons que les qualifications essentielles en matière de traitement de données personnelles (quel est l'un des six fondements légaux utilisés pour le traitement ? Qui est responsable de traitement, sous-traitant, responsable conjoint, responsable disjoint, tiers autorisé ?) n'ont pas été analysées et que les mises en conformité effectuées par la suite s'avèrent en conséquence à reprendre en quasi-totalité.

Nous nous permettrons donc ici de rappeler que seule une approche intégrant les trois piliers fondamentaux (organisationnel, technique et juridique) met en œuvre de façon efficace les principes découlant du RGPD, étant entendu que la plupart des collectivités territoriales ont déjà un acquis sur le sujet sur

lequel s'appuyer et peuvent souvent recourir à des solutions mutualisées et/ou éprouvées :

- cartographie des traitements existants ;
- identification des données traitées ;
- identification des acteurs de l'écosystème traitant les données (sous-traitant, fournisseurs, etc.), des lieux à partir desquels les données sont accédées et qualification de leur rôle au regard du traitement des données personnelles ;
- encadrement juridique approprié des relations économiques avec ceux-ci ;
- construction et sécurisation de traitements orientés « *privacy by design* » ;
- détermination des fondements légaux permettant leur traitement ;
- création/mise à jour d'un registre des traitements, d'un registre des sous-traitants et d'un registre des violations de données à caractère personnel ;
- transparence des informations à communiquer ;
- documentation de l'ensemble de la chaîne de traitement et des décisions prises ;
- nomination obligatoire de Délégués à la Protection des Données (DPD/DPO) pour les entités du secteur public ;
- réalisation d'études d'impact sur la vie privée dans les cas où les traitements ont les conséquences les plus graves pour les personnes ;
- création des processus de notification des violations de données personnelles ;
- etc.

Cet engagement dans un process de conformité au RGPD nécessite ainsi une dynamique portée par les élus, un chef de projet référent, un travail en collaboration avec l'ensemble des services, parfois l'accompagnement d'experts extérieurs de confiance, et un engagement sur le long terme afin de faire de cette réglementation un véritable atout pour les collectivités. Car à la fin, tout le monde, citoyens et collectivités territoriales, doit sortir gagnant de cette conformité !

Parution le 28 août 2020

[1] https://www.economie.gouv.fr/files/files/directions_services/daj/marches_publics/conseil_acheteurs/fiches-techniques/preparation-procedure/impact_RGPD_droit_Commande_Publique.pdf

Convergence sûreté et cybersécurité : du serpent de mer à l'évidence

JEROME SAIZ
Président-fondateur
OPFOR Intelligence

La question de la convergence entre sûreté et cybersécurité est l'un des serpents de mer préférés de la profession (à la différence près qu'il existe quand même quelques observations confirmées de la bête !).

Pourquoi un sujet qui ne devrait pas faire débat - aligner deux rôles ayant le même objectif au service de l'entreprise - fait-il couler autant d'encre depuis si longtemps ? Et, surtout, pourquoi est-il désormais plus d'actualité que jamais ?

L'on peut trouver un début de réponse dans l'origine même de ces deux fonctions. La prévention-sûreté existe depuis que les affaires existent. Son objectif est de protéger l'activité contre la malveillance. L'informatique, quant à elle, est évidemment arrivée bien plus tard, et par la petite porte. À ce titre, il est fascinant d'explorer le site de l'INA à la recherche de reportages illustrant l'arrivée de l'informatique dans l'entreprise. C'est généralement le fait de patrons visionnaires et passionnés, et l'outil est évidemment d'abord aux mains d'experts. À ce stade, l'informatique est donc une affaire de spécialistes, son apport à l'activité de l'entreprise est minime et la malveillance à son encontre quasi inexistante. Il n'y a donc pas vraiment de quoi impliquer la sûreté, qui a déjà fort à faire et dont le personnel n'est, comme beaucoup à cette époque, pas franchement passionné par le sujet.

Mais l'informatique va progressivement s'ouvrir au monde à travers les réseaux de télécommunication et prendre une place grandissante dans les affaires. Ainsi, lorsque la malveillance informatique devient une réalité,

qui peut-on aller chercher pour lutter contre ce nouveau phénomène ? Certainement pas le service de sûreté, qui n'a jamais traité du sujet ! C'est ainsi que l'on a tout simplement chargé les experts en place d'assurer eux-mêmes la protection de l'outil, créant au fil du temps un nouveau métier dans l'entreprise : celui de la « sécurité informatique » d'abord puis de la « sécurité des systèmes d'information » ensuite.

La distinction entre le service de sûreté et celui de la protection des systèmes d'information n'est donc pas née d'une stratégie mûrement réfléchie ni d'une doctrine finement travaillée. Elle est plutôt le fruit d'une évolution par défaut qui n'a jamais été remise en cause.

Remise en cause du statuquo

Certes, ces dernières années des organisations ont bien rapproché avec plus ou moins de succès leurs services de sécurité informatique et de sûreté. Mais elles sont encore l'exception plutôt que la norme, probablement car il s'agit d'une initiative structurante et très politique.

Car un tel rapprochement se fait rarement entre ces deux seules entités. Il s'agit plutôt d'associer cybersécurité et sûreté au sein d'une Direction sécurité Groupe qui intègrera également la gestion du risque de manière transverse, souvent l'Intelligence Économique, et qui leur apportera en prime un soutien juridique et parfois même en communication de crise.

Mais pourquoi se donner autant de mal alors que l'entreprise fonctionne très bien sans tout cela ? Parce qu'aujourd'hui l'irruption de la transformation numérique, des objets connectés, de l'Internet des Objets (IoT), de l'informatique industrielle et du « *edge computing* » (informatique de bordure) change radicalement les scénarios de risque et oblige à penser en termes de stratégie globale plutôt qu'en silos sécuritaires.

Complémentarité des attaques

L'un des premiers arguments techniques pour le rapprochement des deux fonctions (ou a minima leur dialogue régulier) tient au fait qu'une attaque cyber peut permettre ou faciliter une attaque physique et à l'inverse, un

accès physique au système d'information facilite grandement sa compromission. Dans les deux cas, le scénario de menace principal est l'ingérence économique.

Dans un sens, la numérisation permanente des outils de la sûreté (enregistreurs vidéo visibles sur le réseau de l'entreprise, caméras désormais connectées en IP, systèmes de contrôle d'accès reposant sur des serveurs et des logiciels aussi faillibles que les autres) fait qu'en confier l'exploitation à un service de sûreté ne disposant d'aucune sensibilisation au risque numérique peut conduire à des pratiques à risque, ainsi qu'à exposer inutilement des systèmes critiques qui n'auraient pas été identifiés comme tels (d'autant que les outils traditionnels de la cybersécurité ne sont pas toujours adaptés à ces outils ou leurs protocoles).

Dans l'autre sens, les experts de la cybersécurité, qui n'ont que peu de notions de protection physique, ignorent par exemple la résistance d'une ventouse électrique ou les moyens de la forcer et ne conçoivent souvent la menace que sous une forme virtuelle, n'adresseront eux aussi pas l'ensemble des risques.

Miniaturisation

En outre, les incroyables progrès réalisés dans la miniaturisation des systèmes ouvrent de nouveaux risques au croisement de la cybersécurité et de la sûreté. Ainsi un externe à l'entreprise peut parfaitement dissimuler sur lui un système de piratage complet (tel que le LAN Turtle ou un équivalent conçu sur la base d'une carte Arduino ou d'un RaspberryPi).

Il lui suffit alors de laisser un tel outil, de la taille d'une boîte d'allumettes, alimenté et connecté au réseau interne pour ouvrir une brèche dans le système d'information. Si le personnel d'entretien ou de sûreté n'est pas sensibilisé à reconnaître ces outils derrière un copieur ou au fond d'un sac lors d'une inspection visuelle, ils peuvent contribuer à matérialiser un risque majeur pour l'entreprise.

Bien sûr, tout ceci peut se régler : a minima par un dialogue entre les deux directions et des sensibilisations communes, mais de préférence dans le

cadre d'une stratégie de protection globale qui associera la direction des risques en tant que « chef de projet » transverse capable de consolider les différentes approches (les méthodes d'analyse de risques informatiques intègrent, bien entendu, déjà le risque d'accès physique aux actifs).

Le sens de l'histoire

À vrai dire, tous les arguments avancés jusqu'à présent sont connus depuis longtemps et devraient, à eux seuls, motiver l'étude d'un dialogue renforcé entre la sûreté et la cybersécurité. Mais les évolutions les plus récentes du numérique montrent qu'une telle convergence s'inscrit désormais dans le sens de l'histoire. Pour ne citer que les points les plus saillants, l'ouverture de l'informatique industrielle multiplie les points d'entrées « cyber » sur le terrain, dans des caissons, des boîtiers, des armoires ou des sites isolés. Tous ne peuvent être protégés de manière équivalente, et il est donc impératif de leur appliquer une analyse de risque cohérente croisant critères de cybersécurité et de sûreté. Au-delà de l'horizon, la tendance du « *edge computing* », qui vise à décentraliser massivement les traitements de données, signifie là aussi que de plus en plus d'actifs « cyber » critiques seront confiés à des sites distants, et devront donc bénéficier d'une protection physique à la hauteur des informations qu'ils traitent.

Plus envahissant encore : l'irruption d'une multitude d'objets connectés (IoT) expose également à des risques inédits, notamment liés à la capacité de l'attaquant à pouvoir détériorer physiquement à distance un équipement installé au sein des locaux (et en particulier en l'échauffant, ce qui pourrait donner à réfléchir aux spécialistes incendie)

Enfin, et bien que ce ne soit pas tout à fait l'objet de ce billet, les plus inquiets (ou prévoyants) imagineront probablement aussi des scénarios de risque autour de la voiture autonome des cadres dirigeants…

Dans tous les cas, il devient difficile de continuer à réfuter l'existence du serpent de mer…

Parution le 4 septembre 2020

Sécurité du numérique : la réserve numérique de la gendarmerie au cœur de l'action « répondre présent pour la population, par le gendarme »

FLORENCE ESSELIN
Conseiller expert en numérique et cybersécurité
au cabinet du directeur général de la Gendarmerie nationale

L'animation de la « réserve numérique » par la mission numérique de la Gendarmerie nationale a démontré qu'elle est un outil agile, facilitant et même accélérant l'adaptation de la gendarmerie aux évolutions du numérique, dès lors qu'elle est pilotée dans une logique de coordination des projets et de mutualisation des besoins des différents services, centraux comme déconcentrés. Ainsi, la réserve numérique de la gendarmerie a toute sa place au cœur de l'action « répondre présent pour la population, par le gendarme » est d'ailleurs la devise du plan de transformation Gend20.24 initié par le GAR Rodriguez en décembre 2019, en cohérence avec les réformes entreprises par ses prédécesseurs, les généraux Favier et Lizurey.

La réserve de la gendarmerie au cœur de l'action pour la citoyenneté

À l'invitation de la ministre déléguée à la citoyenneté, Marlène Schiappa, lors de la présentation de sa feuille de route le 31 août dernier[1], le général d'armée Christian Rodriguez, directeur général de la Gendarmerie nationale, a pu rappeler la contribution de ses services à la cohésion nationale, et plus particulièrement à quel point la réserve de la Gendarmerie nationale – 30 000 réservistes, 42 % des effectifs de la garde nationale – incarne l'engagement citoyen.

« Être réserviste, c'est être deux fois citoyens » : citant Sir Winston Churchill, le GAR Rodriguez a mis en lumière la richesse de la réserve de la gendarmerie, véritable miroir de la diversité de la société française.
Près des trois quarts des réservistes sont issus de la société civile, des anciens

de l'arme et des actifs et retraités des services publics constituant le « gros » quart restant. On y retrouve à peu près toutes les compétences et tous les métiers - une aubaine pour la gendarmerie qui peut ainsi quotidiennement compléter ses effectifs opérationnels par les compétences venant à lui manquer. L'engagement des femmes dans cette institution militaire y est élevé (> 20 %), de même que la proportion de jeunes adultes de moins de trente ans (un tiers des réservistes opérationnels).

Évoquant le sens de l'engagement des étudiants qui quotidiennement renforcent ses rangs, le GAR Rodriguez a témoigné de leur recherche de valeurs partagées, des valeurs républicaines. « Une sorte de respiration » est apportée par ces jeunes engagés volontaires dans la réserve opérationnelle, dont on peut louer le civisme[2]. L'ancrage territorial des réserves, le fait que les réservistes puissent travailler près de chez eux, est un facteur d'attractivité supplémentaire, et une richesse pour la gendarmerie qui a la volonté d'être au plus près de la population. « Répondre présent pour la population, par le gendarme » est d'ailleurs la devise du « plan de transformation Gend20.24 » initié par le GAR Rodriguez en décembre 2019, en cohérence avec les réformes entreprises précédemment.

Le dispositif des « cadets de la gendarmerie » accueille les filles et les garçons de moins de 17 ans alors trop jeunes pour être réservistes, mais souhaitant s'engager comme leurs aînés pour être au contact des gens dans des missions ayant du sens ; ce dispositif constitue le socle sur lequel la gendarmerie construit actuellement sa contribution au service national universel. Ce dispositif est l'un des moyens retenus par la ministre déléguée à la citoyenneté, pour développer les possibilités d'engagement citoyen dès le plus jeune âge - c'est l'un de ses objectifs relatifs aux questions de laïcité, de fraternité, d'intégration citoyenne et de cohésion nationale, les axes majeurs de son action étant : « faire vivre les valeurs de la République » et « incarner la République qui protège ».

C'est ainsi que « la réserve de la gendarmerie est au cœur de l'action pour la citoyenneté »[3].

Le GAR Rodriguez n'a pas manqué de souligner également l'apport des réservistes citoyens de la gendarmerie, moins nombreux (un peu plus d'un

millier), au statut de bénévoles du service public et non de militaires. Dotés de compétences rares, ces réservistes contribuent notamment à la sélection des hauts potentiels de la gendarmerie et à « challenger » l'image de l'institution.

La mobilisation de la réserve gendarmerie dans la crise

La réserve de la gendarmerie a démontré plusieurs fois sa capacité de mobilisation et son efficacité dans la gestion des crises qui secouent notre pays. En 2017, la gendarmerie a déployé des moyens conséquents pour porter assistance à la population de Saint-Martin et assurer sa sécurité ; près de 150 réservistes volontaires y furent projetés, mettant entre parenthèses pendant plusieurs semaines voire plusieurs mois leur activité professionnelle et leur vie de famille.

Un même élan de fraternité et de solidarité a animé les milliers de réservistes opérationnels et citoyens pendant la crise COVID-19, en renfort des initiatives locales et nationales des gendarmes qui ont spontanément « répondu présent » pour soutenir la population en détresse, tout en assurant prioritairement le contrôle des mesures sanitaires visant à freiner la propagation du virus. Ainsi la sécurisation des bureaux de poste sensibles pendant le confinement et le début du dé-confinement s'est appuyée sur plusieurs centaines de réservistes.

L'impatience des réservistes à être employés dès le début de la crise a nécessité la diffusion d'un message du général de division Olivier Kim, commandant des réserves gendarmerie (CRG), rappelant, en écho au GAR Rodriguez, « qu'on n'engage pas en premier échelon, dans une crise, sa réserve, sinon, ce n'est plus une réserve ».

Sur le front du cyberespace, le confinement provoquant les conditions d'une hausse de la cybercriminalité, la gendarmerie a conduit une manœuvre pour éviter une sur-crise cyber, mobilisant à la fois ses services d'ingénierie de ses systèmes d'information, les référents sûreté et référents sécurité économique et protection des entreprises, les sections opérationnelles de lutte contre la cybercriminalité (SOLC), les groupes cyber des sections de recherche (SR), le centre de lutte contre les cybercriminalités (C3N), etc.

Leur mission : PRÉVENIR et SE PROTÉGER, RENSEIGNER et INFORMER, COMMUNIQUER, SE PROJETER et ENQUÊTER, le tout dans une logique de partenariat avec le monde associatif et professionnel et en coordination avec l'ensemble des acteurs ministériels (notamment DGPN et secrétariat général) et interministériels, au niveau central et territorial.

Les directives opérationnelles cyber précisaient le soutien attendu des personnels confinés, en télétravail et des réservistes numériques dans les démarches de prévention auprès des collectivités, des établissements publics et des entreprises des secteurs particulièrement menacés. Ainsi, réservistes opérationnels et citoyens « numériques » purent participer à distance aux travaux de certaines SR et aux campagnes de sensibilisation par téléphone, courrier électronique et webinaires organisées à l'échelon départemental ou régional. Certains ont été très prompts à proposer des supports de sensibilisation pour les entreprises et les salariés en télétravail, qui ont été diffusés par le SIRPA-G.

Les réservistes « numériques »

Le réseau des réservistes « numériques » est constitué de près de deux cents réservistes opérationnels et réservistes citoyens de la Gendarmerie nationale, de métiers divers (magistrats, avocats, enseignants, chercheurs, anciens gendarmes, chefs d'entreprise, directeurs sécurité, responsables sécurité des systèmes d'information, ingénieurs conseils, architectes informatique, responsables réseaux, webmestres, etc.) des deux sexes et de tous âges. Ils ont en commun un civisme incontestable (certains étant membres de plusieurs associations, élus locaux ou territoriaux), un fort intérêt pour le numérique et la sécurité du numérique et des compétences reconnues dans ce domaine. Réunis en 2017 par le chef de la mission numérique de la Gendarmerie nationale (MNGN), le Colonel Eric Freyssinet, avec l'appui du CRG, ils forment la réserve numérique qui inclut les membres de la réserve cyber, ces deux dernières étant animées en région par un officier de gendarmerie.

Articulation avec la réserve « cyber »

La réserve cyber, qui dispose d'un vivier plus resserré que la réserve numérique, est l'héritière de la réserve citoyenne de cyberdéfense créée

conjointement en 2012 par les armées et la gendarmerie, dans une perspective interministérielle. Ses missions et son organisation ont été précisées par Guillaume Poupard, directeur général de l'ANSSI, le général Olivier Bonnet de Paillerets commandant alors le COMCYBER, et le COL Freyssinet, représentant le directeur général de la gendarmerie, lors du séminaire national des réservistes cyber en septembre 2018 à la direction générale de la Gendarmerie nationale, organisé par la MNGN avec l'actif soutien du COMCYBER et de l'ANSSI. L'idée ancienne de constituer une réserve mobilisable et projetable en cas de crise auprès des organismes d'importance vitale attaqués, avait perdu de sa pertinence face aux conditions nécessaires à sa mise en œuvre. La nouvelle orientation stratégique était alors de faire de la réserve cyber une réserve d'emploi, mobilisée régulièrement pour les besoins des institutions réunies dans une gouvernance tripartite bénéficiant, pour l'animation déconcentrée des activités de la réserve cyber, du maillage territorial de la gendarmerie.

Les réservistes « cyber » de la gendarmerie interviennent ainsi en appui des gendarmes dans leurs diverses actions de prévention des cybermenaces. D'autres initiatives lancées bien avant la création de la réserve cyber, tel le forum annuel du Rhin supérieur sur les cybermenaces (organisé par la gendarmerie d'Alsace et les officiers de la réserve citoyenne réunis au sein de l'association Ad Honores réseau Alsace), perdurent dans ce cadre.

La participation de la réserve numérique à la gestion de crises

Pour autant, la crise COVID-19 a permis d'approfondir encore les besoins et les conditions de renfort des réservistes dans un contexte de crise numérique d'ampleur nationale ou ciblant la gendarmerie, ou de crise de toute nature comportant un volet numérique.

Ainsi la Gendarmerie nationale prévoit dans son dispositif de gestion de crises numériques, la capacité de mobiliser des réservistes « numériques » - ceux disposant d'une expertise en sécurité des systèmes d'information, mais aussi tous ceux qui peuvent contribuer à l'analyse de risques, à l'anticipation, à la mise en œuvre rapide d'outils s'avérant utiles à la manœuvre, à la capitalisation d'expériences, à la communication, etc.

La réserve numérique au cœur de la sécurité des nouvelles frontières

Au-delà de ce contexte particulier de crise, les réservistes comme tous les autres gendarmes au sens large, sont au cœur de l'exécution de la mission de la gendarmerie, et au cœur de la transformation de la « maison ». Le plan de transformation « Gend20.24 » s'articule autour de quatre missions prioritaires, dont l'une est la sécurité des « nouvelles frontières » (cyberespace, monde numérique, données et algorithmes, bio sécurité et protection de l'environnement).

Cette transformation repose sur quatre piliers :
- une offre de protection sur mesure avec l'ambition de mieux protéger la population ;
- une communauté de la transformation permettant de mieux progresser dans le travail quotidien, de donner du sens à l'action, d'innover collectivement, d'améliorer la gestion des carrières et les conditions de vie et de travail ;
- l'innovation technologique pour accompagner les gendarmes dans l'exercice de leur métier avec des outils adaptés à leurs besoins ;
- la recherche de nouvelles marges de manœuvre opérationnelles, au moyen notamment d'une gouvernance agile, d'une véritable stratégie de la donnée et de la recherche de nouvelles ressources financières.

La sécurité « dès la conception » : un principe constitutif de la réserve numérique

Associer des réservistes ayant des compétences complémentaires sur l'ensemble du périmètre des « nouvelles frontières numériques » fait donc sens également dans ce contexte. « La sécurité dès la conception » est une réelle nécessité pour une transformation numérique clairvoyante.
Dans la logique de ses missions exploratoires et stratégiques, la MNGN a animé le réseau des réservistes numériques de la gendarmerie en testant des approches innovantes, telles que :
- l'intervention de réservistes à toutes les étapes de la conception, du développement et de l'homologation de sécurité d'un logiciel, avec l'API « @Gend&Vous », pour permettre la prise de rendez-vous en ligne avec la

brigade la plus proche pour certaines démarches, depuis le site www.lannuaire.service-public.fr ; à cette occasion la MNGN a expérimenté dès 2018 la nouvelle méthode « EBIOS Risk Manager » pour les premières étapes de l'analyse des risques avec un petit groupe de réservistes en audioconférence, ainsi que la constitution d'une équipe d'audit SSI interne pour l'analyse du code source suivant les recommandations de l'ANSSI ;
- l'accompagnement des gendarmes promoteurs de projets numériques innovants pour l'intégration de la sécurité dès la conception.

Le séminaire des réservistes numériques en l'école des officiers de la Gendarmerie nationale, en septembre 2019, a confirmé la pertinence et la richesse, tant pour la gendarmerie que pour les réservistes eux-mêmes, de faire travailler ensemble des réservistes opérationnels et des réservistes citoyens.

Cette approche inhabituelle faisant fi des grades pour mobiliser les compétences personnelles sur des missions communes, permet à la gendarmerie de bénéficier ponctuellement de compétences rares déjà initiées à son contexte particulier.

Pour leur part, les jeunes experts du numérique engagés dans la réserve opérationnelle par civisme, par envie de contribuer à l'ordre public dans un cadre militaire sans s'y engager à temps plein ni sacrifier leur métier, s'accordent parfaitement avec les réservistes opérationnels galonnés et les réservistes citoyens, qui sont généralement dans une logique de transmission de leur expertise et d'enseignement de leur longue expérience ; cette cohésion génère pour les uns et les autres des opportunités exceptionnelles.

L'animation de la « réserve numérique » par la MNGN – laquelle a désormais rejoint le service de la transformation (ST), au sein du département de la prospective et de l'innovation - s'appuyant sur la proximité des coordinateurs de la réserve cyber en région et sur ses contacts avec l'ensemble des services de la gendarmerie intéressés par son renfort, a permis de tisser des liens plus collectifs et donc plus pérennes avec les réservistes.

Cette animation a démontré qu'elle est un outil agile, facilitant et même accélérant l'adaptation de la gendarmerie aux évolutions du numérique, dès

lors qu'elle est pilotée dans une logique de coordination des projets et de mutualisation des besoins des différents services, centraux comme déconcentrés.

Ainsi, la réserve numérique de la gendarmerie a toute sa place au cœur de l'action « répondre présent pour la population, par le gendarme » dans les nouveaux défis numériques.

Parution le 11 septembre 2020

[1] https://www.facebook.com/Interieur.Gouv/videos/788912291884789/?vh=e&extid=iukCtEajmn43vXsV&d=n
[2] Civisme : Zèle du citoyen pour les intérêts de son pays. Pendant la Révolution française, on délivrait des certificats de civisme. (Dictionnaire de l'Académie française).
[3] https://www.gendinfo.fr/actualites/2020/la-reserve-de-la-gendarmerie-au-caeur-de-l-action-pour-la-citoyennete

Former, informer, sensibiliser pour lutter contre les cyberattaques

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

La cybersécurité est une discipline qui s'apprend, qui se maintient, mais aussi qui se vit et se partage. Former les experts dans l'enseignement supérieur, puis en entreprise, maintenir leur compétence, sensibiliser l'ensemble des acteurs d'une organisation sont des conditions nécessaires, mais pas suffisantes pour diminuer les risques. Le reste est un travail quotidien pour ces experts et aussi pour l'ensemble du personnel.

Maillons faibles et piliers forts

On a coutume d'affirmer que le maillon faible de la chaîne de sécurité, sur laquelle repose la force de l'architecture globale qui protège une organisation visée par des cyberattaques[1], est situé entre votre chaise et votre clavier.

Pour les utilisateurs, c'est souvent le cas, mais ce n'est pas une fatalité si ces maillons font l'objet d'une sensibilisation aux dangers du cyberespace, avec l'appui de la direction générale. **Les experts en sécurité du numérique**, piliers de la chaîne de sécurité, doivent être correctement formés durant leur enseignement initial et entretenir leur compétence. Ils doivent connaître les attaques les plus récentes, les faiblesses de leur système d'information et aussi les métiers de leur organisation, car le besoin en sécurité d'un constructeur aéronautique n'est pas identique à celui d'une banque ou d'un site marchand. Les experts doivent évaluer le risque qui pèse sur l'information sensible de leur organisation, et le maintenir à un niveau connu, maîtrisé et « acceptable ».

Les experts, des piliers qui doivent être et rester forts

Les experts en cybersécurité doivent placer les contre-mesures indispensables, dans l'état de l'art de la cybersécurité, pour que le système d'information de leur organisation, surtout là où se trouve l'Information sensible, soit protégé contre les fuites, les destructions ou pire les compromissions. Et ces contre-mesures doivent évoluer en parallèle aux attaques de plus en plus sophistiquées, et tenir compte de la psychologie des attaquants. Cartographier l'Information de l'organisation est un préalable indispensable pour que les experts sachent où se trouve l'Information sensible qui devra demeurer disponible, intègre, confidentielle et traçable (le fameux DICT[2] de la cybersécurité). **Former ces experts par une formation initiale** est le rôle de l'enseignement supérieur et des organismes privés. Trouver ces experts encore trop rares sur le marché, les embaucher et les retenir sont des problèmes que les organisations, grandes ou petites doivent résoudre. Ces experts doivent entretenir les connaissances acquises lors de leur formation initiale par une veille continue, appliquée aux métiers de l'organisation.

La formation des experts dans l'enseignement supérieur

Des écoles d'ingénieurs spécialisées dans l'enseignement des métiers du numérique, et aussi celles plus généralistes dans leur enseignement initial, mais qui présentent dans leur cursus une option en cybersécurité, des universités, des instituts, des IUT/DUT proposent des formations à la cybersécurité sur plusieurs semaines ou plusieurs mois. Au niveau BAC+5, les apprenants peuvent se diriger vers des masters en cybersécurité qui peuvent conduire à des activités de recherche ou des mastères spécialisés et MBA plus adaptés, après un stage professionnel, aux besoins immédiats des entreprises.

Les métiers de la sécurité du numérique sont très divers. Les formations initiales se différencient par la finalité de leurs spécialisations. Contrairement à certaines idées encore trop bien établies, la sécurité du numérique n'est pas une discipline purement technique. Il est aussi important de préciser que ces métiers peuvent être exercés par des hommes comme par des femmes encore trop peu nombreuses dans cet écosystème qui compte seulement 20 % de femmes, aujourd'hui. Les matières juridiques, l'intelligence économique, la

veille technologique, l'enseignement, l'encadrement de projets et d'équipes entrent également dans les métiers de la cybersécurité.

Vers les métiers de la cybersécurité

Côté technique, si on vise une activité de développeur, les langages Python, Java, voire des langages plus proches du matériel, doivent être maîtrisés. Si on vise une activité de chasseur de failles (Bug Bounty) dans les logiciels ou de testeur de la solidité d'une architecture numérique (PenTest), les principes de la sécurité par conception et par défaut doivent être bien connus. Le développement d'algorithmes de chiffrement vous tente ? C'est une question de mathématiques, et bientôt aussi de physique quantique. Il y a les métiers d'architecte sécurité pour lesquels il faut connaître les éléments de base comme l'authentification forte, les coupe-feux, les réseaux privés virtuels, la cryptologie et bien d'autres outils. Mais empiler ces éléments ne suffit pas à constituer une architecture moderne de sécurité. Il y a les édifices à maîtriser comme l'IAM, le PCA, le DLP, le SIEM, le SOC[3].

Il y a également les exercices de simulation de cyberattaques menés en interne ou chez un formateur : une équipe rouge attaque et une équipe bleue défend. Cela permet de connaître les tactiques et stratégies d'un attaquant, et de se connaître soi-même. Comme l'a dit Sun Tzu, il y a 2 500 ans, dans l'art de la guerre : Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.

Côté organisationnel, on trouve le juridique, comme les lois Godfrain qui sanctionnent l'intrusion et le maintien dans un système de traitement automatisé de données sans y être autorisé, et la perturbation de son fonctionnement. Il y a des règlements, comme le RGPD, des directives comme NIS, des normes comme celles de la famille des ISO27000 et des méthodes, comme eBios et Mehari. Il y a l'élaboration de contrats de sous-traitance, la création d'une charte de sécurité, et aussi la gestion de projets, parfois à gros budget, et la gestion d'équipes parfois avec beaucoup de ressources à animer. En effet, l'évolution d'un expert sécurité peut lui ouvrir des voies royales proches de la direction générale.

Le label SecNumEdu, une garantie, mais pas indispensable

Certaines formations initiales de l'enseignement supérieur, pour les futurs experts en sécurité du numérique, peuvent prétendre au label SecNumEdu de l'ANSSI, décerné après étude d'un dossier assez complexe à constituer. Ce label est valable pour une durée de trois ans, à l'issue desquels une nouvelle demande de labellisation doit être soumise. Ces formations labellisées SecNumEdu sont référencées sur le site de l'ANSSI.

Beaucoup de formations à la cybersécurité qui n'ont pas ce label peuvent néanmoins être excellentes, mais n'ont pas fait l'objet d'une demande de labellisation ou ne cadrent pas exactement à la charte et aux critères définis par l'ANSSI.

L'enseignement supérieur couvre-t-il les besoins du pays ?

Malgré des progrès dus à la prise de conscience des dangers du cyberespace, suite à la multiplication des attaques et à leurs conséquences désastreuses et bien que le sujet soit devenu porteur, on ne trouve pas assez d'experts, immédiatement compétents, pour couvrir les besoins croissants des organisations. Les étudiantes et les étudiants hésitent-ils à se lancer dans cette discipline par manque de connaissances sur l'attrait des métiers de la cybersécurité ? Il y a certes un effort de visibilité à réaliser pour rendre ces enseignements et leurs débouchés plus visibles. Les universités restent souvent peu centrées sur le côté pratique des métiers. Les MBA et les mastères professionnels en temps partiel, une semaine par mois, ou deux jours par semaine en présentiel, et le reste du temps dans une organisation, avec un stage en entreprise donnant lieu à une soutenance, me semblent être une bonne formule.

Et l'enseignement supérieur dans la cybersécurité ne doit pas négliger les aspects non techniques comme le juridique, les normes et les standards, les règlements et directives, et la gestion de crise.

Entretenir son expertise

Une veille technologique dans cette discipline en constante évolution est indispensable. Les lettres d'information, les réseaux sociaux professionnels et les salons comme le FIC, à Lille chaque année en janvier, sont de bons moyens d'entretenir sa compétence. Les magazines comme Global Security Mag et Mag Securs apportent un éclairage et des avis d'experts. S'impliquer dans des associations comme le CyberCercle, le CESIN, le CLUSIF, le CEFCYS, l'ARCSI, permet d'entretenir ses compétences par l'apport de l'extérieur, et de partager les siennes. Dans la cybersécurité, vous ne serez jamais seuls si vous saisissez les occasions de côtoyer vos pairs.

Informer : la nécessaire sensibilisation de tous les acteurs

La sécurité de l'Information est l'affaire de tous les employés d'une organisation, et aussi des sous-traitants et autres partenaires. La chaîne de sécurité doit s'appuyer sur les piliers très solides que sont les experts en cybersécurité. Elle ne doit présenter aucun maillon faible que serait l'employé non sensibilisé, trop naïf, trop impulsif, et pas au courant, par exemple des dangers des hyperliens dans des pages web, et des fichiers attachés dans les courriels, pas au courant des menaces que présentent les clés USB que l'on ramasse sur son chemin, et des attaques en ingénierie sociale. Ajoutons les mots de passe trop faibles, ou complexes, mais écrits sur un Post it, l'hygiène informatique permet d'éviter ces vulnérabilités.

Sensibiliser l'ensemble des employés d'une organisation est une sage précaution pour diminuer les risques. Cette sensibilisation doit être appuyée par la direction générale, être souvent répétée et passe par **l'information de tous les employés**, à l'hygiène informatique.

Dis-le-moi et je l'oublie
Montre-le-moi et je le retiens
Implique-moi et je le comprends

Ce proverbe illustre un travail de sensibilisation du personnel d'une organisation, utile et efficace. Laisser traîner des clés USB dans les couloirs d'une entreprise, qui, une fois connectées sur un poste de travail, avertissent

l'utilisateur qu'il vient de faire courir un danger potentiel à son organisation ; envoyer un mail, avec un contenu très bizarre et un fichier attaché ou un hyperlien qui conduit à un message d'alerte en cas d'ouverture du fichier ou de clic sur l'hyperlien, sont de bons moyens de susciter une méfiance salutaire face aux attaques en Ingénierie sociale. Il est indispensable que tous les employés comprennent qu'il faut se méfier du cyberespace.

Citons une campagne célèbre menée par Orange Business Services : un mémo promettait la gratuité pour un siècle sur la 6G illimitée aux premiers répondants qui devaient laisser leurs noms et leur date de naissance. Malgré les fautes d'orthographe bien sûr volontaires, malgré qu'il manquât le « a » dans le logo d'Orange, beaucoup se sont laissés prendre. On peut espérer qu'ils seront moins naïfs les fois suivantes, confrontés à des messages qui pourraient réellement être des débuts de menaces persistantes avancées, ou des tentatives d'hameçonnage ciblé.

Un dernier conseil, allez sur les MooC[4] qui permettent de monter en compétence, chacun à son rythme, comme celui de l'ANSSI[5] sur l'hygiène informatique, et celui de la CNIL[6] sur la protection des données à caractère personnel et la conformité au RGPD.

Parution le 18 septembre 2020

[1] Et toutes les organisations le sont.
[2] DICT : Disponibilité, Intégrité, Confidentialité, Traçabilité.
[3] IAM : gestion des identités et des permissions ; PCA : Plan de Continuité d'activité (dont la gestion de crise) ; DLP : Prévention contre la fuite de données ; SIEM : gestion des évènements de non-conformités, de vulnérabilités et de cyberattaques ; SOC : Tableau de bord de la sécurité.
[4] Massive on line open Courses : cours en ligne, accessibles par un navigateur
[5] MooC de l'ANSSI : secnumacademie.gouv.fr
[6] MooC de la CNIL : https://atelier-rgpd.cnil.fr

Heureusement que le numérique était là !

LAURE DE LA RAUDIERE
Députée d'Eure-et-Loir

La pandémie de la COVID-19 nous fait vivre des situations inédites. Après avoir été confinés pendant près de deux mois, nous voilà tous masqués afin de protéger les plus fragiles d'entre nous de ce virus encore inconnu, il y a moins d'un an. Je ne doute pas qu'avec le recul, nous en tirerons des enseignements majeurs en termes d'organisation sanitaire et économique. Le mot de « souveraineté » est dans tous les propos des politiques actuellement.

Heureusement que le numérique était là ! Beaucoup d'entreprises ont pu continuer à fonctionner grâce aux outils numériques. Nous sommes tous devenus pratiquants de la visioconférence, alors que beaucoup ne l'avaient jamais utilisée dans un cadre professionnel avant.
L'explosion des téléconsultations a permis le suivi médical et ont été plébiscitées par les Français, de tous âges. Nos enfants ont pu poursuivre leur scolarité à distance. Les artistes ont exploré de nouvelles façons d'atteindre leur public, par de nouvelles prestations.

Nous ne reviendrons pas en arrière.

Vers une société plus résiliente grâce à la formation au numérique et aux risques cyber

La douloureuse réalité de la sous-numérisation de nos entreprises a été mise en lumière depuis la période de confinement. Les entreprises numérisées s'en sortent aujourd'hui bien mieux que les autres puisque la capacité à vendre à distance a fait une vraie différence pour les TPE/PME. De même, le niveau de formation de nos concitoyens aux usages numériques est largement

perfectible. D'après le Digital Economy and Society Index (DESI) 2020, la France se classe en 15ème position en Europe démontrant nos fortes lacunes. J'aimerais que l'enseignement des technologies numériques soit vu comme une discipline pleine et entière dès le collège. Pourquoi ne pas remplacer le cours de « technologie » au niveau du collège par un cours de « culture et technologies numériques ». On y retrouverait tout ce qu'un collégien doit connaître pour vivre dans la société du XXIème siècle : un peu de code, beaucoup de temps sur le « bon usage » des réseaux sociaux, sur la qualification des recherches d'information sur Internet ou sur le respect des règles de droit sur Internet (propriété intellectuelle, propos haineux ou racistes, harcèlement…), un peu d'algorithmie pour comprendre que rien n'est « magique » et enfin, du temps pour comprendre les risques Cyber.

Afin de mettre un challenge à cet apprentissage, je propose la création d'une « coupe de France » de la cybersécurité mobilisant l'ensemble des collégiens, avec en ligne de mire l'European Cybersecurity challenge.

Cette formation initiale aux enjeux numériques n'est pas suffisante, car il faut aussi accompagner les citoyens aux usages du numérique. En dehors de quelques experts, personne n'est réellement préparé au risque cyber. La mise en place d'un tutoriel simple de formation et d'une communication massive sur les enjeux de cybersécurité est nécessaire, afin que chacun (dirigeants d'entreprises, salariés, mais aussi citoyens) prennent réellement conscience des enjeux et appliquent quelques règles simples « d'hygiène numérique ».
Nul doute que les attaques vis-à-vis des entreprises, mais plus généralement de notre économie et de nos institutions, sont bel et bien été orchestrées aujourd'hui par nos ennemis et que nous devrions mieux nous « armer » pour y faire face.

Vers des réseaux efficients et au service de tous

Nos infrastructures fixes et mobiles ont fait face à une augmentation considérable du trafic (+30 % selon l'ARCEP) et grâce à la mobilisation des opérateurs, nos réseaux ont bien résisté au choc d'usages. La crise a révélé des inégalités d'accès au numérique toujours inacceptables dans plusieurs territoires alors que les déploiements fixe et mobile ont un impact positif bien réel sur la croissance et l'attractivité.

En ce qui concerne la 5G, le report des enchères d'avril dernier à fin septembre et le débat politique lancé par certains maires et élus « Ecologie – Les Verts » ne doit pas se transformer en retard ! Cette technologie est, d'abord, une nécessité au risque de voir les réseaux 4G saturer d'ici deux ans dans les grandes villes et, ensuite, une véritable opportunité pour le développement de nouveaux usages, en particulier via le déploiement des objets connectés dans les secteurs industriel, agricole ou de la santé. À l'heure où l'Allemagne met 7 milliards pour accélérer le déploiement de la 5G, où les États-Unis et la Chine ont déjà des milliers d'antennes, nous ne pouvons faire une croix sur cette technologie. Derrière l'opposition à cette technologie se cache la théorie de la décroissance très dangereuse pour notre économie et nos emplois.

Écologie et numérique, deux mondes à réconcilier

Ceux qui refusent la 5G et veulent interdire le déploiement sur leur commune arguent de l'augmentation de l'empreinte carbone de la nouvelle génération de réseau Mobiles. C'est devenu l'argument des « anti », qui ne prennent jamais en compte le fait que l'usage du numérique fait aussi économiser nombreux déplacements, rend plus efficient la gestion de l'énergie avec les smart grids... Aujourd'hui peu d'études complètes et non financées par le secteur existent sur ce bilan. En revanche, toutes les études sur l'empreinte environnementale du numérique montrent que la consommation des réseaux de télécommunication est marginale par rapport au reste. Le rapport du Sénat « Pour une transition numérique écologique » de 2020 dévoile que les terminaux sont à l'origine d'une très grande part des impacts environnementaux du numérique (81 %), l'usage de nos outils représente ainsi une part assez faible de l'empreinte carbone du numérique C'est donc sur cet axe qu'il convient de travailler en premier. Et une taxe Carbone aux frontières de l'Europe nous y aiderait bien !

Cet enjeu de réconciliation entre écologie et numérique est majeur. L'ARCEP ne s'y est pas trompé puisque c'est le thème de la grande étude qu'elle a lancée sur l'empreinte environnementale des réseaux[1].

Soyons honnêtes : la crise sanitaire a montré à quel point nos outils numériques sont indispensables pour rendre une société plus résiliente. C'est

donc dans ce monde ultra connecté que nous vivons. À nous d'en faire un levier pour régler les enjeux actuels en matière de protection de l'environnement.

Parution le 25 septembre 2020

[1] https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-des-reseaux.html

Sécuriser le télétravail dans les institutions publiques

CHRISTOPHE AUBERGER
Directeur technique
FORTINET

Dans le cadre de la crise que nous traversons, les gouvernements du monde entier se sont concentrés sur la gestion de la transition globale de leurs technologies de l'information à destination de collaborateurs travaillant soudainement tous à distance. La continuité des opérations et la continuité du gouvernement (COOP/COG) sont devenues plus urgentes. Jusqu'alors ils s'étaient surtout attachés à identifier les employés considérés comme "essentiels" ou " critiques pour la mission " et qui devaient continuer à se rendre sur leur lieu de travail habituel ou sur un autre site officiel.

Les gouvernements doivent maintenant trouver le moyen d'assurer la pleine action de leurs équipes pendant une période prolongée, la plupart de ces employés étant souvent à domicile, pour assurer la continuité des opérations gouvernementales.

D'un point de vue informatique, ce défi se décompose en trois éléments :

- Tout d'abord, la sécurité du point d'accès d'un travailleur à distance. Il peut s'agir d'un réseau domestique auquel sont attachés des dispositifs personnels connectés vulnérables. Les membres de la famille qui utilisent des applications, les médias sociaux et les consoles de jeux, introduisent potentiellement des menaces dans le réseau. L'ensemble de cet environnement d'exploitation échappe au contrôle de l'organisation et donne un nouveau sens à l'expression " risque d'initié ". Alors comment isoler l'appareil du travailleur à distance ou, du moins, garantir l'intégrité des données et des opérations gouvernementales sur cet appareil ?

- La sécurité de la transmission ensuite - il s'agit de s'assurer que les données gouvernementales sont cryptées lorsqu'elles circulent sur Internet.
- Enfin, le HQS ou bureau principal. Les réseaux de presque tous ces environnements ont été conçus pour le cas où les employés travaillent à l'intérieur du périmètre du réseau. A-t-il la capacité d'absorber le nombre de connexions nécessaires à leur déplacement vers des sites distants ? Peut-il gérer ces connexions avec un temps de latence acceptable, afin que les utilisateurs ne soient pas frustrés par la lenteur des performances du réseau ? Peut-il garantir que ces connexions sont sécurisées et uniquement accessibles aux utilisateurs autorisés ?

La bande passante est aussi un élément important. Certaines applications nécessitent-elles des niveaux de bande passante inhabituellement élevés ? Quelle peut être l'efficacité de la solution mise en place lorsque les télétravailleurs ont des difficultés à se connecter ? Et même s'ils ont accès, il est important de reconnaître que non seulement les vitesses varient considérablement, mais que d'autres ressources connectées à un réseau domestique - comme les enfants qui suivent un enseignement à distance - peuvent consommer la bande passante disponible.

Ainsi, l'informatique dématérialisée devient une option particulièrement attrayante. Pour les fonctionnaires, les TIC 3.0 permettent une connexion directe aux ressources basées sur le cloud - plutôt que de devoir faire transiter le trafic par l'agence d'origine - et permettent également l'utilisation de plateformes SaaS (Software as a Service).

En gardant ces considérations à l'esprit, les éléments clés pour un accès à distance sécurisé par un fonctionnaire devraient inclure :
- Un réseau privé virtuel (VPN) dont les points d'extrémité sont l'appareil de l'utilisateur distant et le bureau parent (ou le cloud).
- L'authentification multifactorielle pour garantir que seul l'employé distant autorisé peut accéder au réseau ou aux données de l'employeur.
- La sécurité des points d'extrémité (endpoints) fournie par l'employeur pour garantir la sécurité de l'informatique, des données et des réseaux du gouvernement, même lorsque l'employé travaille à partir d'un réseau domestique vulnérable ou compromis.

- La prévention des pertes de données (DLP) qui fournit un filet de sécurité contre l'exposition par inadvertance de données sensibles, même lorsque les employés travaillent avec des distractions potentielles ou sous des facteurs de stress extraordinaires.
- Le contrôle de la gestion des dispositifs pour répondre aux besoins des organisations qui veulent autoriser - ou peuvent même exiger - des opérations BYOD de la part de leurs employés.

Il existe des solutions commerciales éprouvées qui tiennent compte de tous ces facteurs. Idéalement, du point de vue des frais généraux informatiques, la plupart de ces solutions devraient fonctionner comme un seul système intégré, avec un seul point de gestion. Les organisations qui ont été confrontées à la nécessité d'agir rapidement pour soutenir les populations de travailleurs éloignés ne devraient pas avoir à réinventer la roue, que ce soit en termes de technologies ou de meilleures pratiques requises pour leur adoption.

Parution le 2 octobre 2020

La cybercriminalité à l'heure de la Covid-19

MYRIAM QUEMENER
Magistrat
Docteur en droit

La crise de la Covid-19 a réactivé le fléau des cyberattaques qui se développe et qui profite du contexte anxiogène actuel, les cyberdélinquants jouant souvent sur la peur auprès des internautes. Le constat d'une explosion des attaques et d'une diversification de la menace d'origine cyber est partagé par l'ensemble des observateurs et des acteurs de la sécurité informatique. La digitalisation des activités humaines associées à des nouveaux usages numériques mal maîtrisés[1] conduit inévitablement à une explosion du phénomène qui implique une stratégie renouvelée en particulier au niveau de tous les pouvoirs publics. En outre, les nouveaux usages du numérique instaurent une véritable disruption[2] tant au niveau juridique que sociétal et organisationnel.

Les attaques informatiques par rançongiciels contre les entreprises sont devenues la méthode privilégiée par les cybercriminels, permettant de récupérer des sommes importantes et de faire de l'espionnage économique. Comme le souligne un récent rapport sénatorial[3], la cybercriminalité apparaît comme une menace en hausse notamment en raison de la numérisation croissante de la société.

Ce phénomène vise toutes les organisations y compris des hôpitaux par centaine comme aux Etats–Unis avec les établissements de la chaîne américaine Universal Health Services (UHS), groupe privé qui compte 400 établissements. Récemment, en Allemagne, une patiente est décédée, faute d'avoir pu être prise en charge. En France aussi, des attaques ont eu lieu. La plus grave contre le CHU de Rouen à la fin de l'année dernière, qui avait provoqué de grosses perturbations.

Toutes les entreprises peuvent en être victimes, comme par exemple Orange Business Services, M6, Fleury-Michon, Bouygues Construction, Eurofins, Altran mais également des hôpitaux, des ministères, des cabinets d'avocats et des collectivités territoriales. Les attaques par rançongiciels augmentent en nombre, en fréquence et en sophistication. Dernièrement, le groupe CMA CGM[4], quatrième armateur mondial dans le transport maritime, a annoncé sur Twitter être victime d'une cyberattaque sur ses serveurs périphériques. Depuis le début de l'année, l'Agence nationale de la sécurité des systèmes d'information a traité 104 attaques par rançongiciels : « Leurs conséquences sont de plus en plus dévastatrices, sur la continuité d'activité, voire la survie de l'organisation victime », note l'ANSSI.

Rappelons qu'un rançongiciel[5] est un logiciel informatique malveillant qui chiffre les fichiers contenus sur les ordinateurs et demande une rançon.

L'analyse du rançongiciel permet de comprendre que la pièce jointe n'était qu'un fichier contenant en son sein des instructions permettant le téléchargement de la charge virale sur l'ordinateur de la victime, et ce, à l'insu de celle-ci, à partir d'un site distant dit « site de distribution ». Ces sites de distribution s'avéraient être des serveurs internes compromis, bien souvent à l'insu de leurs propriétaires, qui n'ont généralement pas réalisé la mise à jour des logiciels de leurs systèmes.

Les réponses juridiques

Les attaques par rançongiciel peuvent ainsi être poursuivies sur la base des atteintes aux systèmes de traitement automatisé de données (STAD). Les escroqueries au faux ordre de virement peuvent aussi être poursuivies au titre des atteintes au STAD.

Ces cyberattaques peuvent aussi être qualifiées d'extorsion simple ou en bande organisée sur le fondement des articles 312-1 et 312-6-1 du Code pénal. Les articles 313-1 à 313-3 du Code pénal, qui sanctionnent l'escroquerie, simple ou en bande organisée, peuvent être utilisés pour réprimer les escroqueries à la fausse amitié ou à la romance, les escroqueries à l'investissement en ligne, au faux site de vente en ligne ou encore l'arnaque au faux site administratif.

La justice se mobilise face à ce fléau depuis l'entrée en vigueur de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, l'article 706-72-1 du Code de procédure pénale confie au procureur de la République, au pôle de l'instruction, au tribunal correctionnel et à la cour d'assises de Paris une compétence concurrente nationale en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et d'atteintes aux intérêts fondamentaux de la Nation ce qui peut couvrir des hypothèses de cyber-sabotage.

Au sein du parquet, cette compétence est confiée à la section J3, anciennement dénommée section F1, ou section cybercriminalité. Au titre de sa compétence nationale, la section J3 peut se saisir des affaires de cybercriminalité complexes, où qu'elles se produisent sur le territoire, les parquets locaux demeurant compétents pour le reste du contentieux. Elle est seule compétente pour les infractions commises dans le ressort du parquet de Paris. En 2020, la section J3 a ouvert 249 enquêtes sur le fondement de cette compétence nationale, dont 225 sont toujours en cours.

Plusieurs affaires prospèrent et aboutissent comme en témoigne par exemple l'interpellation d'un russe, Alexander Vinnik[6], soupçonné d'être le créateur du rançongiciel Locky et administrateur d'une plateforme facilitant le blanchiment de fonds et qui va être jugé en France. Ce logiciel malveillant rend illisibles les fichiers qu'il attaque Arrêté pendant ses vacances en Grèce en juillet 2017, il a été remis aux autorités judiciaires françaises en janvier 2020. Il est poursuivi pour extorsion et blanchiment d'argent. Placé en détention préventive, il est soupçonné d'avoir orchestré les malversations de BTC-e, la plateforme d'échanges de bitcoins fondée en 2011 et devenue l'une des plus importantes au monde mais accusée d'extorsions en ligne et d'autres activités de cybercriminalité. Les services saisis de l'enquête ont recensé plus d'une centaine de victimes de Locky.

Le site de paiement vers lequel étaient redirigées les victimes correspondait à un site internet « onion », c'est-à-dire accessible uniquement par l'intermédiaire d'une connexion au réseau d'anonymisation TOR dont la particularité est de masquer l'adresse IP du serveur par une série de « serveurs passerelles ». En outre, à la différence de nom de domaine classique

(.fr ou .eu), les noms de domaine en .onion ne sont enregistrés auprès d'aucune autorité avec une déclaration d'identité mais simplement créé automatiquement par le logiciel. Les investigations ont permis d'établir que le site de paiement indiqué aux victimes proposait en échange du paiement de la rançon en bitcoin, un logiciel nommé « Locky Decryptor » permettant le déchiffrement des fichiers des victimes. Une aide était même proposée à ces dernières pour leur permettre d'obtenir des bitcoins afin de payer leur rançon. Cette procédure est un exemple qui a nécessité de mettre en œuvre de nombreuses investigations à l'international complexes.

Comment renforcer la lutte contre les attaques numériques ?

Les institutionnels conseillent dans les affaires de rançongiciels de ne pas payer la rançon et de déposer plainte et ce d'autant que les cybervictimes risquent de ne récupérer ni la totalité ni même une partie des fichiers chiffrés et cela peut favoriser la promotion de ces activités cybercriminelles. Carlson WagonLit Travel (CWT), spécialiste des voyages d'affaire, victime de Ragnar Locker, aurait payé 4,5 millions de dollars pour remettre en route les 30 000 PC paralysés. Au départ, le gang réclamait 10 millions de dollars et c'est le directeur financier de CWT en personne qui a assuré la négociation. Plaidant les difficultés de l'entreprise liées à la crise sanitaire, il a réussi à réduire le montant de la rançon.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le 4 septembre 2020, en partenariat avec le ministère de la Justice et la DACG, un guide de sensibilisation destiné aux entreprises, collectivités et administrations. Le document propose des mesures préventives issues du guide d'hygiène informatique de l'ANSSI qui permettent d'éviter qu'un rançongiciel n'atteigne l'organisation ou, a minima, de réduire les pertes liées à une telle attaque. Il conseille notamment d'utiliser et de maintenir à jour les logiciels antivirus, de cloisonner le système d'information, de limiter les droits des utilisateurs et autorisations des applications, de sensibiliser les collaborateurs, d'évaluer l'opportunité de souscrire à une assurance cyber, de définir une stratégie de communication de crise cyber. En réunissant témoignages de victimes et bonnes pratiques de sécurité numérique, ce guide sensibilise les

différents acteurs économiques aux rançongiciels et invite les organisations - du comité exécutif aux collaborateurs - à se saisir de ces questions.

Suite à l'explosion de ce fléau bien soulignée par de nombreux rapports ministériels[7] parlementaires[8] et du secteur privé[9], il est indispensable de mettre en œuvre les recommandations phares relatives notamment à la sensibilisation des citoyens, au renforcement des moyens humains et de la coopération internationale.

En outre, plusieurs rapports du Sénat tirent la sonnette d'alarme de façon accélérée depuis quelque temps sur l'ampleur que prend la menace cyber[10]. L'un de ces documents, d'ailleurs souligne l'impréparation de certaines administrations face aux cyberattaques qui nécessitent la mise en place d'un pilotage de la gestion de crise[11].

Si tous les acteurs sont concernés par cette lutte, il faut souligner que les ministères régaliens le sont en première ligne, ministère de l'Intérieur et de la Justice. À cet égard, l'institution judiciaire est de plus en plus saisie par des procédures relatives à la cybercriminalité, la délinquance glissant nettement vers les usages numériques, notamment en matière économique et financière[12] où les préjudices sont souvent colossaux. Une campagne nationale de sensibilisation aurait à cet égard actuellement tout son sens.

S'il apparaît nécessaire d'augmenter les moyens du parquet spécialisé ainsi que le souligne le rapport pour être porté au niveau de ceux des grands États européens les plus engagés dans ce domaine, cette remarque vaut également pour les magistrats du siège. Si la spécialisation est nécessaire, elle ne doit pas être poussée à l'excès, compte tenu du caractère transversal du numérique. Il est important également que l'ensemble de la chaîne pénale, (siège et parquet) soit véritablement au fait de ce fléau et comprenne parfaitement les modes opératoires souvent complexes et évolutifs. Il est clair désormais que la lutte contre la cybercriminalité implique en outre un renforcement de la coopération public/privé et internationale.

En septembre 2020, la France, la Lituanie et la Lettonie ont proposé à l'UE un plan pour protéger les élections en Europe contre les

cyberattaques et la désinformation, ont annoncé en septembre 2020 les présidents français et lituanien lors d'une conférence de presse.

Parution le 9 octobre 2020

[1] M. Quéméner, C. Wierre, F. Dalle, Quels droits face aux innovations numériques ? : Lextenso 2020.
[2] M. Quéméner, le droit face à la disruption numérique , Lextenso Gualino 2018
[3] Sénat, S. Joissains et J. Bigot, « Cybercriminalité : un défi à relever aux niveaux national et européen », fait au nom de la commission des affaires européennes et de la commission des lois : rapp. info. n° 613 (2019-2020) 9 juill. 2020
[4] https://www.usine-digitale.fr/article/cma-cgm-victime-d-une-cyberattaque-l-acces-a-ses-applications-informatiques-est-indisponible.N1010124
[5] ou ramsomwarel en anglais.
[6] https://www.zdnet.fr/actualites/le-russe-alexander-vinnik-extrade-en-france-39898105.htm
[7] L'état de la menace liée au numérique en 2019 : www.interieur.gouv.fr. - Protéger les internautes, rapp. sur la cybercriminalité, 2014 : www.justice.gouv.fr.
[8] O. Cadic et R. Mazuir, Suivi de la cybermenace pendant la crise sanitaire : rapp. d'info. n° 502 (2019-2020), 10 juin 2020, fait au nom de la commission des affaires étrangères, de la défense et des forces armées : www.senat.fr.
[9] Le rapport Risk Solutions souligne la taille, l'échelle et l'exposition monétaire des réseaux mondiaux de cybercriminalité : LexisNexis, https://risk.lexisnexis.com/global/fr/about-us/press-room/press-release/20200304-cybercrime-report.
[10] J. Bascher, La sécurité informatique des pouvoirs publics : rapp. d'info. n° 82 (2019-2020), 22 oct. 2019, fait au nom de la commission des finances : www.senat.fr
[11] ANNSI, État de la menace rançongiciel à l'encontre des entreprises et institutions, 5 févr. 2020 : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
[12] M. Quéméner, criminalité économique et financière à l'ère numérique, Economica 2015

Le retour de la « Panic Room »

HERVE MORIZOT
Co-fondateur et Directeur général
FORMIND

Dans un monde digital, une entreprise ayant perdu ses données est une entreprise morte.

Ce risque semble progresser plus vite que les mentalités et les solutions

Le risque de perte pure et simple de données est apparu très récemment dans les cartographes des risques de nos entreprises. Il était globalement absent des radars jusqu'en 2015 – 2017. Remercions notamment Saint-Gobain qui, en évoquant une perte d'environ 250 M€ de CA et de 80 M€ de résultat d'exploitation avec NotPetya, a commencé à sensibiliser le marché.

L'année 2020 connait d'ailleurs une augmentation particulièrement forte de ces ransomware.

Il devient même « le risque » majeur Cyber

Autrefois limités aux fameux DICT (…), l'indisponibilité du SI ou des données se bornait bien souvent à des délais d'accès allongés, de quelques heures ou quelques jours… parfois avec des restaurations de sauvegardes qui engendraient des pertes ponctuelles de données.

Or l'ampleur des moyens mis en œuvre par les attaquants a décuplé depuis cette date, et le niveau de technicité des attaquants a largement cru.

L'objectif majeur des attaquants est de bloquer une activité, une entreprise,

un état, tant que les conditions demandées ne sont pas réunies (généralement une rançon pour les entreprises, des actes politiques pour les administrations et états,…).

La perte de données au-delà du blocage « ponctuel » de leur accès est donc leur « graal ».

Et bien évidemment, le fait de payer ne garantit pas de retrouver ses données…

Les régulateurs ont bien compris cela, et leurs exigences de disponibilité des données sont croissantes.

L'enjeu est de taille pour les attaquants

Les Mafias et autres bandes organisées ont, elles aussi, engagé de réelles transformations digitales !

Le coût des attaques Cyber a dépassé depuis près de 10 ans ce que rapporte les trafics de drogue sur un plan mondial. Ce coût devrait bientôt avoisiner les 1 000 milliards de dollars (estimation de 600 milliards en 2017 – *source PwC*).

Les attaques de biens physiques sont en effet souvent nettement plus risquées pour l'attaquant, et plus sévèrement punies.

Si elles restent techniquement pointues, on trouve sur Internet des plateformes RaaS, « Ransomware as a Service », qui proposent outillage, formation et même support en ligne.

Enfin, la surface d'attaque s'étend en permanence : monde digital, « geekisation » de la population, ultra connexion et ultra réactivité,…
Bref, les attaquants disposent de moyens forts, d'expertise technique de haut niveau, et ciblent de plus en plus leurs victimes, en mettant à profit les périodes de fragilité des entreprises,...

Les dispositions actuelles de réaction et de continuité sont à réadapter

Les mesures en place en matière de disponibilité sont basées sur trois piliers :
• Prévention
• Détection
• Réaction

Malgré de lourds investissements sur les deux premiers, tout le monde s'accorde sur le fait que l'attaque va arriver, et qu'il faudra en limiter les effets. La question n'est plus de savoir si elle va arriver, mais de savoir quand ?

Or les dispositifs de réaction existants (que faire quand l'attaque est avérée ?) ne permettent pas de répondre à ce risque de manière satisfaisante.

Les coûteuses solutions de haute disponibilité mises en œuvre pour répondre à des forts enjeux de disponibilité présentent aujourd'hui une grosse faiblesse en répliquant potentiellement les données chiffrées par ransomware.

La restauration des données constitue donc le dernier recours à condition que les sauvegardes aient été épargnées par les attaquants.

Je dois préserver des sauvegardes « saines » pour les restaurer dans un environnement IT rendu « sain ».

Or les sauvegardes, pour être utiles, doivent être « fraîches », en temps réel, sinon leur restauration induit une perte de données, de qualité et de cohérence.

Donc ces sauvegardes sont « en ligne », « à chaud », et non plus sur des bandes que nous mettions à l'abri il y a encore quelques années.

Donc il existe un lien réseau entre le SI nominal et les systèmes de sauvegarde, et c'est le cœur du problème.

Une « Panic Room » est-elle LA solution ?

Pour que les attaquants ne puissent pas avoir accès aux sauvegardes, celles-ci doivent être idéalement exclues du SI de l'entreprise.

Un peu comme le SI Industriel doit être distinct du SI de Gestion et du SI accessible aux clients et partenaires (ce qui n'est généralement plus le cas d'ailleurs).

La notion de « Panic Room » vise à « cacher » les données vitales de l'entreprise dans un cocon hyper sécurisé.

Plusieurs grands groupes ont ainsi amorcé ces projets, en mode 'task force', sur 6 mois maximum

En voici quelques pistes de réflexion :

#Frugalité
Soyez très sélectifs dans l'identification de vos données « vitales ». Si elles représentent 50 % du volume globale de vos données, vous allez créer un SI de secours, qui existe certainement déjà …

Limitons-nous à 5 % des données qui sont réellement vitales !

Et acceptons le fait que la perte des autres données serait très grave, sans être nécessairement catastrophique.

#Agilité
Comme tout projet informatique, ce projet doit être mené dans un planning et avec des moyens restreints.

Si vous partez sur un projet en 2 ou 3 ans en impliquant les métiers de l'entreprise, bon courage…

Les modalités d'accès sont activées en cas de crise uniquement.

Les accès sont possibles par des postes qui ne sont pas ceux de l'entreprise

(mon PC personnel ne sera pas nécessairement infecté en cas d'attaque de mon entreprise …).

#Confidentialité
Les attaquants ne doivent pas connaître l'existence de ces dispositifs. Sinon ils se donneront les moyens de mener des attaques coordonnées du SI nominal et de la Panic Room.

#Pragmatisme
Les données de l'entreprise doivent être classifiées en disponibilité / qualité, au-delà de la confidentialité qui est plus fréquente. Commençons par les données exigées de mes régulateurs, souvent vitales.

Les données basculant sur la Panic Room doivent être fiables et sûres. Elles doivent transiter vers un « bac à sable » dans lequel on prend le temps de les « torturer » et d'en attester la sécurité.

#Décentralisation
Pourquoi mettre tous ses œufs dans le même panier ?

Chaque métier sensible peut avoir sa propre « Panic Room », cela compliquera la vie des attaquants.

Ne négligeons pas le dernier maillon de la chaîne de sécurité, il pourrait vous être utile dans les prochaines années.

Parution le 16 octobre 2020

Informatique de santé et cybersécurité : prospectives 2037

CEDRIC CARTAU
RSSI et DPO
CHU DE NANTES et GHT44

Attaques cyber des hôpitaux, crise COVID, informatisation des soins, objets connectés : autant d'évolutions – ou de révolutions – qui se déroulent sous nos yeux, pas au même rythme ni à la même échelle de temps, et qui vont bouleverser le paysage de la santé numérique dans les prochaines décennies. Petite tentative prospective sans prétention.

Les prospectives en informatique constituent un excellent exercice de voltige avec chute assurée – n'était-ce pas cet ancien président d'IBM qui pensait qu'il n'y avait pas besoin dans le monde de plus de cinq ordinateurs, ou de Bill Gates qui affirmait en son temps qu'avec 640 Ko de RAM il y en avait bien assez ? Mais même hasardeux, l'exercice n'en reste pas moins grisant, et nous proposons de phosphorer à ce que seront les SI de santé dans 15 ans, avec leur corollaire cybersécurité.

En 2037, nous aurons changé au moins quatre fois de Président de la République, au moins autant de fois de premiers ministres sans parler du ministre de la santé, et sans parler des modifications réglementaires qui continueront de s'empiler. Avant de se projeter dans 17 ans, prenons un moment pour regarder 17 ans en arrière : il y avait quoi en 2003 ?

Back to the Future

En 2003, le principal enjeu de la SSI est d'avoir un AV à jour, les ingénieurs systèmes sont essentiellement préoccupés par l'efficacité des filtres antispam. La DMZ compte rarement plus de dix @IP (en 2003 au CHU de REIMS il y avait 5 @IP dans la DMZ), seul un CHU a nommé un RSSI (Strasbourg).

Presque aucun établissement de santé n'a dédoublé son datacenter, et la préoccupation majeure de la messagerie est d'attribuer une BAL à chaque agent. D'ailleurs une bonne partie des équipes de direction n'ont pas de BAL et n'en voient même pas l'utilité : suggérer qu'un DG puisse taper lui-même un mail peut envoyer un informaticien directement au goulag.

Le Wifi n'est quasiment jamais déployé, sauf exception notable, quant à la sauvegarde, elle est faite sur bande, les bandes sont changées chaque jour par des pupitreurs, quelquefois les bandes sont déplacées pour être mises en sécurité. Le firewall est souvent un équipement en rack dont peu de gens s'occupent, le nombre de PC d'un établissement est en général égal à son nombre de lits, les smartphones n'existent pas, le dernier gadget à la mode est le Palm voire le Blackberry pour les plus hypes.

Les connexions ADSL commencent à peine à se démocratiser auprès du grand public (à peine 1 million d'abonnés en 2002), le téléchargement illégal est un concept inexistant, autant que Youtube et Dailymotion. Facebook n'existe pas encore.

Les audits techniques de sécurité sont inconnus, les audits organisationnels sont rarissimes, sauf conflit patent entre la DSI et la DG et d'ailleurs la norme ISO 27 001 est inconnue (elle sera reprise de la BSI par l'ISO en 2005).

L'informatique est essentiellement administrative : le cœur de métier (unités de soins) est peu équipé : le plan hôpital 2007… ne sera lancé qu'en 2004.

Une panne de 72 heures de l'informatique d'un établissement n'impacte pas le processus de soins, le hacker le plus dangereux dont on ait souvenir est un adolescent qui s'amuse à pirater le PABX (Kevin Mitnick).

Le seul organisme étatique traitant de question de sécurité est le GMSIH. L'ASIP santé, avec son rôle plus opérationnel, n'est créée qu'en 2009.

Les problématiques d'habilitation n'existent pas : Enron, Jérôme Kerviel et Bâle 2 ne sont pas encore arrivés.

Quand on demande à un informaticien de disserter sur la sécurité

informatique, il pense à la longueur des mots de passe et au compte admin système du contrôleur AD (vécu).

Quand on demande à un DSI ce qu'il pense de la sécurité informatique, il pense à la panne du serveur de paye (vécu aussi).

Quand on demande à un DG ce qu'il pense de la sécurité informatique, il ne pense à rien.

Mais tout ça, c'était avant.

Prospectives : évolution de l'informatique de santé

Alors que la médecine n'a connu que trois révolutions majeures en 2 000 ans (rupture de paradigme au sens kantien du terme : les antibiotiques, l'anesthésie et l'imagerie médicale), au moins six tendances vont se dégager dans les prochaines décennies.

Première tendance lourde : la génomique.
Le séquençage du génome est une réalité depuis plus de 10 ans, et tout un chacun peut se faire analyser son ADN sur des sites tels 23andme.com (avec certes des interrogations sur le devenir de ses données). L'analyse du génome va devenir courante, telles les scènes du film d'anticipation « Bienvenue à Gattaca » : avant toute prise en charge médicale, le génome sera séquencé et cet acte sera aussi banal que peu couteux.

Deuxième tendance : l'intervention directement sur le génome, avec en toile de fond la médecine personnalisée : un médicament sera conçu et fabriqué pour une personne précise, dans un contexte précis et pour un objectif thérapeutique précis.

Troisième tendance lourde : le recours de plus en plus banal au transhumanisme, modification volontaire du corps humain soit par implants, soit directement par modification du génome. Des outils existent déjà, tel le CRISPR-CAS9.

Quatrième tendance, conséquence des deux précédentes : la notion de fontaine de jouvence. Le recours à l'acte médical ne se limitera plus au traitement d'une pathologie, mais va s'étendre à la notion de bien-être. La chirurgie esthétique, inventée à la fin de la première Guerre Mondiale pour réparer les « gueules cassées » est maintenant utilisée à des fins essentiellement esthétiques.

Cinquième tendance : le self quantifying permanent. Les objets connectés tels les montres ou les smartphones permettent déjà de mesurer en temps réel quantité de paramètres telle l'activité physique, le rythme cardiaque, le taux de sucre, etc.

Sixième tendance : la télémédecine généralisée. Plus de 30 % d'actes seront réalisés hors présentiel patient/médecin. La crise sanitaire COVID19 a été un accélérateur foudroyant de ce type de pratiques, et les pays nordiques (Suède et Norvège entre autres) sont très en avance sur nous, configuration géographique et climat obligent.

Quels outils en face de ces besoins ?

Face à ces tendances lourdes, les DSI devront mettre en place des démarches, des infrastructures, des outils, des compétences.

Vers HIMSS niveau 7

La France accuse un retard considérable dans la maturité des SI des établissements de santé, dont la majeure partie ne dépasse pas le niveau 3 ou 4 sur une échelle HIMSS qui va de 1 à 7. Le niveau 7 est la cible, il faudra au bas mot quinze ans pour le voir se généraliser et cela nécessitera au minimum un triplement des budgets SI.

Le Big Data et les centres de calcul

Ce niveau 7 nécessite de monter des infrastructures de stockage et d'analyse. Le Health Data Hub est une réponse à certains besoins mais ne couvre pas ou peu le champ du soin aigu. Les établissements de santé vont devoir mettre en production des Cliniques de données, de consultation des données

d'ambulatoire des données, tel ce qui a été mis en place par le Pr Pierre-Antoine GOURRAUD au CHU de NANTES avec la société WEDATA.

Explosion des IoT : le self quantifying va se traduire par une explosion des gadgets grands publics, l'IoT verra la même courbe dans le domaine professionnel. Les actes médicaux répétitifs (prendre la tension, peser le patient, etc.) peuvent déjà être pour partie réalisés et automatisés.

Forte technicisation des actes médicaux : en 2030 les chirurgiens n'opèreront plus avec leurs mains : ils piloteront des joysticks.

Dispositifs médicaux implantés de nouvelle génération

Prothèses, humains augmentés, capteurs, pilules connectées, etc. : autant d'objet qui vont devenir banals, que ce soit pour suivre une pathologie chronique, pour surveiller un patient au bloc ou en réanimation.

Porosité des réseaux informatiques

Si le BYOD, qui avait le vent en poupe il y a à peine cinq ans, a disparu des écrans radars des fournisseurs. L'ouverture massive des réseaux (LAN) des établissements de santé vont faire que « dedans » ou « dehors » du LAN ne va plus avoir le même sens qu'aujourd'hui. Le débat Cloud / On Premise n'aura plus de sens : les infrastructures IT seront mixtes, réparties à la fois sur les datacenters internes de l'établissement et sur un ou plusieurs Cloud publics ou privés. L'interopérabilité technique ou sémantique sera la principale, sinon la seule valeur ajoutée d'une DSI.

Ouverture massive des DPI

En 2020 il est possible de consulter ses comptes bancaires, son abonnement à Fnac ou ses livraisons Chronopost directement sur son smartphone, mais toujours pas son dossier médical auprès de l'établissement public ou privé de la ville. Cet anachronisme va disparaître.

Nouveaux matériaux

Impression 3D, matériaux composites et nanomatériaux : certains éléments – par exemple les prothèses de hanches – seront « imprimés » en 3D quelques heures avant l'opération.

Vers la certification ISO comme centre de gravité

Pendant des décennies, la valeur ajoutée d'une DSI – son centre de gravité – aura été sa capacité à maîtriser des technologies pointues : serveurs, stockage, virtualisation. À ces compétences s'est progressivement ajoutée depuis les années 1990 la maîtrise du fonctionnel métier. Dans la prochaine décennie, les DSI seront certifiées – ISO 9000, ITIL, ISO 27001, etc. – ou devront tirer le rideau : le centre de gravité passera alors sur la maîtrise des processus et de la qualité de services.

Quelles nouvelles menaces ?

Mais face à ces enjeux de santé et à l'évolution des outils qui les supportent, apparaîtront des nouvelles menaces.

Professionnalisation de la malveillance IT…

Il n'est de secret pour personne que les état dits « voyous » constituent une des premières sources d'attaque. Et dans le même temps on a des STUXNET ou des FLAME conçus par nos « amis » américains.

…et pourtant toujours l'adolescent dans son garage.

La cyber est l'arme du pauvre, et c'est justement ce qui la rend dangereuse.

De l'allégorie des missionnaires dans la savane pour adapter sa stratégie de cyber résilience

Deux missionnaires dans la savane tombent nez à nez avec un lion, et se mettent à courir à toutes jambes. L'un demande à son copain : « tu crois que l'on arrivera à courir plus vite que le lion ? ». L'autre lui répond : « pas du

tout, mais je ne cherche pas à courir plus vite que le lion, je cherche juste à courir plus vite que toi ».

Généralisation des 0-Day

Conséquence de la professionnalisation, le marché des 0-Day est mondial, nul n'est à l'abri. Ce marché s'organise, avec ses producteurs, ses brokers, ses revendeurs.

Multiplication des périphériques

Et ce sont tous potentiellement des sources de vulnérabilité et donc d'attaque. Il y a vingt ans, il n'y avait que des PC. Maintenant il y a des PC, des PC portables, des tablettes, des smartphones, des photocopieurs multifonction, des caméra IP connectées, etc. Si quelqu'un a réussi à patcher ses caméra IP, je veux bien qu'il m'explique comment il s'y est pris.

Multiplication des attaques en déni/usurpation d'identité

Si la grande mode des années 2000 était les attaques en déni de service (DOS, dDOS, etc.), cela rapporte clairement beaucoup plus de réaliser des attaques en déni ou usurpation d'identité : fraude au président, détournement de factures fournisseur, etc.

Nouvel or noir que représentent les bases de données médicales : les bases de données médicales deviennent une cible pour la connaissance médicale et statistique qu'elles représentent et pas pour la valeur marchande du dossier de Mme DUPONT.

Multiplication des procédures juridiques

Les établissements vont devoir faire la preuve par la trace, avec forte contraintes sur les systèmes de traçabilité interne avec valeur probante.

Composants IoT frelatés

Il va être nécessaire de déployer à l'échelon national ou européen une base

d'IoT-vigilance, au même titre qu'il existe une pharmaco-vigilance.
Disparition de la téléphonie, du biomed, de la logistique en tant que domaines « à part ».

En 2037, on aura bien du mal à dire si un serveur abrite une application médicale, biomédicale, téléphonie, etc.

Quelles prospectives pour la sécurité des SI de santé ?

Dans certains domaines il va falloir opérer des changements de paradigmes radicaux, car les outils, les processus et les compétences actuels ne vont plus être suffisants ou tout simplement appropriés.

Il va falloir dans un premier temps acter la fin des outils mastodontes : nécessité d'agilité dans le déploiement d'outils légers, peu chers et pointus. Également intégrer la problématique IoT, notamment dans le domaine des prothèses, des dispositifs médicaux, etc.

Il va falloir également prendre en compte les menaces 0-Day et APT, l'infrastructure de protection antivirale va devoir se complexifier et intégrer de l'analyse en mode comportemental à tous les niveaux du modèle OSI.

L'enjeu des établissements de santé sera d'amener la protection au même niveau que les banques et les telco, et avec la migration d'une partie du SI dans le Cloud, généraliser les solutions de chiffrement.

Il faudra aussi intégrer l'explosion des terminaux : en 2020 il y aura plus de terminaux que d'agents, en 2030 le rapport sera passé à 2 pour 1 voire 3 pour 1. Les smartphones, les MFP et autres caméra IP constituent la prochaine plateforme privilégiée d'attaques.

Il va être nécessaire de déployer la traçabilité généralisée, analyser régulièrement les traces par déploiement d'un SIEM, d'un SOC ou toute technologie qui sera en cours à cette date.

Il va être nécessaire de revoir les processus de recrutement dans le secteur IT, on assiste à la fin des divas techniques : l'ultra compétence technique ne sera

plus suffisante, la culture processus et qualité sera indispensable avec en ligne de mire l'aviation civile.

Il sera nécessaire d'acquérir des outils de déréférencement, de surveillance et de protection de e-réputation : Maltego, XMCO, etc.

Il sera indispensable, et cela va être très complexe à mettre en œuvre, de prendre conscience des exigences croissantes de la patientèle concernant les notions d'accord explicite.

Conclusion

Le lecteur est en droit de se demander pourquoi diable ais-je choisi la date de 2037 pour cible temporelle : pourquoi pas 2040, 2100, 2025 ? La réponse est simple : 2037 est la date de mon départ à la retraite, enfin si Dieu et la CNAV le veulent bien. Et quand je vois tout ce qui va nous tomber dessus et comment on va s'amuser comme des petits fous à déployer et à sécuriser tout cela, j'espère pouvoir repousser un peu, pas vous ?

Parution le 23 octobre 2020

Bibliographie

« Les décisions absurdes », Christian Morel, deux tomes
« Une brève histoire du futur », Michio Kaku
« La mort de la mort », Dr Laurent Alexandre
« Le Big Data, penser l'homme et le monde autrement », Gilles Babinet
« Culturama », Aiden Erez
« La sécurité du système d'information des établissements de santé », Cédric Cartau

La marétique, un enjeu essentiel pour l'humanité ?

COLONEL FLORIAN MANET
Commandant la Section de Recherches de Bretagne, Gendarmerie nationale
Essayiste

La marétique interroge sur la pleine maîtrise par l'homme de cet écosystème numérique complexe. Le capitaine est-il encore maître de son propre navire tant l'internet industriel prospère à bord ?

Le 28 septembre 2020, la CMA-CGM a reconnu avoir été victime d'un rançongiciel, précédant, symboliquement, de quelques jours, l'Organisation Maritime Internationale. En septembre 2018, les ports de Barcelone et de San Diego en Floride ont aussi été perturbés par une cyberattaque. Ainsi, ces exemples illustrent l'actualité de la cybersécurité affectant les acteurs maritimes. Alors s'agit-il d'une manœuvre malveillante coordonnée ciblant l'économie bleue ? Ou bien, le secteur maritime témoigne-t-il d'un déficit de prise en compte de la cybersécurité, s'exposant ainsi à de multiples attaques ?

La *marétique*, néologisme alliant la mer à l'informatique, « désigne l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des activités maritimes, fluviales et portuaires »[1]. La numérisation irrésistible de l'espace maritime accompagne la maritimisation des échanges physiques comme immatériels. Chaque cyber-crise affectant les acteurs maritimes souligne, à sa manière, le caractère stratégique du transport et des ressources maritimes à tel point qu'une marétique sécure ne peut-elle pas être considérée comme une question de survie de l'humanité ?

Ainsi, l'écosystème numérique maritime aiguise les appétits d'organisations criminelles internationales en recherche de profits et de visibilité politiques pour des mouvements terroristes. La prise en otage de données et de services nourrit un capitalisme criminel très prospère. Au total, une marétique sécure

apparaît comme le garant de la résilience de la globalisation et des équilibres interétatiques.

Entre la thalassocratie maritime[2] et les terroristes, les acteurs de la marétique : la marétique, ultime révolution maritime ?

La révolution de la marétique au tournant des années 2000 est comparable à l'apparition du gouvernail ou du GPS. Désormais, le navire est pleinement intégré dans une bulle technologique mondiale qui amarre ce vecteur, jadis totalement indépendant, à un écosystème complexe, celui d'une chaîne logistique mondiale interconnectée.

L'univers mental du marin est aussi bouleversé. Outre les aléas naturels, le suivi mécanique ou l'attention portée aux obstacles à la navigation, il doit désormais intégrer les liaisons numériques. Immatérielle et invisible, cette menace pose problème dans sa prise en compte, car elle est trop souvent résumée à un sujet de sécurité informatique, pré carré de quelques experts.

D'ailleurs, le cadre légal et réglementaire propre au maritime paraît timide sur l'internet des objets et, plus largement, l'internet industriel en comparaison avec d'autres sujets de sécurité maritime (sauvegarde de la vie humaine, pollution maritime).

La marétique est d'autant plus fondamentale que la communauté maritimo-portuaire a tous les atouts pour séduire les cybercriminels. Internationale par construction, l'économie bleue rassemble de très nombreux maillons, certes physiquement distants, mais unis par le digital. Ainsi, l'affrètement d'un conteneur de 20 ou 40 équivalent vingt pieds impose l'échange d'une masse conséquente de données entre au moins une vingtaine d'opérateurs. Sans compter les transactions financières.

La thalassocratie criminelle ou la maritimisation de la criminalité organisée

Les activités maritimes sont une caisse de résonance internationale et une source de profits exceptionnels pour des acteurs malveillants. Ils relèvent de

trois catégories distinctes aux motivations propres : la criminalité organisée ou thalassocratie criminelle quand elle agit en mer, des mouvements terroristes et des États dits « voyous ». Si la première est uniquement mue par l'appât du gain, les deux autres agissent par idéologie et par volonté déstabilisatrice d'une organisation étatique.

Le cyber-malfaiteur est nommé hacker ou pirate. L'analogie avec le monde maritime est riche de sens. Agissant hors des eaux territoriales et hors de toute revendication politique, il illustre le rapport inversé du faible au fort, ce que rend possible le milieu maritime et … le numérique. Un semi-rigide armé par un groupe de pirates peut prendre l'ascendant sur un super tanker affrété par les majors. C'est bien là l'état d'esprit du pirate comme le suggèrent les étymologies grecques qui désigne « un brigand, un bandit qui court les mers pour attaquer les navires » et latine qui enrichit cet héritage de la notion de « tenter sa chance à l'aventure ».

Le nombre de pirates est aussi incertain que celui des attaques perpétrées sur les réseaux et le gain réalisé. L'analyste bute sur un chiffre noir[3] qui dissimule une réalité en expansion.

Un capitalisme criminel se nourrissant de la maritimisation

Un business model fondé sur la valeur ajoutée de la data et du service

Au sein du « capitalisme criminel », ce système économique « gris », tout s'échange et s'achète. Compétences, services, données. À l'image de l'économie réelle, des prestataires (codeurs, hébergeurs, call-center, webdesigner, financiers…) offrent leur service sur le darkweb à des entrepreneurs criminels.

Le paiement de la rançon constitue le fondement de la cyberattaque. Sans lui, le système s'effondre. Il rémunère, certes, l'audacieux pirate mais, plus encore, il justifie et alimente toute une chaîne criminelle à haute valeur ajoutée qui agit en arrière-fond. Crypter, coder et chiffrer des données demeurent un savoir maîtrisé par quelques happy few. Très opportunistes, ces organisations exploitent une faiblesse dans le dispositif de sécurité

numérique. Bien souvent, elles « chalutent » les réseaux à la recherche d'une porte entrebâillée ou non verrouillée. Ainsi, l'économie bleue serait très rarement visée en tant que telle.

L'IT et/ou l'OT au cœur d'une stratégie malveillante

Que les motivations soient criminelles ou politiques, la manière d'opérer consiste toujours à pénétrer, par ruse, effraction ou escalade, les systèmes d'information (IT) ou d'exploitation (OT). Insidieux et discret, le pirate dépose dans un premier temps, une infection sur un système, puis, met en œuvre ses effets (chiffrer, aspirer, contaminer, maîtriser la production d'un service) et, enfin, signe son méfait.

Les cyberattaques sur les acteurs maritimes témoignent d'une grande diversité visant à la fois l'IT (réseaux on shore de l'armement CMA CGM le 28 septembre 2020 ou l'opérateur portuaire MAERSK cible du rançongiciel Not Petya le 27 juin 2017) tout comme les OT (prise de contrôle à distance des fonctions essentielles à la navigation ou au système portuaire, émission d'informations fausses de positionnement…). Ses effets perturbent les opérations à la mer comme à terre, affectant les flottilles comme les infrastructures logistiques.

La marétique, garant d'une globalisation résiliente et de la stabilité internationale ?

Un risque majeur pour la navigation maritime

L'enjeu premier est celui de la sécurité de la navigation maritime dans un contexte de gigantisme des unités du commerce, de la croisière… et de concentration des flottilles sur des autoroutes des mers reliant des hubs internationaux. Les falsifications de positionnement des navires, les prises de contrôle à distance de fonctions essentielles à la navigation génèrent des événements de mer (collision, talonnage, avarie mécanique…) dont les conséquences sont irrémédiables sur l'écosystème maritime (rejet d'hydrocarbures) ou sur la navigation (obstacle à la navigation). La mer amplifie systématiquement les conséquences, dans l'espace comme dans le temps.

Qu'en est-il de l'établissement des responsabilités ? Bien souvent, la réussite d'une cyberattaque repose sur une faute humaine. Même si -admettons le- le hacker agit par ruse ou tromperie, rendant la détection du stratagème très complexe. La marétique interroge sur la pleine maîtrise par l'homme de cet écosystème complexe. Le capitaine est-il encore maître de son propre navire tant l'internet industriel prospère à bord ? Ainsi, émerge, dans le brouillard d'une digitalisation galopante et dans le spectre potentiel du navire autonome ou sans équipage, le concept flou de cyber-navigabilité. En effet, le fréteur doit mettre à disposition de l'affréteur un navire en bon état de navigabilité, ce qui induit des garanties en matière de cybersécurité. Or, un navire dont le système informatique ou l'équipage contreviendrait aux exigences en matière de cybersécurité pourrait-il être considéré comme innavigable ? La gravité de cette interrogation résonne avec les enjeux financiers d'une expédition maritime et de la valorisation du fret transporté.

Le spectre d'un chaos socio-économique

Le transport maritime vecteur de 90 % du commerce constitue le centre de gravité des chaînes logistiques mondiales. Les projets de port connecté ou intelligent ou smart port, conditionnent, en effet, la fluidité des dynamiques d'approvisionnement terrestre en amont comme en aval du navire. Sécuriser l'expédition maritime, c'est donc contribuer à garantir la régularité des approvisionnements d'économies fonctionnant à flux tendus ; c'est fiabiliser l'activité portuaire et l'exploitation des espaces maritimes. C'est in fine contribuer à renforcer la résilience d'économies tributaires du fait maritime. Alors pourquoi ne pas promouvoir une flotte labellisée « cyber-résiliente » au sein des Opérateurs de Service Essentiel afin d'assurer la continuité des approvisionnements stratégiques sous pavillon national ?

Parution le 30 octobre 2020

Les opinions exprimées ci-dessus sont celles de son auteur.
Elles n'engagent aucunement la Gendarmerie nationale.

[1] Livre bleu sur la marétique, 2013
[2] Le crime en bleu, essai de thalassopolitique, Florian MANET, édition NUVIS, 2018
[3] Désigne l'ensemble des crimes qui ne sont pas connus du système pénal et qui échappe à l'investigation et à une réponse pénale faute d'une plainte.

Former à la cybersécurité dans tous les territoires

NICOLAS FORISSIER
Député de l'Indre

Nouveau confinement, nouvelles inquiétudes sur la cyberprotection de nos systèmes informatiques

Rappelons-nous le printemps dernier. À l'annonce du confinement en mars, plus d'un million de Français avaient quitté en une semaine l'Ile-de-France pour rejoindre les autres territoires, selon les données d'Orange. La crise sanitaire changeait ainsi considérablement notre rapport au travail : elle a fait exploser le recours au télétravail. Et le nouveau confinement qui vient de débuter le confirme. Ce changement soudain a concerné l'ensemble de la société - les entreprises grandes et petites, les professionnels libéraux et indépendants, mais aussi l'administration, les collectivités, les établissements de santé, les associations - ont été concernés. Le télétravail s'est généralisé. Mais en parallèle s'est posé et se pose à nouveau de manière accrue le problème de la protection des données, des échanges et des transactions.

Le basculement particulièrement rapide du premier confinement a obligé les entreprises, administrations et collectivités à s'adapter sans toujours pouvoir sécuriser de manière satisfaisante leurs systèmes informatiques. Ainsi, le nombre de cyberattaques de grande ampleur a explosé entre le mois de mars et le mois de juin et tous les domaines ont été touchés : des institutions à la santé en passant par les entreprises.

Le défi de la sécurisation des systèmes informatiques qui pouvait encore sembler une préoccupation éloignée est devenu une réalité quotidienne du monde économique, mais aussi éducatif et scientifique.

La seule façon de répondre de manière concrète et durable à cette réalité est de multiplier les démarches en termes de formation à destination des élus, des entreprises et des administrations afin de couvrir l'ensemble du territoire français et de sa population le plus rapidement possible. Le lancement par le Gouvernement d'une mission de préfiguration d'un Campus de la cybersécurité, en juillet 2019, ne suffit plus. Chaque territoire doit s'armer, en disposant des infrastructures numériques nécessaires, en facilitant l'accueil des entreprises et des professionnels, en offrant des formations complètes aux jeunes au travers d'une variété de diplômes. Car celles et ceux que nous formons auront un rôle majeur au sein de l'entité qu'ils intégreront, pour répondre à des enjeux sécuritaires et stratégiques afin de préserver nos institutions, nos services et nos entreprises.

En effet, l'an dernier, 4 entreprises sur 10 ont été victimes de cyberattaques et le MEDEF indique dans une étude que 20 % des TPE touchées ont subi un préjudice supérieur à 50 000 euros, ce chiffre dépassant les 100 000 euros pour 13 % d'entre elles. On le voit, l'enjeu est colossal. En protégeant le tissu économique français - constitué majoritairement de TPE et PME - nous préserverons l'activité de nos territoires dont l'économie repose largement sur ces petites structures.

Ce tournant majeur ne peut être opéré qu'en demandant à l'État et aux collectivités d'être moteurs dans cette transition. Nous devons nous saisir du sujet, et je veux pour cela saluer l'initiative lancée à Aurillac en septembre 2019 de la création d'un DUT faisant la part belle à la cybersécurité. C'est dans ce sens que je travaille depuis deux ans, en préparant la création d'une École d'Ingénieurs spécialisés en cybersécurité à La Châtre, dans l'Indre, afin de former de futurs cadres capables de gérer des crises de grande ampleur. Il est important que les collectivités locales s'engagent activement dans ce type de projets, afin d'apporter une palette de formations plus large que celles proposées par les entreprises privées.

Le Conseil de l'Europe avait souligné dès 2001 l'importance cruciale de répondre à la menace toujours croissante des cyberattaques. Vingt ans plus tard, où en est-on ? Il est urgent d'obtenir la mobilisation des acteurs

publics et privés pour développer les réponses adéquates en matière de cybersécurité, avec des formations présentes dans les territoires ruraux comme dans les métropoles, démontrant ainsi que c'est toute la France qui avance dans ce domaine crucial pour l'avenir.

Parution le 6 novembre 2020

La cybersécurité a besoin de femmes, et les femmes ont toute leur place dans la cybersécurité

NACIRA SALVAN
Présidente
CEFCYS

Alors que l'histoire de l'informatique repose sur d'illustres pionnières, les stéréotypes persistent dans ce secteur et privent notamment la filière de la cybersécurité, en pleine expansion, de nombreux talents féminins.

D'après les études ISC2, les femmes ne représentaient que 11 % des emplois dans cette filière dans le monde en 2013. Sept ans plus tard, elles représentent près d'un quart de la main-d'œuvre en cybersécurité. C'est très encourageant et prometteur, cependant, le chemin reste encore long avant d'arriver à une véritable parité dans un domaine qui évolue constamment, et qui offre des carrières stimulantes et intéressantes.

Constats

En dix ans, le nombre de professionnels spécialisés en cybersécurité a doublé. Aujourd'hui, ils sont plus de 4,5 millions dans le monde à lutter contre des menaces cyber de plus en plus complexes, sophistiquées et qui réussissent. Des cyberattaques qui explosent en cette période de crise sanitaire liée à la COVID-19. Pour faire face à ces menaces, les entreprises peinent à trouver les ressources spécialisées dans la cybersécurité.

Malgré ce besoin sans cesse croissant de nouveaux experts dans ce secteur en pleine croissance, où les opportunités sont là et les salaires très attrayants, les femmes sont peu nombreuses. Le fait qu'il subsiste une pénurie de talents laisse à penser que d'autres facteurs empêchent les femmes de s'impliquer.

Comment expliquons-nous cette sous-représentativité des femmes dans un des domaines du numérique les plus dynamiques et les plus passionnants ? Voici quelques-unes des principales raisons :

La figure de l'adolescent au sweat à capuche qui pirate une multinationale depuis sa chambre reste ancrée dans les esprits

La cybersécurité est un domaine transverse, essentiel pour protéger le patrimoine numérique de l'individu, les entreprises et administrations, ainsi que l'État.

Et pourtant, la filière est méconnue et mal jugée.

Ce manque de connaissances et de sensibilisation aux métiers de la filière est l'une des raisons de la pénurie de femmes dans ce domaine. En effet, nombreux clichés sont toujours présents dès qu'on parle de cybersécurité : c'est une filière purement technique, c'est un métier de geek, ce n'est pas un métier pour les femmes… Tous ces clichés par méconnaissance font fuir toute initiative de s'impliquer dans ce domaine.

L'organisation, la culture et la place de la femme dans l'entreprise

Le manque d'équilibre entre la vie professionnelle et la vie personnelle est l'un des freins qui touchent et affectent l'évolution de carrière de toutes les femmes au-delà des métiers du numérique. À noter l'aspect positif de la pandémie de la COVID-19 qui a placé de nombreux hommes et femmes en télétravail, mettant ainsi en évidence des défis importants de l'équilibre entre la vie familiale et professionnelle.

Par ailleurs, plusieurs études montrent une différence significative de salaire entre les hommes et les femmes dans des emplois du numérique, dont en cybersécurité. J'ai moi-même été confrontée à cette situation lors de mon arrivée dans une structure la même semaine qu'un homme pour le même poste. Alors que j'avais plus de certifications, de qualification et d'expérience, mon salaire était inférieur de 20 % par rapport à mon collègue. Quand j'ai demandé des explications sur cette différence à notre supérieur, il m'a répondu : « il a su négocier ! ».

Le manque de modèle féminin dans les métiers du numérique

De façon globale, les filières du numérique souffrent cruellement de la persistance de stéréotypes de genre, ainsi que de l'absence de modèle féminin.

De même, l'attractivité des métiers de la cyber pâtit d'un manque de modèles féminins dans lesquels les lycéennes et étudiantes peuvent s'identifier. Ainsi, dans une filière où peu de femmes exercent, les jeunes filles peuvent avoir l'impression que ces métiers ne sont pas pour elles.

Le besoin de prouver sa valeur deux fois plus qu'un homme

Le problème du « mansplaining » et de l'ensemble des discriminations s'exerçant à l'encontre des femmes dans le domaine de la cybersécurité, entraîne qu'ils finissent aussi par décourager les principales intéressées. À force de voir leur travail dévalorisé et sans perspective d'évolution au sein de leur entreprise, de nombreuses expertes se sous-estiment, voire, refusent d'intégrer ce secteur.

J'ai fini par être acceptée dans une équipe d'hommes où j'étais leur cheffe quand j'ai tiré les câbles sous les faux planchers, brassé des baies réseaux, assuré des astreintes techniques la nuit…

Comment améliorer la place de la femme dans ce secteur ?

Combattre les stéréotypes le plus tôt possible

Dans ce secteur, le système éducatif n'incite pas les jeunes filles à s'orienter vers les métiers du numérique. Les écoles et les universités entretiennent encore trop souvent des clichés. Elles mettent peu en avant les modèles féminins, auxquels peuvent s'identifier les femmes.

Dès le plus jeune âge, il existe une perception inégale des programmes de sciences, de technologie, d'ingénierie et de mathématiques. Ces filières sont présentées aussi bien aux garçons et qu'aux filles, cependant les

garçons sont plus encouragés à poursuivre une carrière dans ces domaines. Donc, si l'on souhaite avoir plus de femmes dans les métiers du numérique et notamment dans la cybersécurité, il faut commencer par revoir les discours et les stratégies d'orientation dans le système éducatif pour les jeunes filles. Il faut mettre en œuvre tous les moyens pour encourager les jeunes filles à explorer les études dans les technologies et les mathématiques, et les pousser vers les cyber-carrières afin de rendre les professionnels de demain plus autonomes.

Encourager et explorer les opportunités d'apprentissage

Le faible nombre de femmes dans la cybersécurité montre la nécessité pour les femmes de se mettre en réseau sur le terrain. Partout dans le monde, des organisations s'efforcent de réduire l'écart entre les sexes en connectant et en soutenant les femmes dans la cybersécurité. Ces organisations permettent aux femmes de rejoindre des groupes, d'assister à des conférences, de poursuivre leurs études et d'explorer de nouvelles possibilités en matière de cybersécurité.

Les organisations offrent également des moyens de se connecter avec les leaders de l'industrie et de trouver des mentorats. Un mentor peut être une source fiable d'orientation, d'accompagnement et de réseautage. Les mentors peuvent également fournir les leçons tirées de leurs propres expériences passées.

Ouvrir la voie aux les femmes et attirer plus de femmes vers la cybersécurité

Pour attirer plus de femmes vers la cybersécurité, les gouvernements, les organisations à but non lucratif, les associations professionnelles et commerciales, et le secteur privé doivent travailler de concert.

Attirer davantage de femmes dans le domaine de la cybersécurité nécessite des efforts conjoints dans le recrutement, l'accompagnement et l'évolution de carrière... Ainsi, les offres d'emploi en cybersécurité doivent être rédigées de manière à ce que les femmes professionnelles se sentent les bienvenues. Les efforts de recrutement devraient se concentrer sur les

établissements universitaires à forte présence féminine. Les entreprises devraient veiller à ce que les employées considèrent la cybersécurité comme une opportunité pour les changements de carrière internes. Enfin, le gouvernement devrait collaborer avec le secteur privé et les établissements universitaires pour intéresser plus de jeunes filles aux métiers du numérique, et en particulier la filière de la cybersécurité.

Les engagements du CEFCYS

Le CEFCYS (Cercle des Femmes dans la Cybersécurité), association loi 1901 créée en 2016, est né d'une conviction : l'augmentation de la proportion des femmes dans le secteur de la Cybersécurité devient un enjeu sociétal, économique et souverain.

Le CEFCYS est un mouvement associatif porté par une dynamique collective où les valeurs partagées sont l'humanité, l'éthique, la confiance, l'esprit collectif, le respect et l'engagement pour soutenir et aider la communauté.

Le CEFCYS regroupe des femmes travaillant dans le domaine de la cybersécurité ainsi que toutes celles qui aspirent à y travailler. C'est une association également ouverte aux hommes ! Ils sont nombreux à l'avoir rejointe depuis sa création pour aider dans l'accomplissement de ses objectifs, notamment le mentorat et la formation.

Les adhérentes du CEFCYS ont des profils de femmes expérimentées dans le secteur de la sécurité du numérique : RSSI et Adjointe RSSI, Chef d'entreprise, Avocate, DPO, Consultante, Analyste Cybersécurité, Cryptographe, Experte, etc. Le CEFCYS est également composé d'étudiantes. Des femmes en reconversion professionnelle rejoignent également le CEFCYS pour être accompagnées et réussir leur nouvelle orientation vers les métiers de la cybersécurité.

Les objectifs du CEFCYS peuvent être résumés en 4 grands volets :

- Sensibiliser le grand public et plus particulièrement les femmes, les entreprises, les partenaires éducatifs, les recruteurs à l'importance de la parité homme/femme et à la diversité dans le domaine de la

Cybersécurité, et ainsi faire progresser la présence et le leadership des femmes.

- Valoriser et professionnaliser les compétences des femmes dans le domaine de la Cybersécurité via des groupes de travail, du mentorat, des publications, de rapports…

- Organiser des évènements et conférences rassemblant les femmes travaillant ou aspirant à contribuer au domaine de la Cybersécurité pour :
  - favoriser les échanges, la collaboration et les retours d'expérience ;
  - contribuer au développement du réseau des femmes travaillant ou aspirant à travailler dans la sécurité des systèmes d'information.

- En action sociétale, le CEFCYS contribue à la sensibilisation du grand public à l'usage sécurisé du numérique.

Au-delà de ces 4 objectifs, depuis quatre ans, de nombreuses actions de terrain sont accomplies par les bénévoles et les partenaires engagés auprès du CEFCYS, notamment à travers des interventions dans les collèges, lycées et salons pour les étudiants, l'organisation de webinars (dont 6 se sont déjà tenus durant le confinement) traitant de divers sujets de la cybersécurité, de salons virtuels de recrutement (job dating), etc.

Enfin, l'ambition future du CEFCYS est orientée vers l'éducation et la formation afin de répondre un enjeu majeur et stratégique : celui de la pénurie de compétences et de ressources humaines dans les métiers de la Cybersécurité. Nous souhaitons instruire et porter un projet de création d'un centre de formation en cybersécurité destiné à accompagner les femmes vers la spécialisation dans les métiers techniques.

Le livre « Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité » : guide des métiers, formations et opportunités dans la cybersécurité »

En décembre 2019, le CEFCYS a édité un livre, « Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité » : guide des métiers, formations et opportunités dans la cybersécurité », désormais reconnu par

de nombreux spécialistes comme un livre « d'utilité publique ».

Ce livre, d'une approche inédite, est un plaidoyer en faveur des métiers et des parcours de formation, dès le collège et tout au long de la vie professionnelle. Il s'adresse aux lycéen(ne)s et étudiant(e)s, aux parents soucieux de l'avenir de leurs enfants, aux enseignants, aux professionnels de l'orientation, aux salarié(e)s en reconversion… pour leur permettre de mesurer tout l'intérêt de la filière.

L'ouvrage propose une boîte à outils inédite pour découvrir l'univers cyber, pour comprendre les parcours de formation possibles avant même les choix sur Parcoursup, ou pour alimenter un projet tout au long de la vie professionnelle. Ce guide contient une foule d'informations pour faire apprécier la cybersécurité… loin des clichés habituels.

Nous avons également mis en lumière dans ce livre 23 témoignages de CyberWomen, en résonance avec notre vocation de promouvoir les femmes, et d'être en mesure de proposer à celles qui aimeraient rejoindre ce secteur des « rôles modèles » inspirants. Ces 23 cyberwomen auxquelles s'identifier ont des profils d'horizons, de secteurs et d'expériences divers. Certaines ont choisi les métiers de la sécurité dès leur formation initiale ; d'autres les ont découverts au cours de leur vie professionnelle et ont élargi leurs compétences initiales.

Le trophée de la femme cyber

Mardi 27 octobre 2020, lors du 9ième colloque du CEFCYS, se tenaient les premières remises de « Trophée des femmes cyber ». Cet événement visait à valoriser et à récompenser des femmes exerçant dans les métiers de la cybersécurité, ainsi qu'à remettre une série de prix qui reconnaissent et honorent les réalisations, la valeur et les contributions des femmes dans la filière. C'était une occasion et une opportunité nécessaires pour mettre en lumière et honorer les femmes et les jeunes femmes qui atteignent des objectifs dans ce qui a toujours été une industrie à prédominance masculine.

Des personnalités reconnues représentant les principales organisations et associations dans l'écosystème cyber en France ont délibéré pour désigner, parmi 191 candidates, les 7 lauréates dans les catégories « Femme dirigeante ou entrepreneure », « Femme Cyber Professionnelle », « Femme Cyber Fonctions supports », « Femme Cyber étudiante », « Femme Cyber Coup de Cœur du Jury » et « Femme Cyber Coup de Cœur du CEFCYS ».

Les candidatures étaient toutes excellentes et chacune méritait un trophée. Un des membres de jury a fait remarquer à juste titre que les organisateurs d'évènements ne peuvent plus justifier l'absence de femmes dans leurs tables rondes et leurs conférences par le manque de cyberwomen.

Conclusion

Pour encourager plus de femmes à s'engager dans les métiers de la filière de la cybersécurité, j'aimerais apporter quelques conseils.

Il faut en finir avec l'autocensure : lancez-vous, tissez votre réseau professionnel ! Le mentorat, notamment au CEFCYS, peut vous aider et vous accompagner dans l'apprentissage et l'émancipation. Rien n'est terminé, quel que soit votre âge. Certaines me disent qu'à 45 ou 50 ans leur chance est passée, je réponds NON. La cyber offre des possibilités de rebondir, tant les évolutions du secteur sont rapides et tant il peine à recruter. Ne vous interdisez rien, ne restez pas dans votre coquille ! La révolution cyber doit aussi embarquer une prise de conscience et une révolution culturelle et comportementale.

Ne pas se laisser intimider : il faut prendre le risque et se lancer. Certes, le domaine est dominé par les hommes, mais allez-y et exigez le respect et l'égalité. Il faut arrêter de se sous-estimer, et il faut avoir confiance en ses compétences quand on arrive dans un milieu d'hommes.

Apporter des témoignages de réussite pour encourager les autres : cela peut aider celles qui n'osent pas prendre la parole à se découvrir. Assistez aux conférences, travaillez votre réseau également en interne dans l'entreprise, et cherchez les meilleures opportunités pour évoluer. Osez postuler à des postes de RSSI, ils ne sont pas réservés aux hommes ! Osez

prendre la parole, et exprimez vos convictions ! Engagez-vous et engagez-vous tôt. Découvrez quelle est votre passion. Commencez à apprendre. Qu'il s'agisse d'un hackathon ou d'un défi de cybersécurité, comme une capture du drapeau ou un CyberStart…

Engagez-vous et commencez à apprendre. Voilà la meilleure façon.

Parution le 20 novembre 2020

Cybersécurité : des Hommes de bonne volonté contre le temps qui passe…

FABIEN MIQUET
Product & Solution Security Officer
Siemens Digital Industries France

« Et à chaque fois qu'il y a du temps qui passe, il y a quelque chose qui s'efface » écrivait Jules Romains dans *Les Hommes de bonne volonté* (1932-1946). Alors certes, il visait à travers le récit de destins croisés à dresser un tableau de l'évolution de la société moderne au début du XXème siècle quand il écrivit ces lignes… Néanmoins, transposons cette citation dans notre époque en l'appliquant au monde de la cybersécurité et elle pourrait bien faire du père de l'unanimisme un réel visionnaire !

En effet, le couple Homme-Temps est sans doute celui qui résume le mieux à lui seul la problématique qui me passionne et façonne mon quotidien depuis plus de vingt ans…

L'Homme, d'abord

Bien évidemment. Car malgré l'Intelligence Artificielle, le Big Data et la digitalisation accélérée de notre société, l'Homme restera toujours au cœur de la décision et en particulier acteur de la menace cyber. J'ai souvent utilisé, lors de séances de formations formelles ou même dans le but de sensibiliser mes collaborateurs autour de la machine à café – soit dit en passant le meilleur lieu d'évangélisation qui soit et qui nous manque en ces temps contrariés ! – l'image de la passoire afin d'illustrer le caractère asymétrique de cette menace : un système, quel qu'il soit, peut être symbolisé par une passoire, plus ou moins trouée selon le système considéré, sa maturité, celle de ses « utilisateurs », etc. Le cyber défenseur devra alors s'efforcer de boucher en permanence avec ses dix doigts la totalité des trous, quand un attaquant n'aura qu'à exploiter à un moment donné qu'un seul relâchement de la pression d'un auriculaire sur

l'un des orifices pour s'engouffrer dans la brèche… Injuste n'est-ce pas ? Mais le monde est ainsi fait et celui de la cyber n'échappe pas à la règle. On y retrouve d'ailleurs le meilleur, mais aussi le pire de l'être humain et ses vices sont une source inépuisable de vecteurs d'attaque et de motivations pour les mal intentionnés : comprendre *Vénalité, Idéologie, Compromission & Contrainte, Ego, Sabotage & Sexe*… Cet acronyme, au passage, n'a rien de nouveau, puisqu'il dérive de son équivalent anglo-saxon, le fameux *MICE* ou « piliers de la manipulation » : *Money, Ideology*, Compromise & Coercion, Ego et résume à l'origine les leviers que les services de renseignements actionnent pour corrompre agents et citoyens d'un pays étranger. Néanmoins, et afin de ne pas noircir davantage le tableau, terminons sur une note positive, car même s'il est souvent cité, et il faut le reconnaître à raison, comme étant parfois le maillon faible de la chaîne, l'Homme peut (et doit !) aussi devenir le meilleur garant de sa sécurité. Sensibilisations et plus encore formations doivent rester en première ligne de notre arsenal de défense : quels sont les risques cyber ? Pourquoi cela n'arrive pas qu'aux autres ? Pourquoi suis-je aussi une cible potentielle ? Quelles sont les bonnes pratiques et les bonnes réactions au moindre doute ? Il est également bon de rappeler, dans le cadre de certains milieux sensibles, que la négligence dans le monde numérique et virtuel vaut malveillance et qu'elle peut conduire à des sanctions pénales, pour le coup, bien ancrées dans le monde réel…

Ainsi, le facteur humain est, et restera omniprésent, qu'on soit défenseur ou attaquant, victime collatérale ou simple témoin des dérives du cyberespace… Et si l'argent est souvent énoncé comme étant le nerf de la guerre, et ce n'est pas l'expert cyber peinant souvent face à son décideur à remplir la case « Retour sur investissement du budget demandé ? » qui dira le contraire, la maîtrise du temps est une des clés menant à la victoire.

La grandeur Temps, ensuite

Définitivement, l'année 2020 ne ressemblera à aucune autre. Mais n'oublions pas, elle aura également marqué les dix ans de Stuxnet, ce ver s'étant attaqué aux centrifugeuses iraniennes d'enrichissement d'uranium. Définitivement, chez Siemens, il y aura eu un avant et un après Stuxnet en matière de cybersécurité. Certes le groupe en 2010 n'était pas novice en la matière, loin de là et on retrouve trace de la prise en compte de la « Sécurité des Systèmes

d'Information » appliquée aux systèmes industriels jusqu'à 25 ans en amont, avec notamment la mise en place des premiers contrôles d'accès par mots de passe sur des switchs du constructeur allemand. Autant dire à une époque où l'on faisait, tel Monsieur Jourdain, de la cybersécurité industrielle sans le savoir !

Mais à partir de 2010, tout s'est accéléré. Une prise de conscience mondiale était née, et avec elle une organisation cyber dédiée (on y revient : « l'Homme, d'abord ! »), forte de 1 500 personnes au niveau mondial visant à maintenir au quotidien la pression sur autant de dizaines de doigts pour reprendre la métaphore précédente. Parmi ces cyber-combattants, une équipe en 365/24/7, le ProductCERT Siemens, qui a pour rôle, entre autres, le traitement des alertes et réaction aux cyber-attaques et la gestion des vulnérabilités. Celles sur les produits du groupe, bien évidemment, mais pas seulement, également sur ceux de ses partenaires et de manière générale sur les logiciels que l'on va pouvoir retrouver dans les usines. Ce ne sont pas moins de 53 000 références qui sont gérées actuellement par les experts au quotidien.

L'après Stuxnet, c'est aussi une volonté de monter drastiquement son niveau de maturité et proposer des équipements sécurisés dignes de ce nom avec une gamme complète d'automates programmables, les S7-1500, qualifiés par l'ANSSI, en 2016 d'abord, puis maintenus en qualification en 2019 ensuite. Une qualification n'est jamais qu'une démonstration de robustesse et de confiance que l'on soumet aux autorités, et la décrocher est déjà en soit une belle prouesse. Rappelons d'ailleurs que, souvent convoitée, aucun autre automate à ce jour n'a réussi à se hisser à la hauteur du S7-1500, même près de cinq ans plus tard. Un maintien en qualification va encore plus loin : par rapport à la qualification initiale, démonstration doit être faite de quelles sont les modifications du firmware effectuées (analyse d'impacts), quelles sont les vulnérabilités potentiellement publiées sur la période écoulée, et surtout ont-elles bien été toutes corrigées… En quelque sorte, un maintien en qualification, c'est faire une démonstration de la confiance dans le temps qui passe.

Mais Stuxnet, dix ans après, c'est aussi le reflet d'une persévérance, celle de conserver son rôle de pionnier, de promoteur, encore et toujours, avec

trois nouvelles qualifications ANSSI décrochées et officialisées par Siemens il y a quelques semaines à peine, cette fois pour ses automates redondants, qui illustrent parfaitement l'alliance entre sûreté et cybersécurité. Cette dualité est intéressante tant la frontière entre les deux mondes est perméable et demande souvent aux experts de jouer les funambules sur celle-ci. Tantôt antagonistes (par exemple, j'ajoute un équipement réalisant une fonction « pure cyber », il peut lui aussi tomber en panne, je défiabilise donc mon système dans sa globalité), tantôt collaboratifs (au service d'un objectif commun : la disponibilité !), « safety » et « security » demandent d'apprivoiser le temps. En effet, vaste problème que celui des mises à jour pour ne citer que lui, quand l'informaticien ne jure que par le « PASAP », comprendre le *Patch As Soon As Possible*, et l'automaticien de lui répondre « PAS TOUCHE » à mon système, il fonctionne, la production avant tout et la sécurité ensuite… un grand écart temporel pour un choc des cultures un brin caricatural, mais pourtant encore bien réel de nos jours !

Une bataille perpétuelle

Ainsi va la vie d'un système industriel aujourd'hui, avec ses hommes et ses cultures qui ont tendance à converger moins rapidement que les technologies de l'IT et de l'OT ! Sans la compétence, j'entends par là si nous n'arrivons pas à mettre autour de la table les gens des métiers, les gens de la sécurité, les gens des process et dans l'idéal aussi des profils hybrides facilitant la discussion entre tous, c'est peine perdue, nous n'avancerons pas. Heureux celui qui arrivera à dompter le temps et la progression de ses niveaux de sécurité au cours de celui-ci : celui de ses produits, de ses process, de ses hommes, pour son simple bénéfice d'abord, mais aussi pour celui de ses clients ensuite. Inspirer la confiance n'est pas quelque chose qui se décrète, mais qui se démontre… avec le temps.

Heureux encore celui qui trouvera réponse, au juste besoin, à l'orthogonalité entre sûreté et sécurité, qui passe sans aucun doute par une analyse des risques régulièrement reconsidérée et des objectifs bien ciblés : « ce que tout bien considéré, je décide de protéger et contre quoi ». La cybersécurité est en effet de ces disciplines qui exigent une remise en question permanente et une humilité à toute épreuve : qui se vante d'être

invulnérable un jour sera confondu en menteur un autre jour, juste une question… de temps !

C'est donc par cette image d'une bataille perpétuelle, et en hommage à tous nos Hommes de bonne volonté, classe à laquelle vous appartenez sûrement si vous lisez ces quelques lignes, que nous fermons cette parenthèse comme nous l'avons commencé, avec Jules Romains à peine adapté pour l'occasion, et gardons à l'esprit cette sainte maxime :

« À chaque fois qu'il y a du temps qui passe, mon niveau de sécurité s'efface »…

Parution le 27 novembre 2020

Lancement de la Fédération Française des Professionnels de la Blockchain : créons des alliances pour retrouver notre autonomie stratégique sur les questions technologiques

JEAN-MICHEL MIS
Député de la Loire

Le soutien aux technologies de rupture est une nécessité pour préserver notre souveraineté. C'est en favorisant la création d'écosystèmes porteurs et en aidant nos acteurs économiques à se structurer que nous regagnerons en France et en Europe « *notre autonomie stratégique* » comme le rappelait récemment le Président de la République[1].

C'est tout l'objet de la Fédération Française des Professionnels de la Blockchain dont l'objectif est de mettre en relation les acteurs privés travaillant sur ce sujet afin qu'ils parlent d'une seule voix au niveau national et européen.

Particulièrement investi sur la blockchain depuis plusieurs années, que ce soit en tant que rapporteur de la mission d'information parlementaire qui a rendu ses conclusions en 2018 à l'Assemblée nationale, qu'en tant que co-fondateur et Président d'honneur de la Fédération Française des Professionnels de la Blockchain, je me réjouis de voir que ce sujet progresse aux niveaux national et européen. Néanmoins, nous devons aller plus loin pour structurer nos initiatives sur deux points.

D'abord dans le champ économique où, après avoir raté le virage de la nouvelle économie dans les années 2000, nous devons agir rapidement dans la course aux innovations de rupture face à nos concurrents américains et chinois. La création d'un cadre réglementaire favorable à l'innovation et le lancement d'une stratégie industrielle ont vocation à combler cet écart.

Ensuite dans le champ monétaire, où plusieurs banques centrales mettent en place leurs propres monnaies digitales pour prendre de vitesse le projet de cryptoactif Libra initié par Facebook. L'euro numérique permettrait à la France et à l'Europe de disposer, avec un temps d'avance sur l'étranger, d'un puissant levier d'affirmation de souveraineté[2].

Je suis convaincu que la question de notre souveraineté dans l'espace numérique est décisive pour les années à venir. C'est la raison pour laquelle, en tant que Président d'honneur de la Fédération Française des Professionnels de la Blockchain, j'appelle à faire de la blockchain l'un des piliers de notre stratégie économique et monétaire.

La première étape pour soutenir le développement de la blockchain est de créer un cadre législatif et réglementaire favorable à l'innovation et de formaliser une stratégie industrielle pour les technologies de rupture.

C'est d'abord en établissant un cadre juridique clair que nous permettrons à nos entrepreneurs de recourir à la blockchain et sécuriserons les investisseurs qui soutiennent l'essor de cette technologie.

Le Secrétaire d'État au Numérique Cédric O le rappelait lors de la réunion de lancement de la Fédération Française des Professionnels de la Blockchain[3] : cette technologie incarne la manière dont se développe l'innovation et la manière dont les pouvoirs publics interagissent avec elle. Alors qu'au départ les innovations de rupture bousculent l'ordre établi, elles ont ensuite vocation à s'insérer dans un cadre institutionnel qui en permet le développement.

La France a été particulièrement exemplaire en la matière : elle a su mettre très tôt en place un cadre juridique favorable à l'essor de la blockchain pour renforcer notre attractivité et améliorer la compétitivité de nos entreprises à l'international. Ainsi le cadre juridique français a été progressivement clarifié pour permettre aux entrepreneurs d'utiliser la blockchain sans casser la dynamique d'innovation. Par exemple avec la loi PACTE, nous avons instauré un cadre pour les levées de fonds par émissions de jetons afin de sécuriser les émissions et de garantir l'intégrité

du marché en fournissant une information fiable aux investisseurs.

L'évolution de la réglementation dans un sens favorable aux technologies de rupture est un véritable enjeu pour renforcer l'attractivité de la France à l'international. Il existe en effet une forte concurrence. La Chine a par exemple très clairement annoncé son intention de devenir leader sur la blockchain et aménage son cadre juridique pour soutenir des acteurs chinois.

C'est pour répondre à cet enjeu que j'ai préconisé à l'Assemblée de mener une revue générale des normes qui conditionnent encore l'essor de la blockchain.

Mais créer un cadre juridique favorable est insuffisant. Nous devons aussi aller plus loin en mettant en place une stratégie industrielle aussi bien en France qu'au niveau de l'Union européenne afin de favoriser le développement de la blockchain.

La stratégie nationale blockchain répond en partie à cet objectif, en créant un écosystème alimenté par des financements publics de soutien à la R&D sur le modèle de l'intelligence artificielle. Dans le même sens, pas moins de sept milliards ont été annoncés sur les technologies de rupture dans le cadre de France Relance.

Si je salue l'ensemble de ces initiatives, elles sont encore insuffisantes pour permettre à la France de se positionner comme *leader* sur la blockchain au niveau international et ainsi retrouver sa souveraineté. C'est à nous d'encourager le développement de solutions souveraines sur blockchain avec des infrastructures régaliennes et d'aider nos acteurs économiques à émerger. La Fédération Française des Professionnels de la Blockchain devrait en être un des éléments moteurs. Elle est, en effet, un moyen unique d'unir nos forces afin qu'ensemble, nous facilitions la croissance et l'expansion de nos entreprises tout en partageant une vision commune de la blockchain. Cette vision, je la partage avec Rémy Ozcan, président de la Fédération Française des Professionnels de la Blockchain et l'ensemble de nos partenaires économiques.

C'est également un enjeu décisif en matière monétaire, où il en va de la survie de notre gouvernance publique face aux GAFAM.
Si nous voulons soutenir l'essor de la blockchain nous devons concurrencer les initiatives privées comme le Libra en créant en premier une monnaie digitale de banque centrale pour renforcer notre souveraineté.

L'annonce du lancement du Libra, un cryptoactif privé qui a pour objectif de servir de moyen de paiement sur les applications du groupe Facebook, a été très critiqué au niveau international au cours de l'année 2019.
Le G7 et les gouvernements européens ont refusé en bloc le déploiement du Libra dans les conditions actuelles et rappellent aujourd'hui leur attachement à la souveraineté monétaire.

J'avais en ce sens interpelé Bruno le Maire en juin dernier sur les dangers du Libra. En effet si différents risques ont toujours été associés à l'existence de monnaies digitales privées, leurs récents développements technologiques (les *stablecoins*) impliquent des menaces spécifiques.

Le rapport présenté par Benoit Coeuré met en avant un risque systémique pour la stabilité des monnaies et une menace particulière en matière de blanchiment d'argent. Plus encore, ce sont les risques en matière de souverainetés monétaires qui alertent les gouvernements et les organisations internationales.

C'est pour freiner ces initiatives privées qui menacent notre souveraineté que les banques centrales mettent en place leurs propres monnaies numériques sous forme de monnaie digitale de banque centrale.

Il existe plusieurs projets de ce type au niveau international. Aux États-Unis le lancement de *Fedcoins* convertibles à parité avec le dollar est envisagé par la FED. Le projet de renminbi numérique est un élément déterminant de l'internalisation monétaire de la Chine.

En France la Banque de France a lancé en janvier 2020 son premier appel à projets pour expérimenter une monnaie digitale de banque centrale. Il s'agit du premier test d'envergure pour une monnaie digitale de gros, c'est-

à-dire destinée au secteur financier. Les résultats permettront en outre à la France de contribuer à la réflexion plus globale conduite par l'Eurosystème sur la mise en place d'un euro numérique à l'échelle européenne.

Nous avons aujourd'hui la possibilité de rebattre les cartes sur la blockchain en imposant de nouvelles règles qui s'accorderont mieux avec nos intérêts économiques et stratégiques et nos valeurs. Les acteurs français de la blockchain doivent être moteurs sur le développement d'infrastructures régaliennes indispensables au developpement d'une blockchain souveraine et à la mise en place d'une monnaie numérique de banque centrale européenne.

Parution le 4 décembre 2020

[1] Une conversation avec le Président français dans Le Grand Continent 16 novembre 2020 : https://legrandcontinent.eu/fr/2020/11/16/macron/

[2] Discours de François Villeroy de Galhau Gouverneur de la Banque de France, 4 décembre 2019 : https://www.banque-france.fr/sites/default/files/medias/documents/2019.12.04_conference_acpr_v5.pdf

[3] Retransmission de la première réunion de la Fédération française de la blockchain sous le patronage de Cédric O : https://www.federation-blockchain.fr/accueil/

De l'Ethique européenne à l'avènement de l'ère Post-pragmatique[1]

ALICE LOUIS
Data Governance Consultant, Cyber Ethics Teacher,
Legal Advisor, European Expertise Work (EEEI)

Du fait de son caractère universel et intemporel, l'éthique a été questionnée tout au long des époques au gré des influences morales, politiques et religieuses.

Elle se définit comme étant **la pensée des principes** en raisonnant sur les fondements et les valeurs[2] y afférents.

Toutes les théories de l'Ethique sont issues de l'histoire de la philosophie morale[3]. En premier lieu, **l'Ethique normative** élabore des théories qui permettent d'évaluer moralement les personnes et leurs actions selon les critères du « juste » et du « bien ». Il est à noter que le débat central de l'éthique normative englobe trois courants[4] : l'éthique de la vertu, le déontologisme, ainsi que le conséquentialisme qui considère que l'éthique est un acte de responsabilisation[5].

En deuxième lieu, la **Méta-éthique** étudie les fondements conceptuels, épistémologiques et ontologiques de l'éthique normative.

Enfin, **l'Ethique appliquée**[6], qui comme son nom l'indique, applique les normes de l'éthique normative à des contextes pratiques, en particulier, à celui du numérique où les développements de l'intelligence artificielle (IA) comportent de nombreux enjeux.

Dès 1948, avant l'invention du jeu de l'imitation par **Alan Turing**, le philosophe et mathématicien américain **Norbert Wiener** publiait un ouvrage dans lequel il présentait un ensemble d'idées relatives au

développement de technologies capables de remplacer certaines fonctions mentales de l'être humain[7].

Depuis la théorisation de la cybernétique et les prémices du connexionnisme ainsi que ceux du cognitivisme, de nombreux défis scientifiques ont été relevés. En particulier, la naissance de processeurs très puissants et **l'émergence du Big Data** ont permis des avancées considérables dans le domaine de l'IA.

Néanmoins, cette dernière présente encore d'importantes zones d'ombre. En effet, il apparaît que la fiabilité des algorithmes est fréquemment discutable (fragmentation, discrimination, exclusion, etc.).

Par ailleurs, s'agissant « *des algorithmes issus du paradigme de réseaux de neurones artificiels, en particulier, de* ***l'apprentissage profond*** » il est souvent impossible pour les ingénieurs d'expliquer le résultat produit.[8]

En outre, **l'agencement des algorithmes de l'IA** peut correspondre à un ordre socio-économique sous-jacent. Rappelons que « *la stratégie de captation de l'attention* » développée de manière industrielle par les Big Tech utilise des biais comportementaux[9].

Aujourd'hui, les domaines d'influence de l'éthique sont multiples. Elle peut, entre autres, remplir une fonction visant à évaluer la justesse des règles que le droit et la conformité édictent ainsi que les préfigurer. Il en ressort, en toute hypothèse, que **l'éthique impulse une véritable dynamique d'intelligence juridique au sein même des organisations, et, plus globalement, au niveau international.**

Les 99 articles et les 173 considérants du RGPD, qui traduisent une volonté de responsabiliser les entités (celles-ci doivent veiller à préserver leur équilibre économique tout en intégrant une démarche éthique), en sont une première illustration et les prochains mois vont offrir **une formidable occasion aux DPO bien coachés de démontrer tout leur talent ainsi que leur agilité dans ce domaine.**

L'année 2021, en effet, « *annonce la fin du moratoire de la CNIL pour la*

réalisation des analyses d'impacts devant être diligentées pour tous les traitements à risques conformément à l'article 35 du RGPD ».[10] Aussi, après avoir élaboré la cartographie des traitements, formalisé leur registre, vérifié les 4832[11] points de conformité et déterminé la doctrine de l'entreprise (s'agissant de « l'intérêt légitime »), les DPO devront se concentrer sur la « ***vague d'audits*** *de conformité au RGPD* » qui vont arriver et « s*ur le contrôle des zones principales de risques* ».

Il est à souligner que le rôle d'interface que les DPO devront assurer entre les directions juridique et technique sera déterminant. Ce rôle complexe, qui requiert de **la maturité**, est encore insuffisamment appréhendé/pratiqué en entreprise alors même que les enjeux financiers deviennent conséquents. Rappelons que la CNIL vient de condamner deux sociétés du Groupe Carrefour pour un montant cumulé d'environ 3 000 000 d'euros.

Par ailleurs, **l'éthique révèle toute la dimension géopolitique du droit, en particulier, à l'égard des GAFAMs**.

La récente saisine de la Commission européenne par diverses entreprises et groupes industriels « *pour lui demander de prendre des mesures renforcées à l'encontre de Google*[12] *qui met ses propres services en avant sur son moteur de recherche au détriment de ses concurrents* », en est une parfaite illustration.

L'Union européenne (UE) est déjà très active sur le sujet. Elle vient de demander à Amazon « *de répondre aux griefs d'abus de position dominante* » (notamment sur le marché français) et a diligenté une enquête approfondie en vue de faire toute la lumière sur le fonctionnement de l'algorithme de la plateforme. Il est précisé que pour qu'un abus de position dominante soit caractérisé au sens de **l'article L. 420-2 du Code du commerce**, « *trois conditions doivent être réunies : l'existence d'une position dominante sur un marché déterminé ; une exploitation abusive de cette position ; un objet ou un effet, au moins potentiel, restrictif de concurrence.* »[13]

En outre, la Commission travaille à l'élaboration de deux nouveaux textes

- **le Digital Services Act et le Digital Market Act** - qui visent à réguler ces titans du numérique. Il est à noter que « *l'intervention d'un régulateur peut permettre de gérer des marchés dont il est constaté que la concurrence est empêchée. C'est le cas lorsqu'il existe une concentration factuelle de grands acteurs.* »[14]

In fine, cette règlementation et cette régulation, dont les principes et les valeurs qui sous-tendent la vision sont souvent mal compris par les entreprises, **constitueraient-elles un nouveau modèle**, en l'occurrence, celui du post-pragmatisme européen ?

Rappelons que parmi « *tous les courants d'idées, le pragmatisme est celui qui est le plus solidement enraciné dans* ***la culture Américaine*** »[15] et celui aussi qui a le plus influencé le libéralisme économique aux Etats-Unis. Pour plusieurs grandes figures de l'école classique, tels, Charles Sanders Peirce, William James, John Dewey et Richard Rorty, le pragmatisme représente une méthode d'appréhension des idées où « *l'usage qu'on fait d'une chose suffit à le définir* ».[16] « *On ne s'embarrasse pas de concepts, on traite le réel.* »[17]

Pourtant le cyberespace est encore perçu « *comme un territoire virtuel, un espace à part, sans frontières, qui s'affranchit des contraintes du monde physique (et le Cloud ne fait que renforcer ce caractère irréel*) »[18]. Cette « *puissante métaphore* » a sans doute rendu possible nombre de dérives, en particulier, les logiques de surveillance et d'hyper- ciblage ; autrement appelées « *capitalisme mental.* »[19]

Le post-pragmatisme est ici entendu comme s'adaptant à la « culture » que réclament les mutations générées par les technosciences en « *considérant quels sont les effets pratiques pouvant être produits par l'objet de la conception* (ici **celui des algorithmes de l'IA**), *la conception de tous ses effets étant considérée comme la conception complète de l'objet.* »[20]

Le post-pragmatisme européen pourrait à la fois promouvoir une vision éthique au titre de la confiance numérique tout en procédant à « l'inventaire » de l'école classique, notamment, en vue d'identifier ce dont il conviendrait de s'inspirer.

Car, en effet, pour quelle raison une gouvernance qui intégrerait une pratique de **l'intelligence juridique et économique** ainsi qu'**une posture décomplexée** en matière de compétition et d'innovation, en serait-elle empêchée par la seule volonté d'inscrire l'ensemble dans une démarche éthique et responsable ? Comme l'exprime Anthony Colombani : « *l'éthique n'est pas une barrière mise contre le développement de l'industrie, elle est au contraire la condition de son acceptabilité sociale. Il y a là quelque chose qui est de l'ordre d'un enjeu d'ordre civilisationnel. C'est même un enjeu d'efficacité : qu'est-ce qu'une bonne intelligence artificielle ? C'est celle qui favorise le plus grand bien pour le plus grand nombre.* »[21]

À titre de propos conclusif, citons le très talentueux **Tariq KRIM** : « *les modèles économiques de demain qui seront basés sur le respect de l'utilisateur sont des modèles économiques nouveaux sur lesquels* ***nous avons en Europe la possibilité de peser*** *!* » [22]

Parution le 11 décembre 2020

[1] Il est à préciser que l'éthique est ici entendue au sens de l'éthique du numérique. Par ailleurs, à ce stade, il convient d'envisager le titre sous une forme interrogative.
[2] Simon SUTOUR et Jean-Louis LORRAIN, « La prise en compte des questions éthiques à l'échelon européen », Rapport d'information du Sénat n° 67, 2013, p 11.
[3] Luc FERRY, « Une brève histoire de l'éthique : de l'antiquité à nos jours, Cycle de conférence : philosophie du temps présent », Parenthèse Culture 2, disponible sur : https://www.youtube.com/watch?v=UkzBTLQsGfI&t=4327s
[4] Éthique et Numérique « un référentiel Pratique pour les acteurs du numérique », octobre 2018, Cigref & Syntec numérique.
[5] Max WEBER, « Le savant et le politique », Plon, 1959, p 31.
[6] Il conviendrait d'ajouter l'éthique computationnelle qui émerge dans les années 2000.
[7] Ronand Le Roux, P 40, "Cybernétique et société", Norbert Wiener, Ed Points, janvier 2014. 2 "Cybernétique: d'une théorie naît une pratique international" - Norbert WIENER "Cybernetics or control and communication in the animal and the machine".
[8] Jocelyne Maclure et Marie-Noelle Saint Pierre, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », Les cahiers de la Propriété intellectuelle vol 30, p 758, le 19/09/19, disponible sur : http://www.ethique.gouv.qc.ca/fr/assets/documents/CPI_Maclure_Saint-Pierre.pdf
[9] Maxime Des Gayets, « La grande dépossession : pour une éthique numérique européenne », Ed Jean Jaurès, 2018, p 34.
[10] Stéphane ASTIER, "Comment se préparer à la vague d'audits de conformité au RGPD prévue pour 2021?" Préparez-vous à la vague d'audits de conformité RGPD, prévue pour 2021, https://infos.haas-avocats.com
[11] Gérard Haas, « Gouvernance des données, ce que le RGPD a changé », Maison du Barreau, 22 mai 2019, https://www.youtube.com/watch?v=fnMX1wyYrWY&feature=emb_title
[12] Google fait l'objet d'une plainte antitrust.
[13] https://www.economie.gouv.f
[14] Eve Renaud-Chouraqui, « Big tech, une meilleure régulation pour moins de sanction », https://infos.haas-avocats.com
[15] Universalis France, « Le pragmatisme », : https://www.universalis.fr/encyclopedie/pragmatisme/
[16] Nicolas BOULEAU, « Le pragmatisme », httpps:///www.youtbube.com
[17] Michel ONFRAY, « Une éthique sans morale », conférence du 16 juillet 2017.
[18] Frédérick DOUZET « Le cyberespace, un enjeu majeur de géopolitique », https://larevuedesmedias.ina.fr/
[19] Maxime Des Gayets, « La grande dépossession : pour une éthique numérique européenne », Ed Jean Jaurès, 2018, p 34.
[20] Universalis France, « Le pragmatisme », https://www.universalis.fr/encyclopedie/pragmatisme/
[21] Conférence parlementaire en format « Triangle du Weimar » organisée par le Sénat, 2019, disponible sur : http://www.senat.fr/evenement/colloque/triangle_de_weimar_cybersecurite_et_intelligence_artificielle.htm
[22] Tariq KRIM, interview réalisée par B Smart Tech, émission du 4 novembre 2020.

Le Label ExpertCyber, une brique indispensable pour la confiance et la sécurité numériques

FRANCK GICQUEL
Responsable des partenariats
Cybermalveillance.gouv.fr

Pour assurer la sécurité numérique de son entreprise, de sa collectivité ou de son association, il est indispensable d'intégrer et de concilier les ressources humaines et techniques bien en amont. Trop souvent négligé ou considéré comme non prioritaire, le facteur « humain » est une composante essentielle de la chaîne de sécurisation. Largement exposé aux menaces et démultipliant, par conséquent, la surface d'attaque des cybercriminels qui en profitent pour commettre leurs forfaits à peu de frais, il doit être suffisamment sensibilisé aux risques numériques et formé aux bonnes pratiques. Il contribuera, ainsi, et de façon proactive, au renforcement de la sécurité informatique de sa structure en devenant lui-même un « capteur du terrain », capable d'alerter en cas de problème et, ainsi, de contribuer à la prévention des incidents. Le volet technique, quant à lui, doit, par essence, permettre de renforcer son système d'information, afin de faire face aux attaques toujours plus ingénieuses, sophistiquées, et en constante progression technologique.

Ce sont principalement les grandes organisations qui maîtrisent de mieux en mieux ces deux volets ; elles possèdent en effet des équipements robustes et disposent des ressources internes dédiées, couplées à des prestataires informatiques bien identifiés. Ainsi, lorsque celles-ci sont la cible de cybercriminels, elles sont mieux armées face aux attaques. S'agissant des plus petites structures, en revanche, le constat est malheureusement bien différent. D'après l'analyse des plus de 200 000 demandes d'assistance recensées sur la plateforme Cybermalveillance.gouv.fr depuis sa création en 2017, 12 % concernent les parcours des professionnels (dont les collectivités et les associations). Ces derniers ont eu recours à Cybermalveillance.gouv.fr pour bénéficier de conseils de première urgence ou de l'assistance technique d'un

professionnel de proximité référencé sur la plateforme. Peu équipées, par manque de moyens ou d'informations sur les risques numériques, les victimes constatent trop tard la faible sécurité mise en place au sein du système informatique de leur structure, mettant sérieusement en danger leur activité.

Il est donc indispensable de se faire accompagner par des professionnels pour assurer une sécurisation des systèmes bien en amont et se prémunir ainsi contre les risques numériques. Mais alors, vers quels acteurs de confiance se tourner lorsque l'on est une TPE-PME ou une petite collectivité ? Avec le nombre important de sociétés informatiques sur le marché, sur la base de quels critères faire son choix ? Comment s'assurer de la qualité ou de la compétence d'un professionnel ?

Ce sont les questions auxquelles Cybermalveillance.gouv.fr a souhaité répondre, en lançant fin 2018 un groupe de travail composé des principaux syndicats et fédérations de prestataires de services numériques, membres du dispositif Cybermalveillance.gouv.fr : Cinov Numérique, Fédération EBEN, Syntec Numérique et la Fédération Française de l'Assurance (FFA). Cette dernière a été associée à la réflexion avec son statut d'interlocutrice de proximité des assureurs et des mises en relation qu'elle peut effectuer entre ses assurés et des prestataires de services de toutes natures, dont le numérique. L'objectif de ce groupe de travail était de réfléchir et de proposer des solutions pour répondre au besoin des utilisateurs de se sécuriser en amont par des professionnels de confiance ayant démontré leur niveau de compétences techniques.

La collaboration avec des prestataires de services en sécurité informatique était déjà au cœur de l'action du dispositif et ce, depuis sa création, mais uniquement sur le volet « post-incident ». En effet, Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels qui contribuent activement à sa mission d'assistance aux victimes. Les particuliers, entreprises et collectivités victimes d'actes malveillants sur Internet peuvent ainsi se connecter à la plateforme www.cybermalveillance.gouv.fr pour obtenir un diagnostic de leur situation et des recommandations sur les problèmes rencontrés. Concrètement, en suivant un parcours en ligne au travers de quelques questions simples, ils sont conseillés et, le cas échéant, mis en relation avec un réseau de près 1 000 professionnels, répartis sur l'ensemble du territoire.

C'est notamment grâce aux retours de ces professionnels en sécurité numérique que l'enrichissement de l'outil de diagnostic et la mise à jour des conseils sont rendus possibles. Les profils des professionnels référencés sont très hétérogènes (domaines d'intervention, taille, publics ciblés...), ce qui permet d'être en capacité d'apporter à tout individu ou organisation, une assistance technique qualifiée partout en France. Cela est d'autant plus important pour des entreprises, collectivités et associations victimes d'incidents plus complexes, parfois avec des informations très sensibles en jeu. C'est grâce à l'ensemble de ce réseau présent sur le terrain et en contact avec les publics que nous pouvons apporter une réponse aussi large.

Face à cette grande diversité, et en l'absence d'un « label » dédié aux professionnels en sécurité numérique s'adressant spécifiquement aux publics professionnels (TPE-PME, collectivités et associations), il était nécessaire de reconnaître et valoriser un nouveau niveau de réponse en termes d'expertise et de périmètres. C'est ainsi qu'est né le Label ExpertCyber. Ce label a été créé pour plusieurs raisons, en premier lieu, pour apporter aux utilisateurs une meilleure lisibilité de la qualité d'offre de service, condition nécessaire pour créer un climat de confiance dans le numérique, mais également pour valoriser et aider les prestataires justifiants d'un certain niveau d'expertise en sécurité numérique, et inciter à la montée en compétence. Il était aussi devenu très vite évident durant la phase de conception que le Label ExpertCyber ne pouvait se limiter à l'assistance post-incident. Pour cette raison, décision fut prise d'élargir les périmètres d'action à l'installation et la maintenance afin d'être en capacité de fournir aux entreprises et aux collectivités un accompagnement global sur le volet préventif.

Sur le dispositif de labellisation, le dispositif a opté pour un audit documentaire couplé à un questionnaire technique. Les audits sont menés par l'AFNOR, organisme professionnel de la certification, qui a accompagné le groupe de travail durant toute la démarche afin de valider le niveau d'expertise attendu des candidats. Les auditeurs se basent sur un référentiel qui regroupe un ensemble d'exigences couvrant quatre principaux domaines : les compétences techniques, la qualité de service client, la conformité administrative et le sens de l'intérêt général. Bien que constitutive de l'ADN du label, ce n'est donc pas uniquement l'expertise technique qui est évaluée, mais un ensemble de caractéristiques qui renforce la chaîne de confiance,

notamment pour des publics souvent peu aguerris sur le sujet de la sécurité numérique, voire sur le numérique tout court.

Le label ExpertCyber sera lancé publiquement au début de l'année 2021 et aura pour ambition de contribuer à l'amélioration et au renforcement du niveau de sécurité des entreprises, des collectivités et des associations en favorisant leur mise en relation avec des acteurs de confiance. Elle sera possible depuis un nouveau service dédié sur la plateforme Cybermalveillance.gouv.fr et également accessible au travers d'autres outils, afin que ce nouveau label puisse profiter au plus grand nombre.

Parution le 18 décembre 2020

Table des matières

Préface 3
Bénédicte PILLIET, Présidente, CyberCercle

Pandémie : une situation exceptionnelle… aussi sur le front cyber 5
Loïc GUEZO, Senior Director, Cybersecurity Strategy SEMEA, Proofpoint, Réserviste Cybermenaces Police Nationale - 8 avril 2020

Cybercontrefaçon et pandémie sanitaire 11
Myriam QUEMENER, Magistrat, Docteur en droit - 15 avril 2020

L'identité numérique, c'est aussi un enjeu de souveraineté 17
Jean-Michel MIS, Député de la Loire - 23 avril 2020

Télétravail : échanger en gardant le contrôle de ses données 21
Charles BLANC-ROLIN, RSSI, GHT 15 - 4 mai 2020

Coronavirus : la cybersécurité conjugue résilience et relance..... 25
Jean-Charles LARSONNEUR, Député du Finistère - 8 mai 2020

À l'ère du télétravail, six axes pour assurer la continuité des activités métiers 29
Christophe AUBERGER, Directeur technique, FORTINET - 15 mai 2020

Le port du futur sera un port « smart » et cyber sécurisé ! 33
Jérôme BESANCENOT, Chef du Service du développement des Systèmes d'Information, HAROPA Port du Havre - 22 mai 2020

La cybersécurité post-Covid rimera-t-elle vraiment avec souveraineté ? 39
Raphaël MARICHEZ, Expert cybersécurité, Services du Premier ministre - 29 mai 2020

D'une pandémie l'autre… 49
Christian DAVIOT, ancien conseiller stratégie du directeur général de l'ANSSI - 5 juin 2020

Application StopCovid : quels impacts sur nos données personnelles ? 55
Nacira SALVAN, Présidente, CEFCYS - 12 juin 2020

Vous avez dit souveraineté ?..... 65
Alain BOUILLE, Expert cybersécurité - 18 juin 2020

Sensibiliser à la sécurité numérique au plus près des acteurs sur les territoires : un enjeu majeur..... 73
Jérôme NOTIN, Directeur général, Cybermalveillance.gouv.fr - 26 juin 2020

Identités numériques..... 79
Dr Michel DUBOIS, Chef du Pôle Expertise, Direction de la cybersécurité, Groupe La Poste - 3 juillet 2020

Impact des recherches en cybersécurité sur la stratégie nationale en matière de souveraineté numérique 83
Laurent OLMEDO, Directeur du programme Sécurité globale, Direction des applications militaires, CEA et Bruno CHARRAT, Responsable du programme cybersécurité, Direction de la recherche technologique, CEA - 10 juillet 2020

La ResNumérique : de la sécurité des systèmes d'information vers un numérique de confiance, il est temps d'agir 91
Stéphane MEYNET, Président, CERTitude NUMERIQUE - 17 juillet 2020

Innovation de rupture et cybersécurité 99
William LECAT, Directeur de Programme Grand Défi automatisation de la cybersécurité, Secrétariat Général pour l'Investissement - 24 juillet 2020

Dérive du modèle français de cybersécurité : origines, conséquences, remèdes 105
Christian DAVIOT, ancien conseiller stratégie du directeur général de l'ANSSI - 31 juillet 2020

La conformité au RGPD est devenue une évidence, au service des collectivités et des citoyens 123
François COUPEZ, Avocat associé, Implid Legal - 28 août 2020

Convergence sûreté et cybersécurité : du serpent de mer à l'évidence .127
Jérôme SAIZ, Président Fondateur, OPFOR Intelligence - 4 septembre 2020

Sécurité du numérique : la réserve numérique de la gendarmerie au cœur de l'action « répondre présent pour la population, par le gendarme » 131
Florence ESSELIN, Conseiller expert en numérique et cybersécurité, cabinet du directeur général de la Gendarmerie nationale - 11 septembre 2020

Former, informer, sensibiliser pour lutter contre les cyberattaques 139
Gérard PELIKS, Chargé de cours cybersécurité dans les écoles d'ingénieurs et instituts, Membre de l'ARCSI - 18 septembre 2020

Heureusement que le numérique était là ! 145
Laure DE LA RAUDIERE, Députée d'Eure-et-Loir - 25 septembre 2020

Sécuriser le télétravail dans les institutions publiques 149
Christophe AUBERGER, Directeur technique, FORTINET - 2 octobre 2020

La cybercriminalité à l'heure de la Covid-19 153
Myriam QUEMENER, Magistrat, Docteur en droit - 9 octobre 2020

Le retour de la « Panic Room » 159
Hervé MORIZOT, Co-fondateur et Directeur général, FORMIND - 16 octobre 2020

Informatique de santé et cybersécurité : prospectives 2037 165
Cédric CARTAU, RSSI et DPO, CHU de Nantes et GHT44 - 23 octobre 2020

La marétique, un enjeu essentiel pour l'humanité ? 175
Colonel Florian MANET, Commandant la Section de Recherches de Bretagne, Gendarmerie nationale, Essayiste - 30 octobre 2020

Former à la cybersécurité dans tous les territoires 181
Nicolas FORISSIER, Député de l'Indre - 6 novembre 2020

La cybersécurité a besoin de femmes, et les femmes ont toute leur place dans la cybersécurité 185
Nacira SALVAN, Présidente, CEFCYS - 20 novembre 2020

Cybersécurité : des Hommes de bonne volonté contre le temps qui passe 195
Fabien MIQUET, Product & Solution Security Officer, Siemens Digital Industries France - 27 novembre 2020

Lancement de la Fédération Française des Professionnels de la Blockchain : créons des alliances pour retrouver notre autonomie stratégique sur les questions technologiques 201
Jean-Michel MIS, Député de la Loire - 4 décembre 2020

De l'Ethique européenne à l'avènement de l'ère Post-pragmatique.....207
Alice LOUIS, Data Governance Consultant, Cyber Ethics Teacher, Legal Advisor, European Expertise Work (EEEI) - 11 décembre 2020

Le Label ExpertCyber, une brique indispensable pour la confiance et la sécurité numériques 213
Franck GICQUEL, Responsable des partenariats, Cybermalveillance.gouv.fr - 18 décembre 2020

CyberCercle - 18 rue Tronchet, 69006 Lyon
contact@cybercercle.com - cybercercle.com

Réalisation : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

Directeur de la publication : Bénédicte PILLIET
CyberCercle – 18 rue Tronchet, 69006 Lyon
contact@cybercercle.com – cybercercle.com