Cybersecurity Trends

Édition spéciale. Avril 2020

Ce volume vous est offert par :

MIRAT DI NERIDE
Cyber Sécurité

- **Contexte et impacts**
- **Guide de cyber-défense pour citoyens et entreprises**

«Cyber-covid#19», la plus ample vague de cyberattaques de l'histoire. PROTÉGEZ-VOUS !

Ce volume est placé sous l'égide de :

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

Il a été réalisé en partenariat avec :

Gendarmerie nationale
Une force humaine

Centre de recherche de l'EOGN

POLICE GENÈVE

ROMANIA
CENTRUL NAȚIONAL CYBERINT
SERVICIUL ROMÂN DE INFORMAȚII

DIRECȚIA DE COMBATERE A CRIMINALITĂȚII ORGANIZATE
I.G.P.R.

CERT-RO

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

GLOBAL CYBER SECURITY CENTER

AUSIM
beyond digital

FIC

CHARENTE-MARITIME CYBER SÉCURITÉ

CYBERSECURITY PUBLIC - PRIVATE DIALOGUES

swiss-cybersecurity.ch

et avec le soutien de :

BLOCKAPT

STANCHION STANCHION

Index

CE VOLUME EST PLACÉ SOUS L'ÉGIDE DE :

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

IL A ÉTÉ RÉALISÉ EN PARTENARIAT AVEC :

Gendarmerie Nationale (FR)
www.gendarmerie.interieur.gouv.fr/

Centre de recherchede l'École desOfficiers
de la Gendarmerie Nationale (FR)
www.gendarmerie.interieur.gouv.fr/crgn/

Police de Genève (CH)
www.ge.ch/organisation/corps-police

Centre CYBERINT du Service de
Renseignements de Roumanie
www.sri.ro

Direction de lutte contre la Criminalité
Organisée de la Police Roumaine
www.politiaromana.ro

Centre national de réponse aux incidents
de sécurité informatique (RO)
www.cert.ro

Autorité Nationale d'Administration et
deréglementation des communications (RO)
www.ancom.ro

Global Cybersecurity Center (IT)
www.gcsec.org/

Association des Utilisateurs des Systèmes
d'Informations au Maroc
http://www.ausimaroc.com/

Forum international de la cybersécurité
www.forum-fic.com

Charente-Maritime Cyber Sécurité
www.cmcs-connect.fr

Cybersecurity Dialogues
www.cybersecurity-dialogues.org

ET AVEC LE SOUTIEN DE :

SwissCybersecurity
www.swiss-cybersecurity.ch

www.blockapt.com

www.stanchionpayments.com

La propagation du CoVID19 et des cyberattaques : une double menace pour nos sociétés

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

Auteur : Arthur Mattli,
Ambassadeur de Suisse en Roumanie

La propagation du CoVID19 et la propagation actuelle des cyberattaques ont de nombreux points communs : elles se répandent toutes deux de manière invisible et à grande vitesse, elles perturbent la vie de millions de personnes de manière redoutable, elles ont un impact économique inquiétant dans le monde entier et elles actionnent toutes deux dans la pire des symbioses. La plupart des mesures de verrouillage imposées par les gouvernements ont entraîné une perturbation importante du comportement humain. Alors que les chaînes d'approvisionnement alimentaire et les entreprises de transport semblent tenir bon, nous assistons à une profonde mutation des industries de services vers des postes de travail à distance, des écoles passant temporairement à des cours en ligne et des services en ligne confrontés à une explosion de la demande.

Heureusement, le monde numérique dans lequel nous vivons nous offre, en cette période difficile sans précédent, d'énormes possibilités de continuer à faire des affaires, à maintenir des contacts sociaux et même à améliorer des vies humaines. Mais les effets imprévus de notre brave nouveau monde numérique sur la sécurité des personnes et des pays du monde entier sont décidément réels : ironiquement, les contraintes imposées pour protéger des millions de personnes contre le CoVID19 exposent un nombre record d'utilisateurs numériques à des cyberattaques. Et tandis que le monde a appris, par tous les moyens d'information, l'importance de se nettoyer les mains, le visage et à désinfecter, entre autres, les poignées de portes, peu d'éducation et de prévention ont été rendues disponibles aux utilisateurs pour les aider à protéger leurs ordinateurs et leurs réseaux des cyberattaques. Les cyber-attaques sont notamment accompagnées de *fake news*. Au sujet de l'infestation de l'espace virtuel par les *fake news* concernant le virus, le Secrétaire général des Nations Unies en personne a lancé un avertissement sévère, le 28 mars dernier.

Dans le sillage du CoVID19, la cybercriminalité organisée a multiplié ses méfaits à une vitesse et avec une ampleur sans précédent. Des campagnes de fraude à grande échelle sont en circulation, notamment de fausses publicités pour des produits médicaux dont le besoin est urgent. Les cybercriminels exploitent sans relâche ni pitié le fait que des millions de cyber-utilisateurs partagent leurs informations et leur comportement numérique pendant cette période de détresse. Comme des prédateurs, ils attirent les ignorants, les novices, exploitent des failles et posent des pièges.

La présente édition de Cybersecurity Trends vise à combler un important manque d'informations dans le débat actuel sur la cyber-sécurité et aide à mieux comprendre les risques actuels et les menaces immédiates dans le monde numérique dans le contexte de la CoVID19 et au-delà.

Je remercie Laurent Chrzanovski, son équipe de rédaction, et tous les auteurs des textes de la présente publication pour leur clairvoyance thématique et pour leur contribution à une discussion et une coordination internationale indispensables.

Les opinions et les observations exprimées ci-dessus n'engagent que leur auteur et ne reflètent pas nécessairement celles de la Confédération suisse. ■

I. Préfaces des partenaires

De l'importance de repositionner - de repositiver - l'humain comme acteur de la cybersécurité

Auteur : G.al Marc Watin-Augouard

La crise ouverte par le Covid-19 va sans aucun doute accélérer la transformation numérique pour le meilleur comme pour le pire. Les prédateurs ont compris qu'elle leur offrait une opportunité pour migrer vers l'espace numérique qui, lui, n'est pas confiné. Ils y resteront ! Les internautes honnêtes n'ont jamais autant utilisé les applications qui se sont multipliées, en raison notamment du recours massif au télétravail, au besoin de conserver un contact humain malgré la "distanciation sociale ". Demain nous verrons sans doute les territoires se remodeler, avec un grand retour vers les "campagnes ", plus résilientes que les villes, pour peu que le très haut débit soit au rendez-vous. Demain les apports de la 5G, du Big data, de l'IA favoriseront des usages nouveaux, notamment au profit de la télémédecine, de la prédiction des épidémies et de leur déploiement. Demain, des robots commandés à distance permettront le télétravail à ceux qui sont aujourd'hui "en première ligne ", de livrer des produits, de protéger des personnes vulnérables.

Mais rien ne pourra se faire sans quête du sens ! "Replacer l'humain au cœur de la cybersécurité " ce n'est pas une option parmi d'autres; c'est une exigence ! La cybersécurité, plus que jamais, devra être au service de la liberté. Nous savons combien celle-ci nous est chère et doit être défendue, contre ceux qui ont d'autres conception de l'Homme.

La cybersécurité s'est construite par strates successives. Au contrôle du "traitement" des données (1978) a succédé la protection des "systèmes" de traitement automatisé de données (1988), puis celle des "données", replacées au centre de l'écosystème numérique (2018). Les données à caractère personnel ont toujours fait l'objet d'une vigilance particulière, mais jamais leur sensibilité n'a été autant mise en exergue, du fait de la croissance exponentielle des plateformes, des applications, des systèmes connectés qui "reformatent" notre société avec une vitesse souvent imperceptible par nos propres sens. Plus que jamais, ces données nous caractérisent, dévoilent notre intimité, pénètrent la sphère du secret de notre vie privée sans laquelle il n'y a pas de liberté. Plus que jamais profilé par des algorithmes, l'humain n'est plus tout à fait le maître et tend à devenir sujet, au risque de finir esclave. Pourtant, rien n'est perdu, car la maîtrise de la transformation numérique appelle avant tout une mobilisation des compétences, une acculturation partagée aux enjeux du nouveau monde. Trop souvent abandonnée aux spécialistes, aux experts, la cybersécurité doit être en vérité le fruit d'une posture individuelle et collective qui résulte d'une formation largement diffusée dès le plus jeune âge. Trop souvent identifiée comme une filière réservée aux

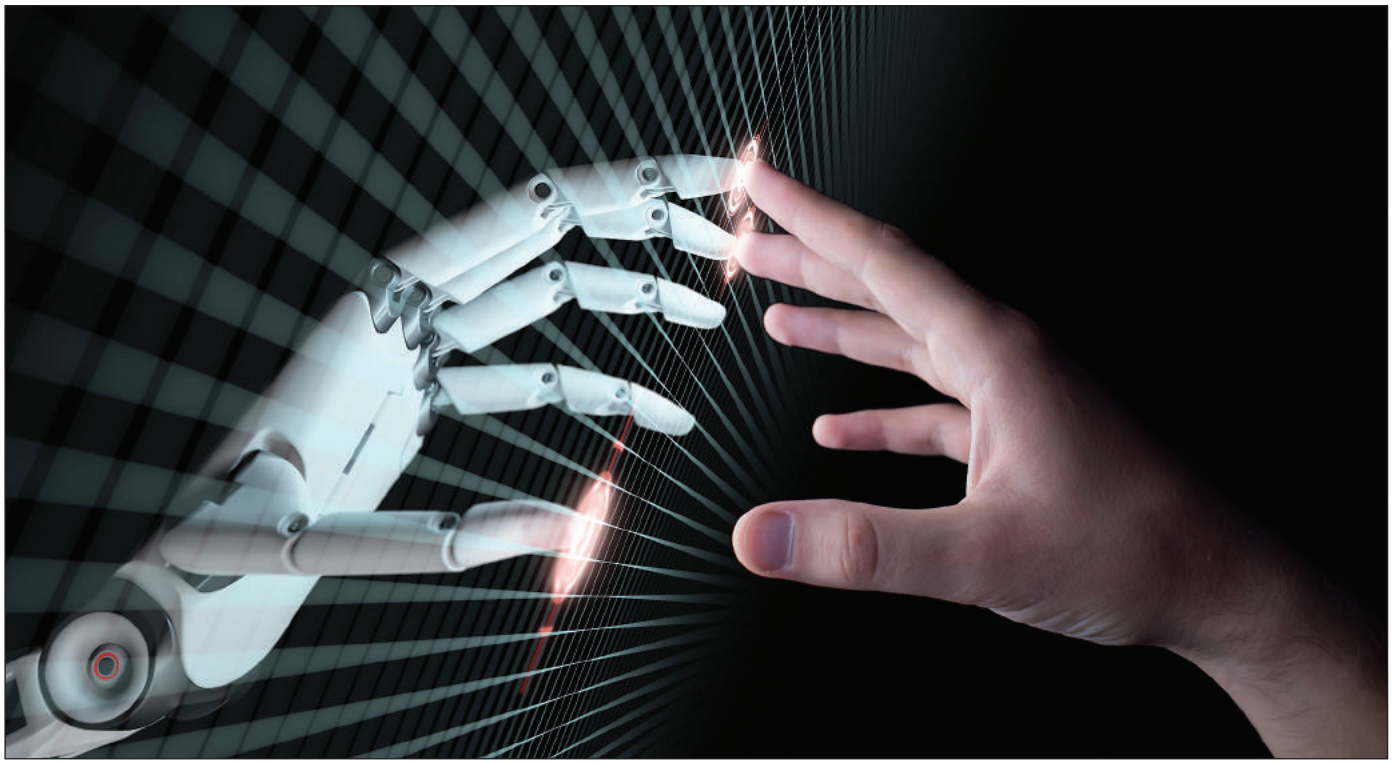
BIO

- **Fondateur et Codirecteur, Forum international de la cybersecurité – FIC**
- **Directeur, Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)**
- **Ancien inspecteur général des armées-gendarmerie**
- **Général d'armée (2008)**
- **Général de corps d'armée (2007)**
- **Général de division (2006)**
- **Commandant, Gendarmerie pour la zone de défense Nord (2005 – 2008)**
- **Commandant, Région de gendarmerie du Nord-Pas-de-Calais**
- **Conseiller pour la gendarmerie, Cabinet de Dominique de Villepin (2004 – 2005)**
- **Général de brigade (2003)**
- **Conseiller pour la sécurité, Cabinet de Nicolas Sarkozy (2002 – 2004)**
- **Commandant de la légion de gendarmerie départementale de Champagne-Ardenne (2000 - 2002)**
- **ENSEIGNEMENT : Chargé de cours en droit, Universités Panthéon-Assas (Paris II), René Descartes (Paris V) et Aix-Marseille III-Méditerranée.**

hommes, la cybersécurité doit aussi être portée par des femmes qui ne représentent aujourd'hui que 10 % des emplois correspondants, alors qu'elles constituent plus de la moitié de la population. Sans doute faut-il envisager le recours aux technologies, comme l'intelligence artificielle, pour sécuriser nos réseaux, nos échanges, nos données. Mais il importe surtout de repositionner – de repositiver – l'humain comme acteur de la cybersécurité, alors qu'il est essentiellement regardé aujourd'hui comme victime ou comme auteur, volontaire ou involontaire, des cyberincidents ou des cybermalveillances.

Dans notre quête de la cybersécurité, nous sommes trop souvent en attente de la réponse à la question "comment ?", en laissant aux technologies le soin d'y répondre ; nous avons ainsi négligé la question "pourquoi ?" en exigeant des finalités conformes à notre conception de l'humain. "*Science sans conscience n'est que ruine de l'âme*" écrivait Rabelais dans Pantagruel. Cette invitation à conjuguer les sciences "dures" et les sciences humaines est plus que jamais d'actualité. La cybersécurité a besoin de juristes, de sociologues, de philosophes, d'historiens, etc., pour garantir une sécurité de tous au service de la liberté de chacun.

Il est temps de replacer l'humain au coeur du discours et de l'action. Nous savons que, sans une vision européenne partagée, nous aurons demain le choix entre une "liberté surveillée" et une "sécurité surveillée ", selon que nous serons "colonisés" par l'ouest ou par l'est. À l'Europe d'avoir enfin un vrai projet politique qui ait pour objectif d'assurer une "liberté sécurisée", garante des valeurs partagées par les 27 États membres. C'est l'occasion de donner du souffle à une transformation numérique par trop matérialiste. C'est le socle minimal pour offrir au reste du monde une alternative à l'imperium croissant des deux géants du numérique. Nous avons perdu la bataille du hardware, du software et des plateformes. Nous pouvons gagner celle de l'humain. Nombre d'internautes, en Europe, "de l'Atlantique à l'Oural" et en Afrique n'attendent que cela. ■



Augmentation des cyberattaques dans le contexte de la pandémie de COVID-19

Auteur : Anton Rog

Dans le contexte généré par la propagation du virus SARS-Cov-2 (COVID-19), au cours du mois de mars de cette année, on a observé une intensification des cyber-activités illégitimes, certaines d'entre elles étant dirigées contre des institutions de l'État roumain.

Dans ce cadre, les hackers sont intéressés à lancer de nombreuses campagnes de cyber-attaques pour endommager et/ou immobiliser le fonctionnement des systèmes institutionnels, en exploitant la pandémie. Les types les plus courants de campagnes recensées durant cette période sont, spécifiquement, des attaques de type *ransomware* et celles dites de *"web defacement"* (piratage et modification d'un site web, ndr.).

Ces vagues d'attaques visent *in primis* les infrastructures de TIC utilisées et gérées par les ministères et les institutions gouvernementales, les organismes responsables des mesures d'atténuation des effets générés par le COVID-19, mais aussi plusieurs entreprises du secteur privé, en particulier celles actives dans les domaines de la santé, de l'éducation et de la recherche.

Pour assurer à leurs actions un taux élevé de réussite, les cybercriminels ont mis à jour leurs opérations en fonction du contexte international/national, ont diversifié leurs tactiques mais aussi leurs techniques d'attaque. Ils suivent la distribution de logiciels malveillants, par des campagnes d'hameçonnage et/ou de *spear-phishing* (hameçonnage ciblé ou "harponnage", ndr), grâce auxquelles ils exploitent le besoin généralisé d'information sur l'état de la propagation de COVID-19, et spécialement le manque de ressources médicales.

De plus, pour gagner la confiance des victimes, les attaquants intègrent dans leurs courriels et autres formes de messages transmis par des campagnes d'hameçonnage et/ou de *spear-phishing* des éléments d'usurpation d'identité (adresses e-mail, titres, contenu textuel) se faisant passer pour les institutions internationales et nationales habilitées à faire face à la situation de pandémie.

La cyber-menace est également renforcée par la circulation d'un grand nombre de fichiers sur des canaux non officiels.

On s'attend donc à ce que le nombre de campagnes de cyber-attaques augmente, dans le contexte de la pandémie du COVID-19, c'est pourquoi nous recommandons à tous l'adoption de mesures préventives dans l'environnement numérique. Il s'agit surtout d'éviter d'accéder aux courriels et aux pièces jointes reçus de la part de sources non fiables, d'appliquer une utilisation stricte d'applications légitimes (légalement acquises sur le marché, n.d.r.) et surtout de s'informer uniquement qu'en consultant les sources officielles. ■

BIO

Le Général Anton Rog est directeur général du Centre national CYBERINT du Service roumain de renseignement (SRI). Le Centre CYBERINT est l'institution responsable de la détection, de l'analyse et de la lutte proactive, 24 heures sur 24 et 7 jours sur 7, défendant des logiciels malveillants tous les systèmes et les réseaux essentiels à la sécurité nationale de la Roumanie. Au sein du SRI, Anton Rog a précédemment occupé plusieurs postes au sein du service de développement technique, notamment dans la conception de logiciels et de systèmes. Il a également travaillé comme directeur adjoint au sein du département central IT&C du SRI. Il est également actif au sein de la communauté universitaire en tant que Professeur Associé au DRESMARA (Département régional d'études pour la gestion des ressources de défense) de Brasov. Anton Rog a obtenu une licence en informatique à l'Université de Bucarest en 1998 et a obtenu en 2011, au DRESMARA, un diplôme de troisième cycle en «Gestion de programmes et de projets». Il a été décoré de l'Ordre de la virilité et de la foi (avec grade de Chevalier) en 2014 et de l'Ordre de la vertu militaire (avec grade de Chevalier) en 2005, par décret de deux différents présidents de Roumanie.

Une publication bienvenue dans le cadre d'une vague d'attaques sans précédent

Auteur : Patrick Ghion

Comme toute l'Europe, notre pays est la proie d'une vague d'assauts cybercriminels sans précédent, par leur nombre, leur ampleur, leur diversité et, surtout, par la qualité des plus dangereux d'entre eux.

On y trouve, outre les hameçonnages et les formes connues d'arnaques digitales, des nouvelles générations de *ransomwares*, d'attaques aux systèmes et aux softwares les plus utilisés, en sus d'un nombre impressionnant de *zero-days** et de mutations accélérées des *Advanced Persistant Threats***.

Pire, ces attaques touchent désormais non seulement les citoyens de toutes les tranches d'âge et de toutes les catégories sociales, mais aussi toutes les entreprises, des plus petites aux plus grandes. L'ensemble des outils digitaux utilisés quotidiennement, du smartphone aux tablettes et ordinateurs jusqu'aux serveurs et au cloud sont sous attaque.

Pour exemple, il suffit de se rapporter aux statistiques officielles de la Confédération pour constater l'échelle des dégâts : de 14 annonces dénonçant des incidents / attaques graves durant la première semaine de janvier 2020, le *Centre National pour la Cybersécurité* a enregistré, durant la première semaine d'avril, près de 240 annonces (1), soit un bond de plus de 1700%.

Opérationnel depuis l'an dernier, le Centre de Compétence Régional de lutte contre la cybercriminalité pour la Suisse occidentale est situé au sein de la Police cantonale de Genève. Le principe issu de la nouvelle stratégie de protection de la Suisse en matière Cyber a pour objectif de mutualiser des compétences avancées au niveau inter cantonal. Ce changement de paradigme annonce une ère collaborative sans précédent dans l'histoire de la Suisse, où chaque Canton (Etat) constitutif de la Confédération a sa propre police et son propre organe de police judiciaire avec sa cellule cyber, compétente en la matière.

Dans ce cadre, et avec les nouvelles responsabilités extra-cantonales qui incombent désormais à la Police Cantonale de Genève, une attention particulière est accordée à l'importance fondamentale aux partenariats public-privé, qu'elle multiplie depuis des années avec des résultats extraordinaires. Comme dans tout le continent, avec notre personnel spécialisé au front – nous sommes dans l'impossibilité de mobiliser des forces supplémentaires pour grouper, concentrer et faire une synthèse des alarmes diffusées auprès de la population et des entreprises.

A notre avis, la présente brochure destiné à tout un chacun, véritable guide de prévention et de défense numérique à la structure limpide, basée par catégories d'attaques et de cibles, rendue dans un style clair et synthétique et doublée par d'innombrables références en ligne, vient à point nommé. C'est donc pour nous un devoir et un honneur que de figurer parmi les principaux partenaires internationaux de la présente publication, qui verra le jour en trois langues.

Pour avoir pris cette initiative et assumé bénévolement tout le travail qu'elle représente, nous remercions chaleureusement notre partenaire de longue date, la Swiss Webacademy, organisatrice du triptyque de congrès internationaux Cybersecurity-Dialogues, matérialisés par la revue Cybersecurity Trends, ainsi qu'à toutes celles et ceux qui ont contribué à la présente édition spéciale, *in primis* son fondateur et rédacteur en chef, Laurent Chrzanovski, ainsi que son équipe de travail. ■

BIO

Le Capitaine Patrick Ghion travaille pour la Police Cantonale de Genève depuis 20 ans. Auparavant responsable de la brigade de lutte contre la criminalité informatique, Patrick Ghion est aujourd'hui chef de la section forensique de la police judiciaire de l'Etat de Genève, constituée de 4 brigades dont celle de lutte contre la criminalité informatique. Avant de rejoindre les forces de l'ordre, il a travaillé dans plusieurs banques suisses et a également vécu un temps comme instructeur de plongée en Asie. Père de deux enfants, ses principaux hobbys sont la plongée sous-marine et le pilotage d'avions.

*zero-days = Attaque inédite visant une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu

**Advanced Persistant Threats = types de piratage informatique furtif et continu ciblant souvent une entité ou un secteur spécifique.

(1) www.melani.admin.ch/melani/fr/home/ueber_ncsc/meldeeingang.html

Y parviendrons nous ?

Auteur : Nicola Sotira

Aujourd'hui, il semble presque «normal» de parler de mesures d'urgence, de pandémies, de COVID-19 ; une situation d'urgence qui a commencé à se manifester publiquement en Italie le 30 janvier avec deux touristes chinois testés positifs.

A partir de là, les chiffres augmentent et nous devrons nous habituer à **tout** voir sous un nouveau jour. Comme le rapport du MIT du 17 mars l'indique très clairement, pour stopper cette pandémie, nous devrons changer toutes nos habitudes, notre façon de travailler, de faire de l'exercice, de faire nos courses, d'éduquer, d'étudier, de socialiser et surtout de voyager.

BIO

Nicola Sotira est Directeur de la Sécurité de l'Information du Groupe Poste Italiane et le Directeur Général du Global Cyber Security Center (Fondation du Groupe). Il possède plus de 25 ans d'expérience dans le domaine de la cyber-sécurité, acquise dans différentes compagnies internationales, au cours de ses mandats. Avant de rejoindre le Groupe Poste Italiane, Nicola Sotira a été Sales Director UC&C & Security Practices au Westcon Group Italy et Vice-Predident Sales Italy pour Clavister AB. Professeur à l'Université La Sapienza de Rome depuis 2005, il enseigne dans le cadre du Master in Network Security, il est également membre de l'Association for Computing Machinery, depuis 2004. Promoteur des innovations technologiques, il a collabore avec de nombreuses start-ups, en Italie comme à l'étranger. Membre d' Italia Startup depuis 2014, il y participe au développement et à la conception de services mobiles. Il est en outre collaborateur de l' Oracle Security Council.

Certaines de ces transformations pourraient-elles devenir permanentes ?

Jusqu'à récemment, le *smart working* semblait ne concerner que certaines niches de travailleurs; il est aujourd'hui adopté à grande échelle et à la grande satisfaction des entreprises, notamment celles qui opèrent dans le secteur des services.

Nous avons donc découvert que cela peut se faire, que notre journée de travail peut être marquée par des réunions menées grâce à des plateformes digitales de collaboration sans que la qualité du travail en soit affectée.

Mais qu'adviendra-t-il des écoles, des universités ? Nous souvenons-nous des images des actualités qui nous ont offert des salles de classe complètes et le manque d'amphithéâtres ?

Ce sujet semble devenu presque anachronique aujourd'hui et je ne veux même pas aborder l'aspect de l'entretien coûteux des locaux éducatifs, qui reste à faire, voire de la construction de nouveaux espaces.

À ce stade, les écoles ont lancé des sessions en ligne et le thème de l'apprentissage en ligne a été entièrement intégré.

Fini, les salles de classe bondées : chacun peut suivre les leçons depuis chez lui et interagir avec le professeur via des chat ou des formulaires en ligne.

Les centres d'analyse de la qualité de l'air et les images satellites montrent également une diminution de la pollution, un autre élément qui nous fait réfléchir à la manière dont un modèle de croissance différent peut combiner le développement et la durabilité environnementale.

Le numérique s'avère de plus en plus pertinent et permet de changer les règles du jeu, dans la production, dans le cycle de vie des entreprises, mais aussi pour la gestion du temps libre dans des moments où la socialisation physique est réduite par la force des choses, comme ceux que nous connaissons actuellement.

De plus, dans le cadre de cette urgence, de nombreux Etats ont également dématérialisé les prescriptions médicales et il sera possible de demander digitalement les médicaments par e-mail et même via WhatsApp.

Nous utilisons le Big Data et des techniques prédictives dans le domaine de la santé, nous parlons d'utiliser des applications pour surveiller la propagation de la pandémie, nous pensons à la mise en œuvre de la télémédecine. On a la preuve que tout ce dont nous discutions sans fin avant la tragédie peut se faire réellement et concrètement !

Le monde a changé à de nombreuses reprises et cette pandémie va encore changer nos vies. Nous devrons tous nous adapter à une nouvelle façon de vivre après cette expérience.

Mais comme pour tous les changements, il nous faut apprendre à apprécier les aspects positifs pour faire un bond et accélérer une véritable métamorphose numérique, qui sera obligatoirement accompagnée d'une minutieuse tutelle de tous les aspects de la sécurité et de la vie privée, seuls à pouvoir garantir une vraie amélioration de notre qualité de vie.

Le mieux que nous puissions espérer est que la gravité de la tragédie actuelle ne forcera pas seulement tous les pays à repenser les questions sociales qui ont généré des inégalités, mais les incitera à mettre en œuvre les changements positifs qui méritent de continuer au-delà de cette période d'urgence. ■

Comment les cybercriminels exploitent le COVID-19, le travail à distance et comment riposter

BLOCKAPT

Auteur : Marco Essomba

BIO

Marco Essomba est le fondateur et le directeur technique de BlockAPT. Cette entreprise de pointe en matière de cybersécurité, basée au Royaume-Uni, offre aux organisations une plateforme de cyberdéfense avancée et intelligente. La plateforme BlockAPT permet aux organisations de surveiller, gérer, automatiser et réagir (MMAR) aux cyber-menaces, 24 heures sur 24 et 7 jours sur 7. La passion, l'expertise et les connaissances de Marco depuis 15 ans dans l'élaboration de solutions de cyber-sécurité ont abouti à la conception de notre plateforme unique BlockAPT. Développée au fil du temps comme une boîte à outils pour aider les petites et grandes entreprises à résoudre leurs problèmes de sécurité, la plateforme BlockAPT réunit le renseignement sur les menaces, la gestion des vulnérabilités, la gestion des dispositifs et la gestion proactive des réponses aux incidents pour aider à lutter contre les cyberattaques.

LinkedIn : https://www.linkedin.com/in/marcoessomba/
Twitter : https://www.linkedin.com/in/marcoessomba/
Site web de la société : https://www.blockapt.com

Introduction

Les cybercriminels sont toujours à l'affût pour exploiter les événements les plus médiatisés en utilisant l'ingénierie sociale. L'épidémie de coronavirus (COVID-19) est un parfait exemple de la manière dont les cybercriminels créent des systèmes de fraude sophistiqués destinés à inciter les utilisateurs à cliquer sur des liens créés *ad hoc* afin de télécharger des logiciels malveillants, en utilisant des techniques de hameçonnage. Parmi les nombreux types d'attaques, les hameçonnages continuent de représenter une menace importante pour les individus et les organisations de toutes tailles. Ils restent un outil très efficace utilisé par les cybercriminels car il leur est relativement facile de cibler directement des millions d'utilisateurs par le biais de courriels, de messages transmis aux smartphones et sur les pages des réseaux sociaux, en utilisant le coronavirus comme un appel à l'action.

Le coronavirus a forcé des millions d'utilisateurs à travailler à domicile. De nombreuses organisations ont été prises au dépourvu et ont dû se précipiter pour mettre en place des solutions d'accès à distance, souvent inadéquates et peu sûres. Cela pose un problème important pour les organisations dont les employés sont directement visés par toutes sortes d'escroqueries «COVID-19» qui ont pour but d'utiliser les logiciels d'accès à distance, vulnérables, comme autant de vecteurs leur servant à obtenir un accès non autorisé à des systèmes sécurisés et à des données sensibles. Plus important encore, puisque que de plus en plus d'organisations ouvrent leurs infrastructures critiques à l'ensemble de leur personnel à distance, les cybercriminels sont en permanence à la recherche de nouveaux moyens de s'introduire dans ces systèmes à des fins malveillantes.

COVID-19 - un point d'attaque idéal pour pirater les particuliers et les PME

Les cybercriminels cherchent à compromettre les dispositifs centraux et à voler des informations sensibles en utilisant des techniques d'attaque

courantes telles que le hameçonnage, l'exploitation de logiciels sans leurs correctifs les plus récents et le recours à des attaques par force brute : tous les moyens sont bons pour obtenir un accès non autorisé à des systèmes distants. Étant donné le manque d'expertise et de compétences en matière de cyber-sécurité, on s'attend à ce que les PME en particulier soient prises au dépourvu. La plupart auront des solutions inadéquates pour protéger leurs employés contre diverses cyberattaques comme le hameçonnage. Pour cette raison, le risque pour ce type d'organisations sera beaucoup plus élevé que d'habitude, entraînant un vol de données important pouvant même conduire à des dommages plus élevés que le vol lui-même, comme l'augmentation de leur cyber-assurance.

Il devient encore plus essentiel de renforcer la cyber-sécurité pour permettre aux employés de continuer à travailler à domicile de manière productive. Étant donné la nature très variée des cyber-menaces que les cybercriminels peuvent exploiter, la logique voudrait que chaque organisation mette en place une défense en profondeur, combinant la surveillance des dispositifs, leur gestion, l'automatisation et la réaction *(MMAR framework : Monitoring, Management, Automation and Response)* afin de garantir que les menaces soient découvertes et neutralisées rapidement.

Comment se défendre et rester en sécurité face aux cyberattaques liées au COVID-19

Compte tenu de l'augmentation du nombre de cyberattaques liées aux coronavirus, les employés et les organisations devront monter la garde et faire preuve d'une plus grande habileté pour se défendre. Bien entendu, aucune solution ne peut à elle seule nous protéger totalement face à l'ensemble des cyberattaques que les cybercriminels ont dans leur arsenal afin maximiser leur impact. Cependant, l'application d'une stratégie de défense à plusieurs niveaux est toujours très efficace. Cela signifie qu'il est essentiel de déployer divers contrôles de sécurité aussi bien au niveau du réseau et des points d'accès, celui de l'entreprise et ceux des employés *(endpoints)*.

En tant que première ligne de défense, il est crucial d'appliquer des contrôles constants de sécurité du trafic réseau entrant et sortant. Comme deuxième ligne de défense, il est indispensable de déployer une protection contre les logiciels malveillants au niveau des dispositifs d'accès et de stockage en utilisant l'analyse traditionnelle des logiciels malveillants combinée avec l'analyse comportementale. Ainsi, même si un système est compromis, l'attaque peut être détectée et interrompue avant que le mal ne soit fait. Troisièmement, la formation à la sensibilisation à la sécurité joue un rôle important dans le cadre de la stratégie de sécurité globale d'une organisation. En augmentant la sensibilisation, les organisations peuvent réduire considérablement leur exposition aux risques d'attaques par hameçonnage. Le compromis entre la sécurité et la commodité signifie que les employés ne seront pas en mesure de détecter et d'éviter systématiquement toutes les attaques (même de type hameçonnage) les plus ciblées et sophistiquées. Toutefois, la formation, lorsqu'elle est combinée à une solution de sécurité globale et solide de défense en profondeur, offre la protection la plus forte pour garantir que les attaques de hameçonnage ne fassent plus des employés la première de leurs cibles.

De plus, une solution de protection des terminaux, tant sur l'ordinateur portable que sur l'ordinateur de bureau, est essentielle pour garantir la protection des appareils contre les logiciels malveillants et les logiciels de rançon. L'utilisation d'une authentification multi-facteur dans tous les systèmes externes est indispensable. Elle permet en effet non seulement d'assurer une résistance significative contre les attaques basées sur les mots de passe, qui sont les plus courantes, mais constitue aussi un moyen de dissuasion utile contre les attaques de base. Les conseils pratiques suivants doivent être suivis lorsque l'on travaille à domicile :

- Assurez-vous que votre ordinateur portable ou de bureau est équipé des derniers logiciels antivirus ou de protection des points d'accès.
- Soyez particulièrement vigilant contre les attaques de hameçonnage liées au coronavirus et aux logiciels d'accès à distance.
- Veiller à ce qu'un niveau élevé d'authentification soit requis lors de l'accès aux systèmes d'accès à distance et aux vidéoconférences à distance.
- Veiller à ce que, dans la mesure du possible, tous les systèmes externes nécessitant un mot de passe utilisent une authentification à deux facteurs en plus des mots de passe traditionnels.
- Si vous vous connectez au net dans un endroit non fiable, comme un Internet café, utilisez un logiciel VPN pour vous assurer que votre trafic Internet est crypté et protégé contre les écoutes.

Conclusion

Le coronavirus a forcé des millions d'utilisateurs à travailler à domicile. Les cybercriminels sont constamment à la recherche d'un moyen rapide et efficace de compromettre les systèmes à des fins malveillantes. Les particuliers et les organisations doivent faire preuve de plus d'habileté pour se défendre contre diverses attaques ciblées. L'application régulière des correctifs des logiciels, l'utilisation d'une authentification à deux facteurs, la mise en place d'une solution à jour de protection des points d'accès et une sensibilisation permanente à la sécurité sont de loin les moyens les plus efficaces de garder une longueur d'avance sur les cybercriminels. Enfin, la défense en profondeur doit faire partie de l'arsenal global de sécurité des gestionnaires de réseaux et de sécurité. La combinaison de la surveillance des dispositifs, leur gestion, l'automatisation et la réaction *(MMAR framework : Monitoring, Management, Automation and Response)* est sans aucun doute la meilleure pour garantir que les menaces soient découvertes et neutralisées rapidement. ■

Pour une hygiène aussi nécessaire dans le monde digital que dans le monde physique

Auteur : **Mohamed Saad, Président de l'Association des Utilisateurs des Systèmes d'Informations au Maroc (AUSIM)**

Pour notre première action en partenariat avec la revue Cybersecurity Trends, fruit des congrès public-privé "Cybersecurity Dialogues", nous aurions aimé rédiger ces quelques lignes en présentant notre Association, ses réalisations, la richesse des échanges humains qui a abouti à notre présence dans ce volume, entre autres grâce à notre ami et partenaire commun Didier Spella.

Au vu des circonstances, il est de notre devoir de traiter du sujet d'actualité peut-être le plus médiatisé depuis la deuxième guerre mondiale, qu'aucun d'entre nous n'a vécu, bien évidemment…

BIO

Mohamed Saad est un acteur dans le monde des Technologies de l'Information depuis 1991, Digital Evangelist ; Président de l'AUSIM et Directeur du Pôle Ressources de la Bourse de Casablanca, il a opéré dans le secteur du service, de l'industrie et du bancaire. Sur le plan associatif, il est membre fondateur de Isaca-Casablanca, chapitre marocain de l'ISACA, Vice-Président de CCAM (Club de la Continuité d'Activité Marocain), membre du PMI. Il est diplômé de l'INSEA et détenteur d'un MBA, et des certifications CISA, PMP, CRISC, ISO 27001. Mohamed Saad est l'auteur de plusieurs articles sur l'IT Governance, les risques IT, le ROI IT, les standards et référentiels IT et bien d'autres.

Mais une guerre, dites-vous ? C'en est une, comme dirait l'autre. Cette crise sanitaire jamais vécue auparavant, et qui s'est propagée à la vitesse de la lumière, confinant des nations toutes entières, est en train de gagner du terrain et d'engloutir des milliards de dollars de pertes… mais surtout, elle est en train de détruire un capital confort, plaisir et bien-être.

Permettre à nos institutions, d'abord de protéger l'humain en mettant à la disposition de nos collègues les outils nécessaires pour travailler à distance, rester chez soi, et se protéger au maximum du contact avec les autres.

Ensuite, faire en sorte que l'activité des institutions ne s'arrête pas, à travers les outils IT et autres dispositifs digitaux, afin de permettre au business de survivre, car cela a un impact sur l'économie de la nation toute entière.

Fidèle à ses actions et bonnes pratiques, l'AUSIM est en cours de lancement de Webinars qui traiteront des Plans de Continuité d'Activité, y compris sur le plan de la protection de la santé humaine, mais aussi de la sécurité des IT et de la cybercriminalité, un autre fléau qui trouve son terreau de fertilité avec la prolifération des actions de télétravail.

La sécurité digitale sera également traitée car c'est un thème "relativement nouveau" dans notre mode de travail dans notre culture, C'est une urgence aujourd'hui plus que jamais, puisque que la pandémie a ouvert toutes les portes aux cybercriminels, avec une croissance mensuelle d'attaques de plus de 500% par mois au niveau global depuis février. Du jamais vu, ici aussi.

Dans ce cadre, c'est pour l'AUSIM un plaisir que de se joindre à l'effort collectif que constitue la présente publication, éditée en quatre langues et destinée à offrir au plus grand nombre les outils de compréhension numérique nécessaires pour, ensuite, lire et faire bon usage du guide des menaces cyber qui pèsent sur chacun d'entre nous depuis le début de la pandémie.

La vie doit continuer, d'abord en nous armant des mesures sanitaires nécessaires pour sauver l'humanité et, ensuite, en créant une atmosphère d'entraide, entre humains d'abord mais également entre institutions.

L'AUSIM promeut le confinement comme l'une des mesures les plus efficaces pour endiguer ce fléau, et c'est l'avis de la plupart des experts, chercheurs et virologues.

Dieu merci, notre pays a pris les mesures nécessaires à temps afin de limiter et réduire l'impact et la propagation du virus, mais nous, tous, citoyennes et

citoyens, devons faire preuve de civisme, de responsabilité et de respect des consignes des autorités et des institutions de contrôle et de surveillance.

A chacun de nous, dès maintenant, de prendre les mesures d'hygiène digitale afin de profiter de ce moment particulier pour faire évoluer notre degré de maturité en sécurité numérique, qu'elle soit citoyenne ou entrepreneuriale, qu'elle relève de notre vie privée, de nos activités professionnelles ou de la sphère publique.

Dans un moment où nos remerciements vont en tout premier lieu au personnel médical et paramédical et aux agents qui veillent sur la sécurité des citoyens, nous soulignerons le rôle vital de tous ceux qui oeuvrent, à l'instar des inititiateurs de la présente revue, pour que demain soit meilleur, et il le sera In cha Allah. ■

** Vous pouvez visionner l'intégralité du premier Webinar (Webinar AUSIM : PCA et télétravail pour gérer la crise) sur : http://www.ausimaroc.com/webinar-ausim-pca-et-teletravail-pour-gerer-la-crise/*

Une mobilisation sans précédent

Cybersecurity Trends

Auteur : **Laurent Chrzanovski, fondateur et rédacteur en chef de Cybersecurity Trends**

En préparant, fin mars, le volume de *Cybersecurity Trends Italie**, l'idée nous est venue de partager notre article suivi de notre petit guide aux usagers du numérique à de nombreux spécialistes, travaillant dans les Institutions étatiques, mais aussi privées spécialisées dans la cyberdéfense, pour recueillir avis, conseils, données et, *last but not least*, critiques constructives.

Tous ces experts roumains, suisses, français, marocains, italiens et anglais, luttant en première ligne contre la pandémie de cyberattaques 24/7, en croissance exponentielle depuis plus de deux mois, nous ont aidé sans relâche, sacrifiant dans un effort collectif de divulgation positive le peu d'heures libres qui leur sont octroyées quotidiennement.

Ce qui a suivi est dans la même logique, mais tient de ces petits miracles que seuls les temps les plus durs peuvent faire éclore. Constatant le manque de personnel pour informer le grand public autrement que par des "brèves" concernant des attaques ponctuelles, plusieurs Institutions et Associations professionnelles des pays mentionnés nous ont demandé de projeter, concevoir et éditer cette présente édition, dans les langues des citoyens de leurs pays respectifs : le français, l'anglais et le roumain.

Aussi, le 6 avril, les directeurs de toutes ces entités avaient sur leur courriel la demande officielle nécessaire à obtenir leur approbation concernant les partenariats - et permettre aux spécialistes de rédiger les préfaces et contributions que vous pouvez lire ici. Le même jour, l'Ambassade de Suisse en Roumanie décidait d'accorder son égide à l'ensemble de ces trois versions linguistiques, placées sous le Haut Patronage de l'Ambassadeur Arthur Mattli.

Nous sommes le 15 avril, tous les textes ont été reçus et sont en finalisation de traduction ou déjà en cours de mise en page. Une vitesse de réaction inouïe à la hauteur de l'enjeu, puisque la mise est de sauver par la prévention le plus possible d'emplois, en protégeant les entreprises mais aussi la vie privée de tous.

Que toutes les Institutions et Organisations partenaires, que tous les auteurs des textes constitutifs de ce volume et que les dizaines de spécialistes qui nous ont assisté soient ici remerciés, du fond du cœur.

L'ouvrage présent ne vise aucunement à l'exhaustivité. En revanche, il veut susciter autant de réflexions que possible, grâce à la pluralité des points de vue que vous y découvrirez et aux renvois aux approfondissements disponibles en ligne.

Profitons ensemble de ce moment très difficile pour enfin comprendre le numérique, ses indispensables apports à notre quotidien mais aussi ses dangers et la pléthore de pièges qui nous guettent. La résilience paiera très prochainement face au Coronavirus. Mais une résilience "cyber" mûrie par chacune et chacun d'entre nous paiera sur le court, le moyen et le long terme.

Contribuons, tous ensemble, à stopper aussi bien la maladie que sa cohorte de virus digitaux ! ■

**Tous les volumes, y compris le nouveau-né n. 1/2020, sont disponibles en ligne sur le site créé ad hoc par les Postes Italiennes et le GCSEC : www.cybertrends.it/rivista/*

II. Comment en est-on arrivé là ? Sur le terrain et dans nos vies

Vocabulaire stratégique oublié

Auteur : Olivier Kempf

L'article original, réservé aux abonnés, vient de paraître dans le bimensuel LA VIGIE (n. 139, 1er avril 2020 p. 4-6). Pour plus d'informations : www.lettrevigie.com

Nous adressons nos plus chaleureux remerciements à Olivier Kempf pour sa gentillesse et pour l'autorisation donnée de reproduire, traduire et publier en exclusivité ce texte dans les différentes variantes linguistiques de Cybersecurity Trends.

Tous les observateurs l'affirment : la pandémie en cours constitue un point de rupture et il y aura un avant et un après. Il est évidemment trop tôt pour discerner efficacement les traits de ce "jour d'après".

Quelques indices commencent toutefois à se faire jour : constatons prudemment que les affaires géopolitiques reprennent leurs droits, ici ou là, certains acteurs profitant de ce que l'attention est mobilisée par les chiffres de victimes pour relancer dans la discrétion leurs actions.

Nous y reviendrons. Pour l'instant, attardons-nous sur une grande partie du vocabulaire stratégique qui a été oublié, sciemment ou non, par négligence ou changement de priorités.

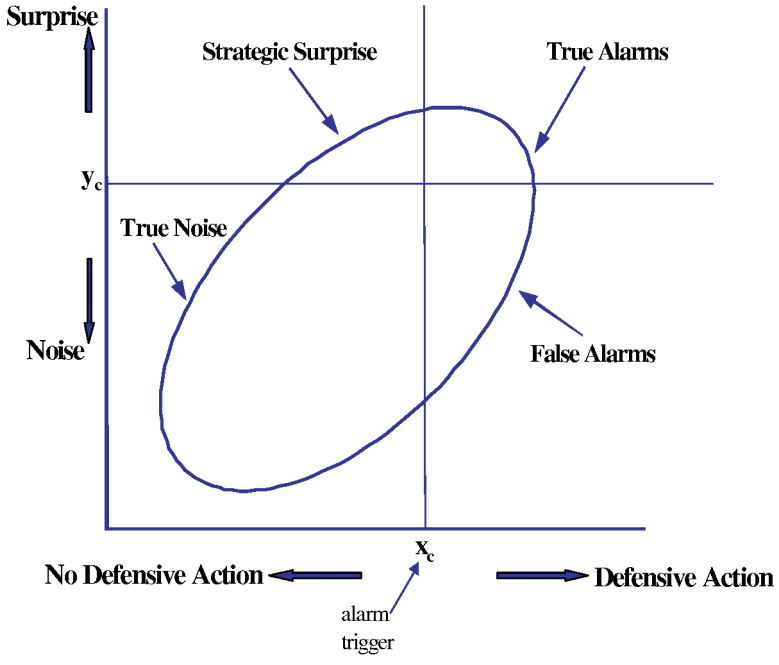
Surprise stratégique

Souvenez-vous: le terme était très en vogue à la suite des attentats de 2001. Nous avions alors tous travaillé sur ce thème, produit des analyses plus ou moins intelligentes, et puis nous étions passés à d'autres expressions, venues comme souvent d'outre-Atlantique :

GWOT, MENA, COIN ou A2AD, par exemple. Promis, nous avions retenu la leçon, nous ne serions plus surpris !

D'ailleurs, on avait anticipé la prochaine surprise stratégique en investissant beaucoup dans la cyberdéfense. Bien sûr, l'affaire de Crimée en 2013 nous avait un peu alarmés, mais tactiquement pourrait-on dire: on avait alors forgé le concept (peu convaincant) d'hybridité.

Mais nous restions dans un cadre convenu et les brillants stratèges dissertaient sur des questions d'opérations multi-domaines.



Le concept de la surprise stratégique : image © Joseph Lampel, Zur Shapira, Judgmental Errors, Interactive Norms, and the Difficulty of Detecting Strategic Surprises, in Organization Science Vol. 12 No. 5 (2015), fig. 1

BIO

Après une carrière militaire où , outre des opérations, il s'est occupé d'affaires internationales et de transformation, le général (2S) Olivier Kempf conseille les entreprises et organisations sur les questions de stratégie digitale et de cybersécurité (Truchements consultants). Auteur de *«Introduction à la cyberstratégie»* (Economica, 2015), il est directeur de publication de La Vigie, cabinet de synthèse stratégique qu'il a fondé en 2014 qui publie une lettre bimensuelle et rédige diverses études pour ses clients.

Certes, ces questions sont importantes (insertion du spatial dans la stratégie, évolutions technologiques, combat collaboratif) et il ne s'agit pas de les oublier: mais elles appartiennent à la théorie stratégique militaire et non à la grande stratégie.

Or, un concept est pertinent s'il s'adapte aussi bien à la stratégie militaire (dans ses niveaux stratégiques, opératifs ou tactiques) qu'à la grande stratégie.

Le concept de surprise appartient indubitablement à cette catégorie. Il devrait donc être l'obsession du stratège. Force est de considérer qu'en la matière, nous avons échoué.

Pourtant, la probabilité d'une pandémie était bien connue. Voici donc un nouveau cas, celui de la surprise qui n'est pas tellement une surprise mais qui a quand même surpris. Les années 2000 avaient connu quelques exemples: le SRAS tout d'abord, mais aussi le H1N1. Or, c'est justement la succession de ces deux crises qui a causé l'impréparation que nous constatons.

Le SRAS en 2003 a été une surprise qui a suscité une grande mobilisation. Lors du H1N1 en 2009, la réaction fut vigoureuse, mais l'épidémie en question fut moins virulente que ce qu'on avait craint.

Il s'en est suivi un débat sur le gâchis et la disproportion de la réaction: ce débat n'aurait pas dû avoir lieu car les autorités avaient alors réagi en contexte d'incertitude et ne connaissaient pas la virulence de la menace. Leur reprocher après-coup d'avoir trop dépensé fut une réaction non stratégique, digne des commentateurs de football après le match.

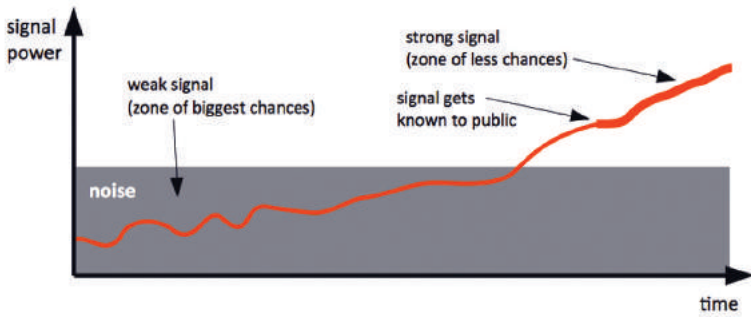
Il reste qu'on a laissé les choses filer pendant une décennie, ce qui nous a conduit à la situation actuelle: du coup, cette pandémie apparaît comme une surprise stratégique.

Elle est stratégique au regard de ses conséquences car l'autre caractéristique de la surprise stratégique n'est pas seulement qu'elle soit surprenante, mais qu'elle soit stratégique du fait de ses conséquences…

Signaux faibles

Autre vocable hérité du 11 septembre, la notion de signaux faibles. Il ne s'agit pas de revenir sur les propos de Rumsfeld qui, à son époque, évoquait les "inconnus inconnus" (unknowns unknowns), ni même de revenir sur l'écoute des services de renseignements: une information ne vaut que par la capacité d'écoute du décideur.

Mais en l'occurrence, constatons que les signaux n'étaient pas faibles, mais forts. Rappelons ici les critères évoqués par le plan de réaction à une pandémie de grippe, énoncés par le SGDSN en 2009 : *Les signes d'alerte pouvant justifier l'utilisation de cette fiche sont les suivants :*



L'utilité de comprendre les signaux faibles avant que les chances de contrer un phénomène ne s'amenuisent © Robert Eckhoff, Mark Markus, Markus Lassnig, and Sandra Schön, No Outstanding Surprises when Using Social Media as Source for Weak Signals? First Attempt to Discuss the Impact of Social Media Sources to Detect Surprising Weak Signals. In : Proceedings of The Ninth International Conference on Digital Society (ICDS) in Lisbon, Portugal, 2015,l fig 1

brusque signalement par des sources concordantes, quelque part dans le monde d'une extension de grande ampleur de la maladie avec un grand nombre de cas de syndrome grippal (supérieur à la centaine), avec suspicion d'extension rapide (forte contagiosité), avec une mortalité anormalement élevée et/ou une gravité clinique ou biologique nécessitant une hospitalisation sensiblement plus fréquente que pour la grippe saisonnière.

Il ne s'agissait pas d'être grand clerc : dès le 5 février, La Vigie signalait le virus, soit plus d'un mois avant les premières mesures du gouvernement.

Conclusion : si non seulement les signaux forts ne sont pas entendus, combien moins le seront les faibles: au fond, ils n'existent pas.

Stratégie des moyens

Nous avons évoqué la question de l'alignement des moyens sur les fins et les voies: il est ainsi d'usage d'évoquer la stratégie des moyens pour désigner la façon de mobiliser l'appareil industriel pour acquérir les ressources dont les armées ont besoin.

Or, ce que cette crise nous apprend, c'est qu'une stratégie civile nécessite aussi une stratégie des moyens.

L'analogie est valable dans toutes les dimensions: il convient d'avoir des stocks, ici de munitions et de carburant, là de masques médicinaux, de respirateurs et de tests ; mais il faut également une stratégie industrielle pour permettre une souveraineté de fabrication : industrie de défense dans un cas, industrie chimique ou sanitaire dans l'autre.

Pointons ici à quel point la notion de "politique industrielle" a été dévalorisée ces dernières décennies: la politique économique de confiance à la mondialisation a fait passer ceux qui s'en émouvaient pour des esprits chagrins et attardés.

La notion d'intelligence économique retrouvait un peu de faveur depuis deux ou trois ans, à la faveur des décisions radicales de Donald Trump. Nul doute que demain, la notion d'industrie stratégique sera en vogue.

Défensive et innovation

Bien sûr, il n'y a pas de guerre contre le virus. La formule peut éventuellement passer pour une métaphore, mais elle est difficilement

acceptable quand il s'agit d'user du vocabulaire guerrier pour favoriser une mobilisation nationale qui n'a pas été spécialement encouragée auparavant.

Accessoirement, les appels à "l'armée", formulés ici ou là, montrent à quel point l'imaginaire commun n'a aucune idée de la faiblesse résiduelle des moyens militaires, effet de trois décennies d'optimisation, comme on disait alors. La mise en scène de l'appel aux armées inquiète plus qu'elle ne rassure.

Pourtant, qu'il y ait un front, celui des hôpitaux, nul n'en doute. Observons d'ailleurs la capacité d'innovation, avec des moyens du bord, l'aménagement en urgence de chambres de réanimation, la confection de masques ou d'appareils, la mise en œuvre de médications d'urgence: on se croirait, toutes choses égales par ailleurs, en présence de la formidable inventivité des armées (et de leur Service de santé) lors de la Première guerre mondiale.

Masques de plongée (snorkel) utilisés dans les hôpitaux français, belges et canadiens © radiocanada

La défense (coup d'arrêt, freinage, contrôle, disions-nous) suscite également des adaptations dans la durée.

Liberté de mouvement

Qui ne connaît les trois principes de la stratégie, chers à Foch ? L'un d'eux est la liberté de mouvement.

Avec le confinement, la population se voit privée de cette liberté de mouvement: mais c'est pour entraver la liberté de mouvement du virus (on parlerait de liberté de contagion).

Il est curieux et paradoxal que notre seule stratégie défensive consiste à s'immobiliser afin de fatiguer la propagation. Mais la logique est respectée: cette pandémie a une dimension mondiale due à l'exacerbation des flux, causés par la mondialisation. Logiquement, cesser les flux permettra de freiner le virus.

Résilience

La résilience: encore un mot qui a été fort à la mode, importé du monde psychologique par les stratégistes. Mais alors qu'à l'origine le terme désigne une capacité individuelle de surmonter les épreuves, les stratégistes l'ont appliqué à des ensembles collectifs.

Notons qu'ils ne parlaient pas de nations mais de "résilience des populations". Il s'agissait d'expliquer comment elles allaient pouvoir surmonter les attaques terroristes, puisqu'il était entendu que ces dernières voulaient instiller la peur, modifier les opinions collectives et parvenir ainsi à de nouvelles politiques.

Or, très curieusement, voici que ce virus (que bien sûr nous ne désignerons pas d'ennemi) n'a pas fait peur, dans un premier temps. Au contraire, on l'a minoré: une "grippette", qui n'allait pas nous empêcher d'aller au théâtre, comme conseillé par les plus hautes instances.

Et puis les choses se sont aggravées et l'on a parlé de guerre et aussitôt après, de résilience. Car si la population française paraît moins émue que lors des attentats de 2015, constatons qu'elle subit plus profondément les atteintes de la pandémie: outre le confinement, un bilan humain qui se compte déjà (en France) en milliers de morts.

Certes, une grippe saisonnière, les suicides ou l'alcool causent beaucoup de décès. Un cynique trouverait qu'à la fin, cela n'affecterait pas tant que ça l'équilibre du pays et que la résilience est donc assurée.

C'est ne pas voir les dégâts économiques que cela suscitera. De ce point de vue, il est bien moins sûr que l'on pourra parler d'une résilience.

La convalescence sera certainement bien plus longue. Ce n'est pas l'opération Résilience (mobilisation des moyens militaires contre le C-19 en France) qui y suffira. ■

Militaires français engagés dans l'opération résilience © Europe1

COVID#19 ou quand la cyber-sécurité aurait beaucoup à apprendre aux gouvernements en matière de gestion de crise

Auteur : Laurent Chrzanovski

Sur le terrain : la politique du chaos et l'idéologie du "chacun pour soi".

La gestion européenne du COVID#19 (Coronavirus) est catastrophique. Plans d'urgence nationaux avec mesures de plus en plus restrictives qui se succèdent à un rythme effréné, fermeture des frontières, isolement des individus, populations en état de siège et, en partie, paniquées.

Tout cela est doublé d'un cynisme politique rarement atteint. Pour les gouvernements, l'urgence est triple : lutter efficacement contre l'expansion du virus, faire en sorte que l'économie fonctionne au mieux et ne perde pas sa part de popularité électorale.

Dans les "think-tanks" des dirigeants européens, ces trois fronts, qui ont chacun des besoins clairs et précis, sont totalement contradictoires. Le résultat est palpable, nous vivons dans un chaos où chaque pays applique des lois d'urgence, des mesures sanitaires et des utilisations de médicaments différents, exactement comme vient de le décrire Giorgio Agamben : *"Jamais auparavant nous n'avions assisté au spectacle, typique des religions en temps de crise, d'opinions et de prescriptions différentes et contradictoires, allant de la position hérétique minoritaire (également représentée par des scientifiques prestigieux) de ceux qui nient la gravité du phénomène au discours orthodoxe dominant qui l'affirme et, cependant, diverge souvent radicalement quant à la manière de le traiter. Et, comme toujours dans ces cas, certains experts ou soi-disant experts parviennent à s'assurer la faveur du monarque qui, comme à l'époque des conflits religieux qui divisaient le christianisme, prend partie selon ses propres intérêts pour tel ou tel courant et impose ses mesures"* (1).

La politique du chaos : Korczowa - Krakovets, point de passage à la frontière entre la Pologne et l'Ukraine, 28 mars 2020. En pleine crise COVID#19, des dizaines de milliers de citoyens ukrainiens affluent pour rentrer dans leur pays avant que les frontières ne soient fermées. © Novynarnia.

Un bar à Stockholm et un second, à Chicago, vendredi 10 avril. © Getty

La population est laissée à la merci d'une explosion d'informations alarmistes, doublée de fake news et, de plus en plus, abandonnée à la situation parfaitement exprimée par la devise de Noam Chomsky : *"La population générale ne sait pas ce qui se passe et elle ne sait même pas qu'elle ne le sait pas".*

BIO

Titulaire d'un doctorat en archéologie romaine obtenu à l'Université de Lausanne, d'un diplôme de recherche postdoctorale en histoire et sociologie de l'Académie roumaine des sciences et d'une habilitation UE à diriger des doctorats en histoire et en sciences connexes, Laurent est professeur (chaire) à l'École doctorale de l'Université de Sibiu et à l'Université de Varsovie (invité permanent). Il donne régulièrement des cours postdoctoraux dans plusieurs grandes universités de l'UE. Il est l'auteur/éditeur de 32 livres, de plus de 150 articles scientifiques et d'autant d'articles grand public. Dans le cadre de la cybersécurité, Laurent Chrzanovski est membre du groupe d'experts de l'UIT. Il a fondé et gère les plateformes annuelles «cybersecurity dialogues», organisées en partenariat avec les plus hautes organisations publiques et privées de chaque écosystème (Roumanie, Italie, Suisse). Dans le même esprit et avec les mêmes partenariats, il est co-fondateur et directeur de la première revue trimestrielle gratuite de prévention en cybersécurité, publiée en roumain dès 2015 et également dans ses versions italienne et anglaise, depuis 2016 et 2017. Ses principaux domaines d'étude sont axés sur la relation entre les comportements humains et le monde numérique, ainsi que sur l'assurance de trouver le juste équilibre entre sécurité et vie privée pour les citoyens en ligne.

La collaboration européenne et internationale, la seule qui pourrait vraiment faire face à l'épidémie, est presque inexistante, comme l'a magistralement souligné Yuval Noah Harari : *"Je pense que le pire est la désunion que nous constatons dans le monde, le manque de coopération, de coordination entre les différents pays. Et le manque de confiance, tant entre les États qu'entre les populations et les gouvernements. (...) Ce qui me fait vraiment peur, c'est le manque de leadership et de coopération. Et ce que les gens devraient comprendre, c'est que la propagation de l'épidémie dans chaque pays menace le monde entier, car si elle n'est pas contenue à temps, le virus évoluera. C'est peut-être l'un des pires scénarios avec ce type d'épidémie : une évolution rapide du virus".* (2).

Pire encore, dans les pays aux frontières fermées, où, parmi les mesures de santé publique, la quarantaine (isolement) totale des citoyens a été institutionnalisée, nous assistons à un véritable coup d'État dicté par l'incapacité à identifier et à isoler les foyers du virus sur le terrain faute de tests suffisants. Cela crée une

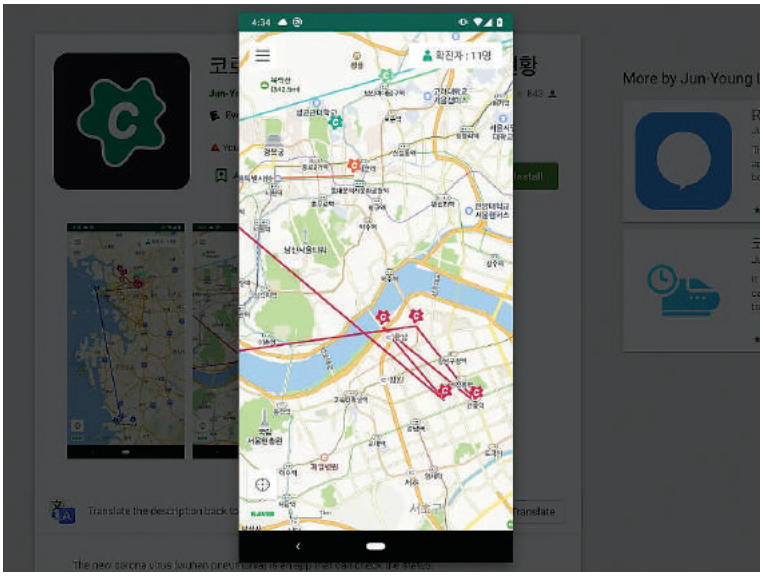
psychopathologie où le parent, le voisin, l'ami deviennent méfiants et une frontière doit être créée autour de chaque individu, comme l'explique bien Michel Onfray : *"Or, qu'est-ce que ce confinement sinon l'invitation à fabriquer autant de frontières qu'il y aura de Français ? La frontière nationale n'est pas bonne, mais la frontière qui sépare de son prochain est présentée comme la solution, la seule solution nous dit-on. (…) Maastricht tousse, crache et menace l'embolie".* (3)

Les démocraties face à la tentation de la surveillance de masse

Ces mesures ne sont pas les seules à nous faire réfléchir sur notre avenir, et en premier lieu sur l'avenir numérique, puisque de nombreux gouvernements utilisent désormais nos "smartphones" pour contrôler notre localisation, comme l'avait déjà prévu Slavoj Žižek : *"L'épidémie provoquée par le coronavirus sert à justifier et à légitimer des mesures de contrôle et de régulation des populations jusqu'alors impensables dans une société démocratique occidentale - l'enfermement total de l'Italie n'est-il pas un fantasme totalitaire ? Il n'est pas surprenant que la Chine (qui a déjà fait un usage massif des nouvelles technologies à des fins de contrôle social) s'avère être la mieux équipée pour faire face à une épidémie catastrophique - du moins à en juger par ce qui semble être la situation actuelle. Cela signifie-t-il que la Chine incarne notre avenir, au moins à certains égards?"* (4).

Yuval Noah Harari, dans son dernier essai, va beaucoup plus loin, en soutenant que la possibilité que la surveillance liée au Coronavirus établie dans bien des démocraties soit ensuite utilisée quotidiennement : *"Pour arrêter l'épidémie, des populations entières doivent respecter certaines lignes directrices. Il existe deux moyens principaux pour y parvenir. (...) Aujourd'hui, pour la première fois dans l'histoire de l'humanité, la technologie permet de surveiller tout le monde en permanence. Il y a cinquante ans, le KGB ne pouvait pas suivre 240 millions de citoyens soviétiques 24 heures sur 24, ni espérer traiter efficacement toutes les informations recueillies. Le KGB s'appuyait sur des agents et des analystes humains et ne pouvait tout simplement pas placer un agent humain pour suivre chaque citoyen. Mais désormais, les gouvernements peuvent s'appuyer sur des capteurs omniprésents et des algorithmes puissants au lieu de s'appuyer sur des spectres de chair et de sang. (…)*

De nombreuses mesures d'urgence à court terme deviendront régulières. C'est la nature des situations d'urgence. elles font avancer rapidement les processus historiques. Les décisions qui, en temps normal, pourraient nécessiter des années de délibération, sont prises en quelques heures. Des technologies immatures et même dangereuses sont mises en service, car les risques de ne rien faire sont plus importants. Des expériences sociales à grande échelle démontrent leur utilité dans des pays entiers. Que se passe-t-il lorsque tout le monde travaille à la maison et ne communique qu'à distance ? Que se passe-t-il lorsque des écoles et des universités entières fonctionnent en ligne ? En temps normal, les gouvernements, les entreprises et les conseils scolaires n'accepteraient jamais de mener de telles expériences. Mais ce ne sont pas des temps normaux. En ces temps de crise, nous avons deux choix particulièrement importants à faire. Le premier est celui de l'option de la surveillance totalitaire versus la responsabilisation des citoyens. Le second est celui de la tentation de l'isolement nationaliste versus la solidarité mondiale". (5)



Suivi en temps réel, Corée du Sud © The Conversation
Applications du gouvernement sud-coréen montrant les itinéraires et les lieux où se trouvent les personnes infectées © Businessinsider

Cybersécurité : un domaine mondial avec des acteurs en dialogue permanent

C'est ici que commence notre glissement vers la cybersécurité et sa coordination, exemplaire par rapport à la plupart des choix sanitaires et sécuritaires gouvernementaux.

La raison est simple : aux dommages économiques purement liés aux conséquences du virus - que diverses sources indiquent comme étant les symptômes d'une récession bien plus grave que la crise de 2007, il faudra ajouter les dommages supplémentaires apportés par la cybercriminalité.

Pour donner une dimension métaphorique à ce qui se passe dans le monde numérique, si au moment de la rédaction de ce texte, le COVID#19 était un virus multimédia unique, le nombre de ses victimes (asymptomatiques, symptomatiques, guérissables ou non) aurait au moins quatre zéros de plus que les personnes qui ont contracté la maladie. Pire encore, en ne s'attaquant pas à un seul système (comme le système respiratoire humain dans le cas du vrai virus), c'est comme si chaque partie interne et externe de notre corps était en danger.

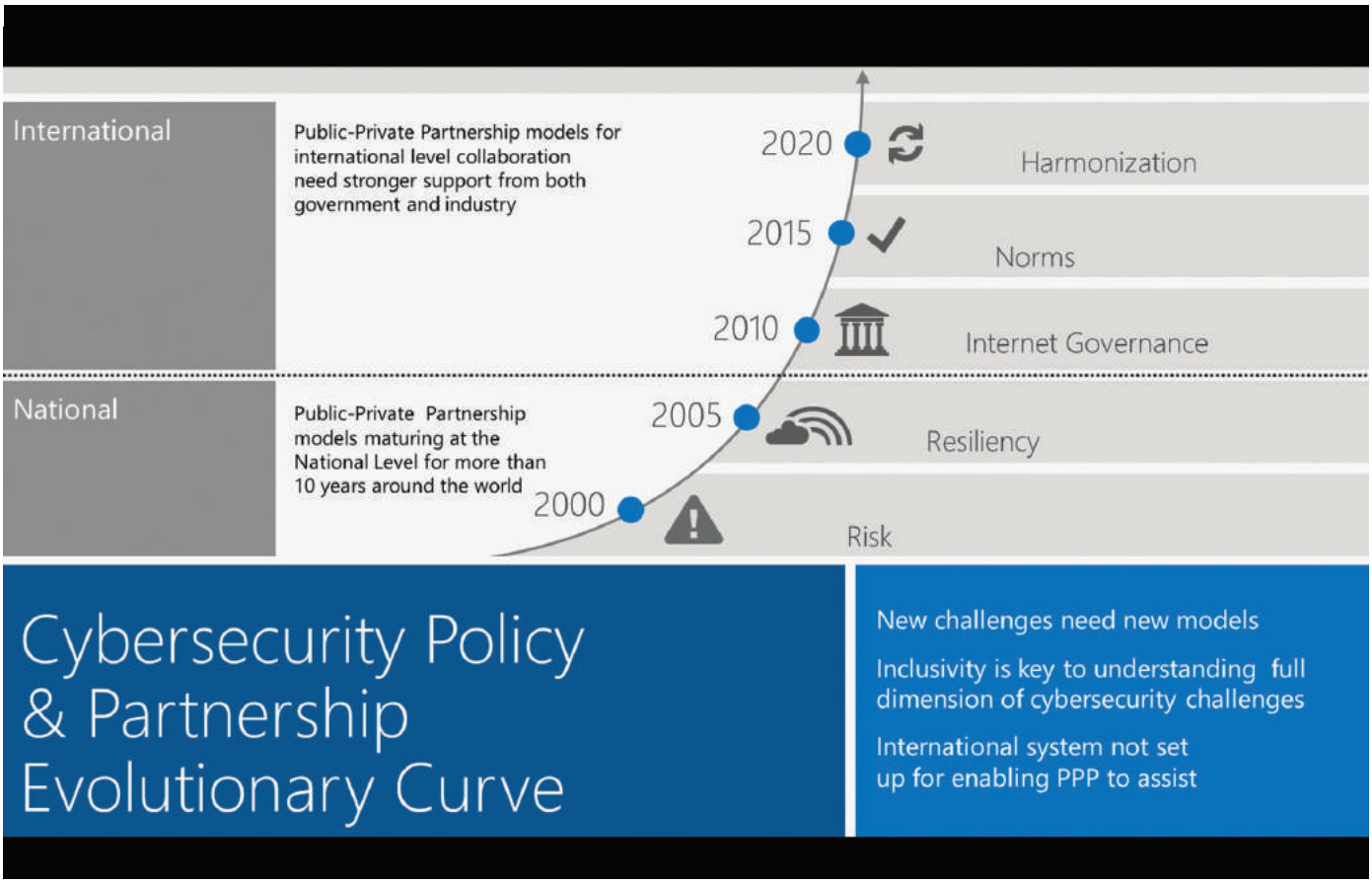
Cette mobilisation globale de tous les secteurs, dans un véritable partenariat public-privé, qui était l'objectif - très optimiste - fixé pour 2020 par Microsoft dans un rapport de 2012, prend forme sous nos yeux.

La naissance de ce mouvement est purement économique et, en même temps, liée à la stratégie des Etats les plus avancés et des compagnies de sécurité. Tout événement problématique, même "mineur" (inondation à petite échelle, incendie, grèves dans les secteurs vitaux) est immédiatement suivi de tentatives multiples de cyber-attaques, et ce depuis au moins 10 ans.

Aussi, même si le virus avait été contenu dans la mégalopole de Wuhan, il aurait connu un tsunami d'attaques. En effet, tout événement majeur se produisant en Chine ou aux États-Unis, a un impact économique, politique et... cybernétique mondial. Aussi, dès les premiers cas connus début février, les experts en sécurité numérique de tous les pays se sont mobilisés.

Au fur et à mesure de l'expansion de la pandémie, le pire des scénarios s'est réalisé - et se poursuit encore - l'exploitation par des groupes de cybercriminels de la médiatisation de la pandémie, en suivant de près son évolution et en s'adaptant rapidement: des attaques à grande échelle, des stratégies multiples, utilisant tous les moyens et toutes les langues, pour essayer de toucher tous les types d'utilisateurs et tous les outils possibles (hard, soft, cloud) - pour les données techniques, voir le rapport très détaillé du groupe Insikt, *"Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide"* (6).

Ces opérations avaient déjà été menées, mais avec moins de succès – précisément parce qu'il n'y avait pas eu de réactions gouvernementales aussi puissantes qu'incohérentes au niveau mondial lors du premier pic de l'épidémie d'Ebola (2002-2003), comme l'expliquent parfaitement François Mouton et Arno de Coning dans l'introduction de leur toute récente étude sur ce qui se passe dans le monde virtuel (7).



L'évolution espérée par Matt Thomlinson dans Cybersecurity Norms and the Public Private Partnership : Promoting Trust and Security in Cyberspace © Microsoft, 05.10.2012

La différence avec la gestion des épidémies : de véritables PPP internationaux ou même mondiaux

Pour faire face à une panoplie d'attaques visant des mineurs aux adultes, tentant de s'insinuer dans toutes les activités privées et professionnelles, la grande différence entre la gestion de la pandémie virale *humaine* et celle de la *cyberpandémie virale* est que dans cette dernière, le facteur politique est absent.

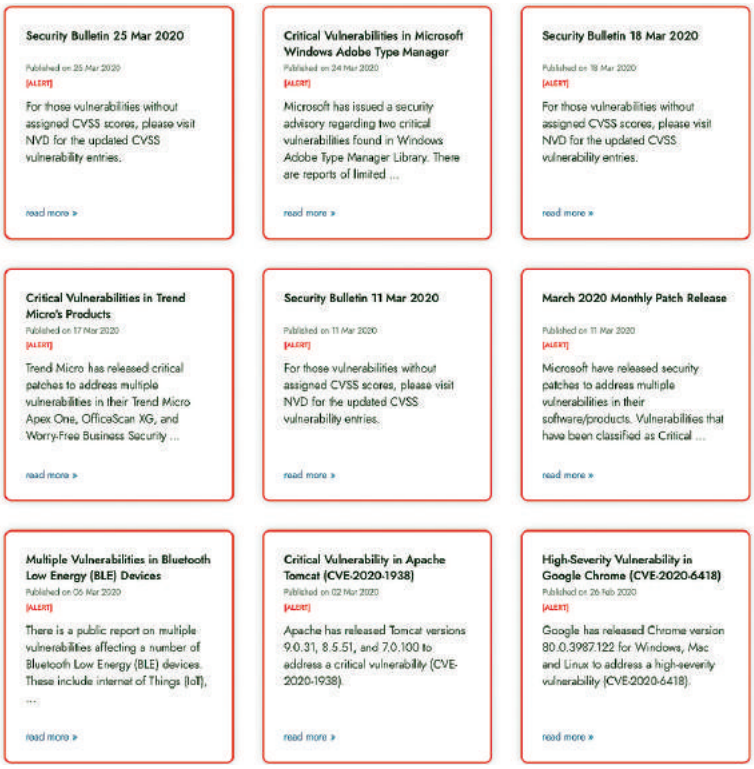
Ce sont les agences spécialisées des différents États qui sont chargées de contrer les attaques et de limiter les dommages causés aux citoyens, aux entreprises et, *enfin et surtout,* aux outils numériques des institutions publiques de leur pays. La cohérence, la rigueur, la très haute qualification et l'interaction interdisciplinaire constante de ceux qui s'occupent, partout dans le monde, de l'urgence numérique actuelle sont, en comparaison, aux antipodes de ce que nous voyons sur le front "physique" et humain.

Comme toujours, on remarquera la proactivité des pays qui sont à l'avant-garde dans la publication immédiate non seulement des nouvelles vulnérabilités des matériels et des logiciels (ainsi que des correctifs développés par les fabricants respectifs), mais aussi dans la description, d'abord généraliste puis, le plus rapidement possible, technique, des différents logiciels de rançon, des virus et des "zero-days", comme **Singapour**, qui possède à notre avis le CERT le plus dynamique au monde en termes de concentration, de tri et de diffusion de l'information, excellant dans la clarté et la synthèse des éléments-clé (8).

Il convient de noter que SingCert ne fait pas seulement partie du département de cyber-sécurité des services de renseignement de l'État, mais qu'il a un nombre record de collaborations aussi bien avec des États tiers qu'avec des entreprises privées, des grandes aux moyennes. Un modèle d'efficacité.

En outre, l'efficacité du petit État asiatique a épaté la planète aussi sur le plan sanitaire. Fort de l'expérience de la gestion du SRAS, nous rappelons que Singapour est, avant Taïwan et Hong Kong, le pays qui a le mieux géré la crise et qui a également réussi à contenir le virus humain, sans confinement de la population et avec crèches, écoles et entreprises ouvertes (9).

À l'autre bout du monde, les États-Unis d'Amérique ont multiplié les efforts et ont réussi à faire un saut quantique qualitatif que peu de pays européens ont atteint: évitant d'innombrables recherches et consultations de sites web publics et privés, l'ONG **Staysafeonline** propose depuis un mois une *"Bibliothèque de ressources sur la cyber-sécurité COVID-19"* (10), très utile et constamment mise à jour. Extrêmement claire, elle comporte trois sections: les rapports d'urgence et les conseils rédigés



SingCERT
Singapore Computer Emergency Response Team

La page "news" de Singcert et une école maternelle à Singapour, 24 mars © Axios

par les institutions d'Etat, les rapports des entreprises de sécurité et des articles spécialisés triés sur le volet et issus des meilleures revues cyber. Les communiqués de presse succincts, en revanche, se trouvent dans le *flux d'informations* spécial consacré à chacune des quatre cibles principales : enfants, adultes, professionnels, entreprises.

L'explication est simple: Staysafeonline est une émanation de la **National Cybersecurity Alliance**, un groupe de travail très puissant qui comprend le Department of Homeland Security et presque toutes les entreprises spécialisées en sécurité , grandes et moyennes entreprises, ainsi que les associations de white hats et les universités. Cette alliance est ainsi à considérer à ce jour comme l'écosystème PPP (partenariat public-privé) le

La page de la bibliothèque de ressources sur la sécurité de COVID-19 © Staysafeonline

plus efficace au monde, à l'exception des cyber-partenariats dédiés à des niches (infrastructures critiques, industries ou secteurs particuliers tels que l'aviation, les banques, les producteurs/fournisseurs d'électricité etc.).

Un seul exemple pour illustrer le front constitué pour contrer la masse des attaques

Pour faire face au siège total de tous les objets connectés et de leurs utilisateurs, partout dans le monde, la réponse la plus impressionnante est née le mercredi 25 mars. Le co-fondateur du célèbre congrès DefCon, Marc Rogers, a créé la La **COVID-19 Cyber Threat Intelligence (CTI) League (CTI)**, déjà rejointe par 400 experts de haut niveau de plus de 40 pays, choisis par cooptation et sur une base totalement volontaire.

La Ligue CTI a déjà signé des protocoles de collaboration mutuelle avec de nombreux États, principalement le Canada, ou directement avec leurs agences de cyber-intelligence. Laissant de côté les logiciels malveillants et les "zero days" sophistiqués, qui sont maintenant surveillés et disséqués par le groupe en temps réel, Rogers a motivé la création de ce groupe d'élite en faisant remarquer : *"je n'ai jamais vu un tel volume de phishing. Je vois littéralement des messages de phishing dans toutes les langues connues de l'homme"*. Et grâce à son idée de coopter les meilleurs, des white hats aux plus hauts responsables de cyber-sécurité des grandes multinationales en passant par les spécialistes des sociétés de sécurité, après seulement deux jours, le même Rogers a déclaré qu'il n'avait *jamais* vu autant d'ouverture de la part des agences d'État et a conclu : *"Je n'ai jamais vu ce niveau de coopération, j'espère qu'il se poursuivra après, parce que c'est une belle chose à voir."* (11). Les résultats de la Ligue, qui ne veut pas de publicité, auront sans doute des effets aussi rapides qu'efficaces, sans que l'utilisateur lambda ne s'en rende compte.

Le secteur privé au travail 24/24 et 7/7

Outre les efforts collectifs mentionnés, il y a aussi les entreprises spécialisées, qui proposent chaque jour de nouveaux rapports détaillés, établis par leurs équipes, qui sont actives sur tous les continents. Il n'est pas nécessaire de dresser ici une liste, qui ne saurait être exhaustive, car la meilleure façon de connaître et d'accéder ensuite aux dernières informations disponibles pour tous est de lire les articles quotidiens offerts par les magazines spécialisés en ligne, comme par exemple que les excellents textes de Montalbano (12), Pilkey (13), Lakshmaman (14) ou, en italien, l'excellent texte de Salvatore Lombardo (15) avec des conseils et des liens utiles. ■

Notes :

(1) Giorgio Agamben, Riflessioni sulla peste, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste) (passage cité: traduction de l'auteur)
(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/ (passage cité: traduction de l'auteur)
(3) Michel Onfray, Berezina, in Les Observateurs, 17.03.2020 (https://lesobservateurs.ch/2020/03/17/michel-onfray-berezina/)
(4) Slavoj Žižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plaît ! in Le Nouvel Observateur, 18.03.2020
(https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)
(5) Yuval Noah Harari, Il mondo, dopo il Coronavirus, in Ottimisti e Razionali, 22.03.2020
(http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/) (passage cité: traduction de l'auteur)
(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020
https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf
(7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020)
www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape
(8) https://www.csa.gov.sg/singcert
(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020
https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html
(10) Stay Safe Online: COVID-19 Security Resource Library
https://staysafeonline.org/covid-19-security-resource-library/
(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020
https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049
(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020
https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/
(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020
https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/
(14) Ravie Lakshmanan: Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020
https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html
(15) Salvatore Lombardo: L'allarme: Coronavirus, in aumento attacchi cyber, phishing e malspam: consigli per difendersi, in Cybersecurity360, 26.03.2020
https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

III. L'impact digital du COVID#19 : un tsunami d'attaques. Explications.

Le COVID-19 et la cybersécurité

Auteur : Marc-André Ryter

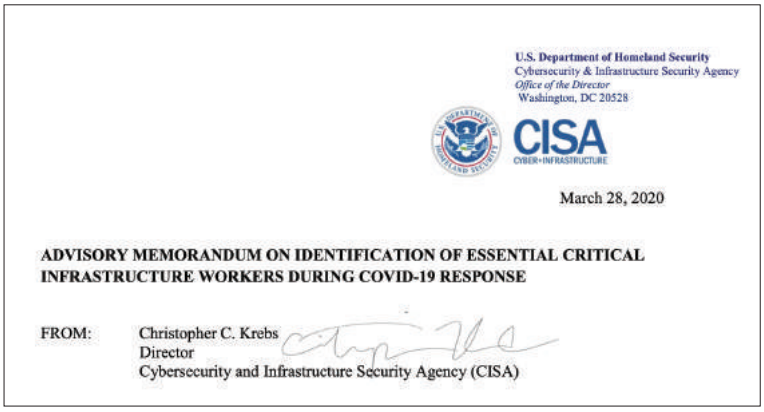
La situation engendrée par le COVID-19 livrera des enseignements dans un grand nombre de domaines qui vont du traitement hospitalier à la gestion de crises en passant par les capacités de production autonomes minimales nécessaires dans chaque pays. Il faut espérer que ces enseignements déboucheront sur la mise en œuvre de mesures concrètes.

Il est en effet légitime de se demander comment les gouvernements ont à ce point pu être surpris, alors que depuis près de deux décennies, les pandémies s'enchaînent régulièrement, avec un impact non-négligeable sur les populations. Nous faisons référence ici en particulier à l'épidémie due au SRAS en 2002-2003, suivie par celle de la grippe porcine H1N1 en 2009-2011 puis par Ebola en 2014. Et ce ne sont pas les seules.

Ce qui nous intéresse ici, ce sont les similitudes et les liens entre cette crise et la cybersécurité. En premier lieu, mentionnons l'environnement instable et générateur de risques. Dans un tel environnement, la complexité, le besoin accru de sécurité, le contrôle de l'information, le contrôle des produits et des comportements et la sécurité du traitement des données sont des paramètres qu'il faut gérer. Tant dans le cyberespace qu'actuellement, il faut trouver des solutions flexibles, rapides, coordonnées et efficaces. On retrouve dans la crise sanitaire actuelle les mêmes enjeux que dans le cyberespace: une compétition globale, la nécessité

d'innover rapidement et le besoin de pouvoir intégrer les secteurs publics et privés.

Les liens entre les deux domaines se retrouvent dans les risques qui les menacent. En premier lieu la fragilité des réseaux et à leur fiabilité. Celles-ci sont mises à rude épreuve par la dépendance envers les nombreux partenaires extérieurs. Le risque de voir la conduite perturbée par des



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

CISA
CYBER+INFRASTRUCTURE

March 28, 2020

ADVISORY MEMORANDUM ON IDENTIFICATION OF ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS DURING COVID-19 RESPONSE

FROM: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

Les pages de conseils et de prévention se multiplient sur le site du Department of Homeland Security dédié aux infrastructures critiques (CISA - www.cisa.gov). Ici l'en-tête de la dernière lettre du 28 mars signée par le directeur de l'Agence.

BIO

Expert en politique de sécurité, le colonel Marc-André Ryter travaille pour l'état-major de l'armée suisse. Il a suivi une formation de base en sciences politiques avant de se spécialiser dans les études de sécurité. Il est aussi diplômé du collège de défense de l'OTAN à Rome. Il suit et étudie les évolutions technologiques qui peuvent s'avérer pertinentes pour les forces armées pour en déduire les conséquences sur la doctrine militaire.

systèmes défaillants est aussi élevé dans le milieu sanitaire que dans les autres domaines de la vie publique. Les acteurs malveillants du cyberespace sont capables très rapidement de profiter de nouvelles vulnérabilités temporaires. Les attaques redoublent et elles sont spécifiquement développées en fonction des craintes de la population. Les manipulations et fake news se multiplient, tout comme les fraudes en tous genres. Cette désinformation peut avoir un impact important sur la société et sur le comportement des gens, et donc sur les infrastructures critiques.

La lenteur de la réaction ne fait qu'aggraver la situation. L'interprétations des signaux faibles et forts reste souvent lacunaire, ce qui ralentit le passage de l'analyse des renseignements à l'action. Cette réaction est rendue difficile par le système de production en flux-tendu de l'économie. Les entreprises ainsi que les institutions publiques ne disposent plus que de ce dont elles ont immédiatement besoin, quantitativement et qualitativement. Il n'y a plus ni stocks ni réserves. La résilience des systèmes économiques et sanitaires doit être améliorée. La situation actuelle montre l'étendue de nos dépendances, en particulier en ce qui concerne les sources d'informations et les canaux d'échanges de données. Il y a un décalage important entre la réalité et la perception par la population.

Le télétravail est une mesure importante prise par les gouvernements pour faire face à la propagation du COVID-19. Il nous montre à quel point nous sommes dépendants des réseaux, de leurs capacités de

Country or State	Traffic Change	DL Speed Change
France	↑ 38.4%	↓ 13.9%
Italy	↑ 109.3%	↓ 35.4%
Japan	↑ 31.5%	↑ 9.7%
Spain	↑ 39.4%	↓ 8%
United Kingdom	↑ 78.6%	↓ 30.3%
USA - California	↑ 46.5%	↑ 1.2%
USA - Michigan	↑ 37.9%	↓ 16.1%
USA - New York & New Jersey	↑ 44.6%	↓ 5.5%

Augmentation du trafic en mars 2020 et réduction de la vitesse
© Fastly https://www.fastly.com/blog/how-covid-19-is-affecting-internet-performance

transmissions de données et donc de leur bon fonctionnement. En raison du télétravail, les échanges de données ont augmenté de façon exponentielle, et de ce fait les vulnérabilités qui leur sont liées.

Les crises comme celle que nous vivons ouvrent de nombreuses et nouvelles brèches pour les cybercriminels. La quantité de biens achetés via internet explose. De nombreux acteurs recherchent des solutions digitales à leurs nouveaux problèmes d'écoulement de marchandises ou de déplacements. Les cybercriminels profitent de cette état de faiblesse et des craintes de la population. D'un côté, ils multiplient les attaques connues, souvent sous la forme de courriels d'apparence officielle qui sont censés rassurer. De l'autre côté, les cybercriminels organisent des fraudes massives en tous genres principalement concernant la vente de biens particulièrement recherchés.

La protection des données est essentielle. Durant les crises, la collecte de données s'accroit, tant par les particuliers que par les autorités. Le contrôle et la protection doivent être assurés, de même que l'utilisation et éventuellement aussi l'effacement lorsque les données ne seront plus utiles. Les menaces déjà existantes, comme par exemple les attaques classiques, du type rançongiciels, peuvent avoir des conséquences dramatiques lorsqu'elles bloquent par exemple le fonctionnement d'un hôpital.

A l'exemple de la crise du COVID-19, ***il est impératif de comprendre pourquoi la sécurité dans le cyberespace représente une nécessité absolue***. Elle seule permet de se protéger contre les agissements des cybercriminels et surtout, d'assurer le bon fonctionnement des réseaux et la disponibilité des informations indispensables. La gestion et la maîtrise des crises doit pouvoir s'appuyer sur un cyberspace sûr. Il s'agit d'éviter les conséquences négatives sur le long terme en développant la coopération entre tous les acteurs afin d'assurer la cohérence et la similarité des mesures prises.

Cette nécessité de sécurité, cette coopération entre acteurs ainsi que le devoir de partager et de promouvoir une base de connaissances défensives au plus grand nombre, voilà la raison d'être de ce volume spécial, vital en ce moment particulier. Grâce la qualité et à la diversité des contributions recueillies, nous sommes convaincu qu'il restera une base de réflexion précieuse lors de la sortie de crise qui, tôt ou tard, va commencer à s'amorcer. ■

Les limites des plans actuels de cyberdéfense et le besoin de repenser le numérique

Auteur : Didier Spella

Problématique

La crise actuelle nous plonge dans un état unique qui pourtant n'est pas le premier et ne sera sûrement pas le dernier.

En effet, cette crise n'est pas la première. Mais comme elle a un impact direct sur notre santé, pour une fois elle a été prise en compte par l'ensemble des dirigeants de la planète. Le dérèglement climatique a peut-être été le premier, mais tout le monde se sentait à l'abri, ou peu concerné…On retrouve ce type de crise au niveau des cyber attaques.

Si ces crises sont inévitables, l'objectif des dirigeants doit être d'en minimiser les impacts afin que la structure puisse continuer à fonctionner même en mode dégradé et puisse reprendre au bout d'un certain temps une activité normale. On parle alors de Résilience (valeur caractérisant la résistance au choc d'un métal).

Le concept de BCP *(Business Continuity Plan)* a été créé. À cela, on y a associé le DRP *(Disaster Recovery Plan)* et afin de comprendre les "fragilités" de la structure le BIA *(Business Impact Analysis)*.

BIO

Président de Mirat Di Neride, Expert en stratégie des entreprises et en cybercriminalité, Responsable Bureau CLUSIR - Nouvelle Aquitaine Ouest, Didier Spella, ancien officier supérieur de l'Armée de l'Air, est le co-fondateur du congrès PPP Charente-Maritime Cyber Sécurité. Il a vu évoluer les différents concepts qui régissent aujourd'hui le cybermonde. Ses connaissances en sécurité tant analogiques que numériques, son expérience d'analyse de risques et ses expertises auprès d'une compagnie américaine, lui ont permis de se positionner en tant qu'expert en définition de stratégie de sécurité. Confronté aux attaques cyber de plus en plus importantes et intrusives dans nos modes de vie, il étudie spécialement les risques encourus par la population en général et, plus particulièrement, les menaces qui pèsent sur les TPE et les PME.

Définitions

- Business Continuity Plan : Plan de Continuité des Activités
- Disaster Recovery Plan : Plan de Reprise d'Activité
- Business Impact Analysis : Analyse d'Impact Métiers

La norme 22301

Une norme nous aide pour bien prendre en compte ces problématiques de reprise d'activité. Cette norme est la norme ISO 22301. Celle-ci spécifie les exigences pour planifier, déployer, mettre en œuvre, exploiter, surveiller, revoir, maintenir et améliorer en permanence un système de gestion documenté. Elle permettra ainsi de réduire la probabilité d'occurrence d'un événement désastreux, de s'y préparer, d'intervenir et de récupérer à la suite de la survenance d'incidents perturbateurs quels qu'ils soient.

Les exigences spécifiées dans la norme ISO 22301 sont génériques et prévues pour s'appliquer à toutes les organisations (ou parties de celles-ci), indépendamment du type, de la taille et de la nature de l'organisation. La portée d'application de ces exigences dépend de l'environnement opérationnel de l'organisation et de sa complexité.

Nouveaux enjeux

Afin de comprendre ce qui se passe, nous pensons qu'il est nécessaire de modéliser ces crises afin de mieux en appréhender les enjeux.

Ces crises comportent plusieurs caractéristiques communes :

- Absence de frontières géographiques;
- Propagation rapide;
- Propagation aléatoire;
- Impact global;
- Multi-activités;
- Multi-secteurs;
- Etc…

Ces différentes caractéristiques nous amènent à identifier des limites au BCP et DRP. En effets les BIA ne couvrent pas de telles caractéristiques. Les prérequis sont généralement les suivants :

- Les risques couverts sont généralement assez co-localisés (glissement de terrain, incendie, inondation, etc…);
- Les prestataires ne sont pas inclus dans la crise (pas dans le même lieu, pas la même activité, pas les mêmes ressources, etc…);
- Les personnels ou une partie peuvent se déplacer;
- Les organisations étatiques sont en fonctionnement nominal;
- Etc…

Alors, nos analyses restent-elles bonnes ? Nos Plans sont-ils et seront-ils efficaces pour repartir ?

Les structures qui avaient déjà ces analyses et plan ont pu les utiliser pour passer en mode confinement. Celles qui n'en avaient pas, une grande majorité, ont "bricolé" sur le terrain des organisations et des solutions techniques afin de pouvoir poursuivre leur activité. Les mesures de sécurité passant au second plan, elles ont "délibérément" affaibli la protection de leur système d'information.

Dans les deux cas, leurs prestataires étant dans le même état, elles n'ont pas pu bénéficier de leur soutien, contrairement à ce que l'on a généralement dans des cas de crise localisée à une entreprise, au pire une région.

Nous constatons donc la limite des analyses et des plans que nous avons élaborés jusqu'à présent. Bien qu'elle ne soit ni la première ni la dernière, cette crise l'a encore prouvé, il faut repenser nos activités plus globalement.

Nos analyses doivent prendre en compte les notions suivantes :

- Entreprise étendue;
- Crise étendue;
- Degrés d'autonomie.

Nos plans doivent :

- Avoir une approche globale stratégiquement, tactiquement et opérationnellement;
- Prendre en compte les spécificités complètes de la structure;
- Faire développer une conscience collective auprès des collaborateurs.

Premières conclusions sur l'impact du «cyber-covid»

Cette crise sanitaire nous montre les limites des modèles de sécurité que nous avons mis en œuvre et qui, on le constate aujourd'hui, n'avait qu'un but: rassurer les citoyens et collaborateurs. Elles ont montré leurs limites.

Il faut repenser nos approches sécuritaires d'une manière plus globale. Comme toujours, restons dans une approche d'amélioration continue; chaque fois que nous pensons avoir couvert un risque, soyons capable de penser au nouveau risque que nous venons de développer.

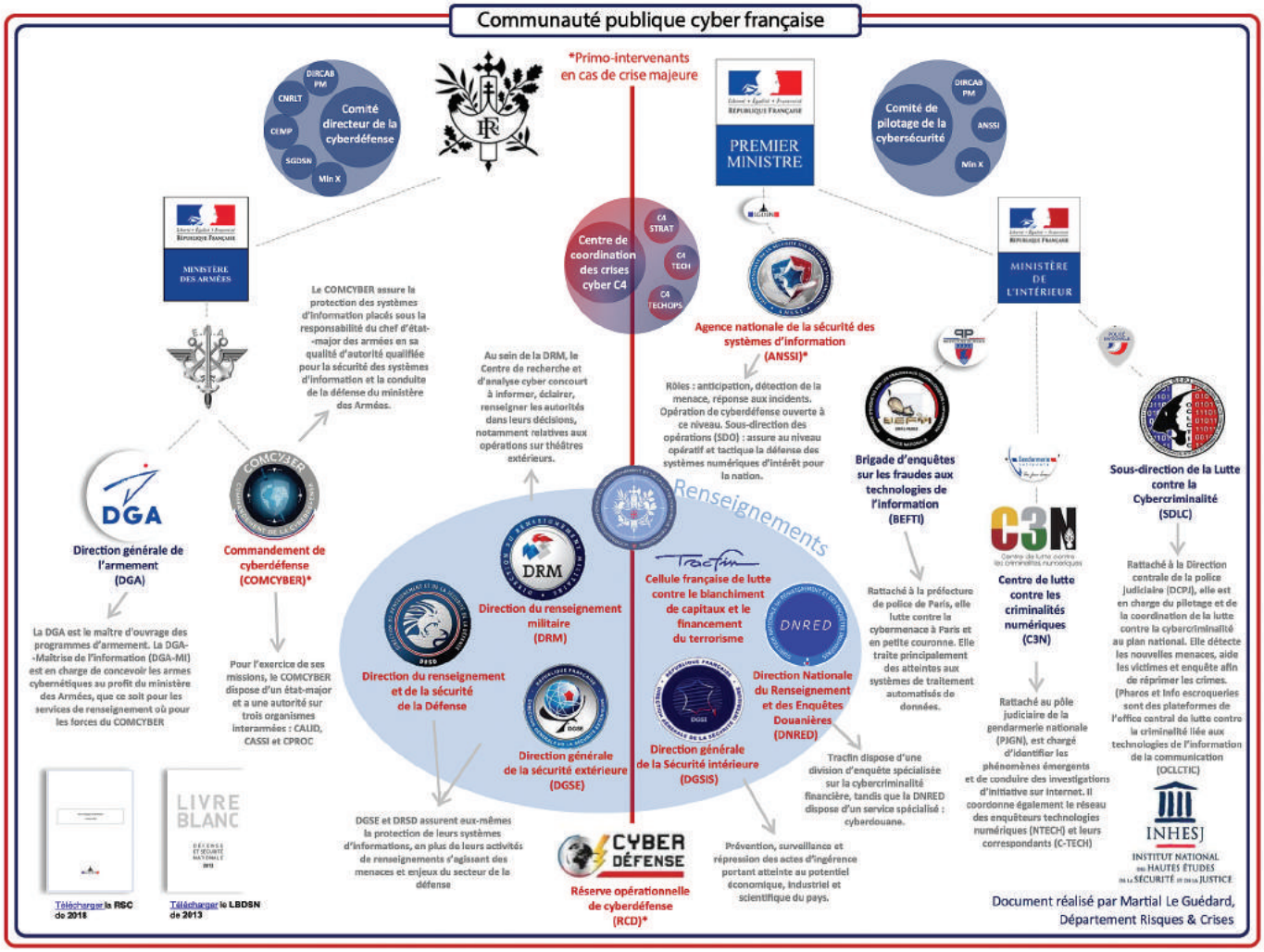
Penser déjà à préparer l'après-crise : pour une maturité de la numérisation

La numérisation touche tous les secteurs d'activité et toutes les professions qui y évoluent. Cela nous amène à nous poser plusieurs questions. Parmi celles-ci nous pourrions choisir celles-ci.

1. Quelles seront les évolutions des compétences professionnelles ?

2. Avec l'essor de l'IA, allons-nous vers la fin de la réflexion humaine au profit de celle de la machine ?

3. Comment peut évoluer système de formation ?



Vue générale de la communauté cyber en France à l'état actuel (https://inhesj.fr/index.php/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure)

Ces trois questions et bien d'autres d'ailleurs relatives à l'impact de la numérisation sur notre vie quotidienne, n'étaient en fait que la déclinaison d'une problématique plus générale concernant la "numérisation".

Pour moi la "numérisation" ne peut pas se résumer à un terme qui définit vaguement l'action ou les actions de transférer ou transformer une économie et des comportements analogiques en une économie et des comportements numériques.

Je pense qu'avant toute chose il est nécessaire de modéliser la numérisation et d'y adjoindre un critère de maturité.

Je propose donc que nous analysions l'ensemble des questions posées au moyen du modèle que nous allons réaliser.

Le modèle de maturité de la numérisation

Afin de mieux comprendre ce que nous sommes en train de vivre actuellement, je pense que nous pourrions décrire une démarche de numérisation en 4 étapes :

Etape 1 : la numérisation des supports

Il s'agit de la toute première étape qui consiste à transformer tout type de support analogique en support numérique, les documents, les musiques, bref tous les types possibles. L'humain a un usage plus pratique de ces supports.

Etape 2 : la numérisation des outils simples

Il s'agit de transformer, d'adapter les outils analogiques en outils numériques. La machine à écrire devient traitement de texte, la calculatrice, tableur, etc. Les machines-outils sont numérisées. L'humain devient un utilisateur.

Etape 3 : l'intégration des outils

Cette troisième évolution consiste à intégrer ces outils simples pour en faire des outils plus complexes en combinant différentes technologies : plate-forme numérique – communication – énergie. On y combine aussi les supports numérisés.

Nous voyons alors apparaître des outils complexes, utilisant plus ou moins bien les caractéristiques techniques de chacun de ces composants technologiques. Les concepteurs de ces outils proposent du confort par le biais de paramétrage mais nous ne pouvons parler de réel progrès. L'humain doit s'adapter à l'outil numérique.

Etape 4 : l'intégration numérique

Par "intégration numérique", j'amène le concept de concevoir des systèmes numériques totalement intégrés qui offrent notamment la personnalisation de tous ces outils et non pas uniquement un seul paramétrage. L'humain devient l'élément central de cette numérisation. Il peut choisir les outils qui lui sont nécessaires et utiles. Ces outils évolueront avec ses besoins. La personnalisation est effective.

Ce modèle étant développé, nous sommes en mesure de répondre aux questions posées

Quelles seront les évolutions des compétences professionnelles ?

Si nous reprenons notre modèle, nous voyons bien que l'évolution des compétences est bien réelle. Tout d'abord, il faut que nous soyons en mesure, quelque soit l'activité exercée, d'utiliser les fonctionnements de base des outils qui composent mon activité.

Cependant, ce niveau de compétence ne permettra que d'atteindre les 3 premiers niveaux de maturité.

Il faudra envisager de développer de nouvelles compétences qui permettront d'atteindre le niveau 4.

Ce niveau passe par une "re-définition numérique" de mon activité. Cela nécessite, outre de maîtriser mon activité, de connaître l'intégralité des possibilités qu'offre le numérique, afin d'être capable de concevoir une intégration numérique de mon activité.

Avec l'essor de l'IA, allons-nous vers la fin de la réflexion humaine au profit de celle de la machine ?

Le monde numérique nous propose aujourd'hui d'énormes possibilités de calcul qui nous permettent d'envisager de développer des outils aptes à "prendre des décisions". C'est du moins ce que nous propose le monde de l'intelligence artificielle.

Cependant, même si ces calculs semblent "infinis", ils n'arriveront jamais à créer un "point zéro", quelque chose, comme seul l'esprit humain sait le faire, ce qui nous a permis d'évoluer et ainsi d'envisager l'impossible.

De manière très simple, je dirai qu'aujourd'hui nous sommes capables de rêver, ce que ne saura jamais faire une machine numérique.

C'est donc plus vers une aide à la décision que nous nous dirigeons, dans le cas où nous serions au niveau 4 de la maturité de nos systèmes. La machine nous proposerait ainsi l'ensemble des solutions envisageables avec leur contraintes, peut être des modèles d'évolution et leur représentation "médiatique".

Il nous resterait alors à choisir la meilleure solution.

Et le système de formation dans cette évolution ?

A la vue de toute notre réflexion, il apparait évident que la formation doit évoluer, pour ne pas dire changer.

Nous ne pouvons nous contenter de ramener l'évolution de la formation à ne profiter que de la numérisation des supports (cartable moins lourd des écoliers) ou à l'utilisation d'outils numériques qui permettent de mettre un peu d'interaction entre élèves et enseignants.

Il faut, dans le cadre de "l'intégration numérique", envisager de nouvelles formes d'enseignement où l'apprenant est vraiment au centre du dispositif de prise de connaissances.

Le rôle de l'enseignant évolue vers plus un rôle de prescripteur d'apprentissage pour ses élèves. Nous replaçons "l'élève" ou "l'apprenant" au centre du dispositif de formation. Quel est son niveau, quels sont ses besoins, quelles sont ses compétences, voilà les premières réflexions que pourraient avoir l'enseignant face à son élève. Une personnalisation complète de l'enseignement serait mise en œuvre afin que chaque élève acquière les compétences nécessaires à son "évolution".

Conclusion

En conclusion, je pense que nous avons devant nous à prendre en compte, par le fait du numérique, une transformation sociétale majeure.

La numérisation de notre société ne peut pas se résumer à n'être que des utilisateurs d'outils numériques plus ou moins bien développés et intégrés dans nos modes de vie. Il ne faut pas confondre progrès et amélioration du confort. Aujourd'hui, nous sommes dans l'amélioration du confort. Il est nécessaire de s'adapter au monde numérique pour en profiter, d'où les ruptures numériques que nous observons.

Le vrai progrès passera par une intégration complète du numérique dans nos activités. C'est au numérique de prendre en compte nos activités et pas l'inverse. ■

La manipulation par la gestion de l'émotion

Les interactions virtuelles confèrent un anonymat et peuvent cacher la motivation subjacente d'une communication. Les utilisateurs créent des réalités au travers d'énoncés à la validation incertaine. La fugitivité et la circonstance de l'échange confine alors à une communication émotive. Les réactions se transforment en productions soigneusement formulées. Cette mise en scène des émotions a parfois pour objectif de manipuler un ou plusieurs interlocuteurs en les fascinant ou en les terrorisant. Cela peut donner un champ aux stratégies discursives des mouvements terroristes qui mettent en œuvre, lors de l'approche de sympathisants potentiels, des scénarios susceptibles de susciter une certaine émotion. Interagissant directement avec son interlocuteur, un manipulateur construit une relation sémantique basée sur un chevauchement d'émotions positives ou négatives articulées sur l'appartenance à une communauté, une relation à l'évènement ou une fascination quant à une imagerie culturelle. L'article de Laura Ascone explore ce champ cognitif peu approché de manière scientifique. Bien que centrée sur l'étude du phénomène djihadiste, son approche se révèle de la plus grande utilité pour comprendre notre réceptivité aux faux messages COVID#19 en cette période particulière de notre vie à tous.

Le recours aux émotions dans le cyberespace : entre stratégie discursive et manipulation

Auteur : Laura Ascone

Souvent accusé de déshumaniser les relations interpersonnelles, le cyberespace est en réalité le théâtre de nouvelles formes d'expression des émotions. Les réactions émotionnelles, qui sont par nature spontanées, se transforment ici en productions soigneusement formulées. Cette mise en scène des émotions a parfois pour objectif de manipuler un ou plusieurs internautes, que ce soit en les fascinant ou en les terrorisant.

Émotions et cyberespace

L'ouverture au cyberespace et les nombreuses innovations dans la communication ont inévitablement modifié la façon dont l'individu se rapporte au monde et à ceux qui l'entourent. Plus particulièrement, ce sont les notions de temps et d'espace qui ont changé dramatiquement. Dans le cyberespace, la communication médiée par les réseaux a son propre axe du temps. Malgré une apparente instantanéité, les interactions virtuelles ne sont pas aussi temporellement fluides que les interactions réelles. Si un utilisateur doit attendre que son interlocuteur rédige et envoie le message, l'autre doit attendre que le message soit lu avant de recevoir une réponse. Cependant, les deux utilisateurs ne semblent pas percevoir ce décalage temporel. De même, les interactions virtuelles se distinguent des interactions réelles sur le plan spatial. Bien que l'utilisateur se trouve face

BIO

Docteure en Sciences du Langage, Laura Ascone a réalisé sa thèse sur « La radicalisation à travers l'expression des émotions sur Internet » à l'Université Paris Seine. Actuellement, elle effectue un post-doctorat à l'Université de Lorraine dans le cadre d'un projet ANR sur les discours de haine contre les migrants. Ses recherches portent sur l'expression des émotions sur les réseaux sociaux, la propagande djihadiste et le contre-discours, et les messages haineux contre les migrants.

REMERCIEMENTS : L'article original de Laura Ascone a été publié dans la Revue de la Gendarmerie Nationale n. 266, décembre 2019, pp. 30-35. Nous exprimons notre plus profonde gratitude au Général Marc Watin-Augouard, directeur de la rédaction, et au Colonel Philippe Durand, rédacteur en chef de la Revue, pour nous avoir donné le privilège de reproduire ce texte et de le traduire en exclusivité en Roumain et en Anglais. Notre gratitude va également à l'auteur pour sa gentillesse et sa disponibilité.

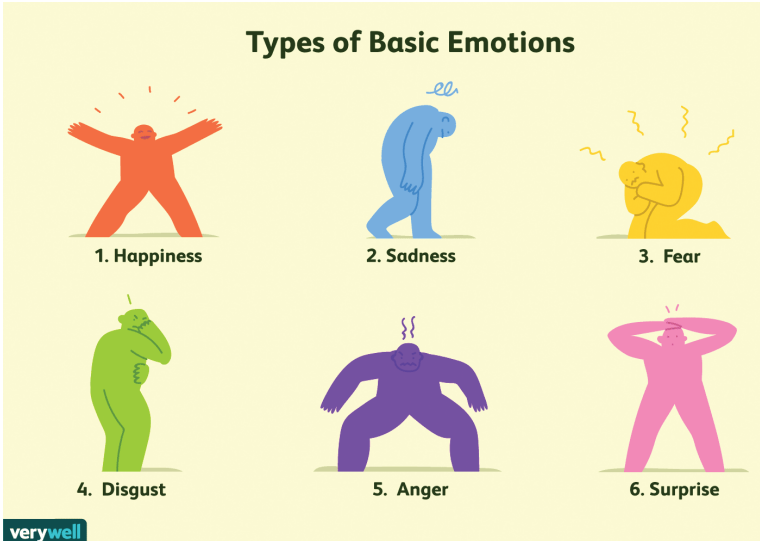
Les numéros de la Revue de la Gendarmerie Nationale sont disponibles en ligne à l'adresse :

https://www.gendarmerie.interieur.gouv.fr/Notre-communication2/Publications-Documentations/La-revue

à l'ordinateur dans le monde réel et que les messages soient visibles sur l'écran, les interlocuteurs ne partagent pas le même espace (1).

La spontanéité des émotions mise à l'épreuve

Le décalage spatio-temporel, qui caractérise les interactions virtuelles, donne la possibilité aux utilisateurs de cacher leur identité ainsi que la motivation subjacente à la communication. Autrement dit, les utilisateurs peuvent créer tout type de réalité et d'identité à travers des énoncés plus ou moins véridiques. En outre, ce décalage influence fortement la façon dont les interlocuteurs interagissent et expriment leurs émotions. Dans le cyberespace, lorsque l'utilisateur a une réaction émotionnelle et qu'il veut la communiquer à son interlocuteur, il tiendra automatiquement compte du contexte dans lequel il est en train de s'exprimer. Il aura donc tendance à moduler l'expression de ses émotions selon son interlocuteur, le type de conversation qu'il est en train de mener et le moyen de communication employé.



Les émotions de base © ONG Verywell Mind, www.verywellmind.com

En outre, la modulation des réactions émotionnelles influence indirectement les réactions de l'interlocuteur et, par conséquent, la conversation même. En d'autres termes, décider de la manière d'exprimer une émotion signifie décider comment agir sur l'interlocuteur, sur la communication et sur l'environnement. Plus particulièrement, l'utilisateur agit sur l'interlocuteur car l'interprétation et la réaction de ce dernier dépendent principalement de la façon dont l'émotion a été exprimée. Kramer et al. (2) ont montré comment une émotion exprimée sur Facebook influence les émotions des autres utilisateurs.

L'exposition à un nombre important de messages positifs amènera les utilisateurs à publier des messages positifs.

L'expression des émotions joue donc un rôle crucial dans toute interaction, qu'elle soit réelle ou virtuelle. Quand l'utilisateur interagit dans le cyberespace, les émotions qu'il ressent se dissipent instantanément, avant qu'il n'ait le temps de les exprimer par écrit. Cette caractéristique vient du fait que les émotions ne durent que quelques millisecondes. Par conséquent, l'utilisateur pourra, plus ou moins volontairement, décider comment verbaliser ses réactions émotionnelles. Ne s'agissant donc plus de l'expression d'une réaction spontanée, la communication virtuelle peut être considérée comme une communication émotive. Contrairement à la communication émotionnelle, où l'individu exprime son émotion à l'instant même où il la ressent, la communication émotive est caractérisée par la description de l'émotion une fois qu'elle s'est dissipée (3). En d'autres termes, la communication émotive se rapproche davantage des notions de performance, de rhétorique et de persuasion (4). Les émotions peuvent donc être mises en scène afin d'influencer les réactions et le comportement de l'interlocuteur.

Le discours de propagande terroriste diffusé dans le cyberespace constitue un exemple évident de cette exploitation, plus ou moins subtile, de l'expression des émotions.

Le lien entre le discours de propagande terroriste et les émotions peut être retrouvé dans le nom latin terror. Ce terme vient de la racine indoeuropéenne ter-, qui veut dire "trembler" et qui marque donc le lien entre le terrorisme et la peur (5).

Le discours djihadiste témoigne de la proximité entre l'action terroriste et la peur. Le 4 juillet 2014, jour où le califat a été réinstauré, Abu Bakr Al-Baghdadi a affirmé qu'il fallait *"revenir à l'Islam des premiers âges pour obtenir le pardon d'Allah et retrouver la fierté arabe en inspirant la peur aux infidèles et aux mauvais musulmans".*

Autrement dit, selon le leader de Daesh, il importe d'inspirer la peur plus que de tuer les infidèles et les mauvais musulmans. En ce qui concerne le discours propagandiste diffusé dans le cyberespace, la revue djihadiste Dar al-Islam constitue une source d'analyse cruciale. Elle nous permet de mieux comprendre les stratégies discursives employées par Daesh.

Diffusée à partir du 23 décembre 2014, Dar al-Islam compte dix numéros et s'adresse à un public qui a déjà adhéré à l'idéologie djihadiste. Ne s'agissant pas d'une interaction, la revue ne peut pas moduler son discours selon l'interlocuteur. L'éditeur doit donc tenir compte des différents profils qui peuvent avoir accès à ce contenu. Bien que l'expression des émotions joue un rôle central dans le discours propagandiste, il est possible de constater que les émotions sont rarement exprimées directement. Au contraire, l'énonciateur recourra à des scénarios susceptibles de susciter une certaine émotion. Discours et images contribuent ainsi à la mise en scène des émotions afin de renforcer l'adhésion à l'idéologie djihadiste. Si l'exaltation du groupe djihadiste vise à nourrir l'amour pour cette communauté, la condamnation de l'ennemi a pour objectif d'alimenter la haine contre celui-ci.

Émotions et embrigadement

Le discours djihadiste dans le cyberespace ne circule pas seulement à travers des revues officielles. Les réseaux sociaux constituent également des vecteurs de la propagande djihadiste. Contrairement à Dar al-Islam, les interactions sur les réseaux sociaux s'adressent à un public qui est en voie de radicalisation. Par conséquent, l'expression des émotions vise à influencer l'interlocuteur afin qu'il adhère à l'idéologie promue. Le clip *Ils te disent*, produit par le gouvernement pour contrer la radicalisation djihadiste dans le cyberespace, montre un exemple de cette manipulation. Après avoir regardé le profil Facebook de plusieurs djihadistes, le protagoniste de la vidéo reçoit un message :

1. Salut
Cool les trucs que tu like,
ça t'intéresse ce ki se passe
au Cham en ce moment ?

si ta des questions hésite pas,
la vérité elle est la bas,
c'est maintenant qu'il faut partir !

si tu me donnes ton num j'ai des amis
la bas ki se battent jte met en contact.

Le discours suscite des réactions émotionnelles positives et négatives qui peuvent s'alimenter autour d'une appartenance communautaire et du rejet d'un adversaire. © Fotofabrika/Revue de la Gendarmerie Nationale

Bien qu'il s'agisse d'une reproduction, ce message montre le caractère anxiogène des messages envoyés par des recruteurs. Interagissant directement avec son interlocuteur, l'embrigadeur peut facilement moduler son discours. Il peut également créer une identité ad hoc grâce à la nature du cyberespace: la perception que l'on a d'un individu se construit principalement. sur les informations que cet individu nous transmet (6). Le choix de nombreux djihadistes d'utiliser une photo de lion comme photo de profil sur Facebook vise à les montrer comme des personnes fortes et courageuses. L'internaute, qui aura tendance à oublier et à se détacher du monde réel qui l'entoure, finira par percevoir comme vrai et réel tout ce qui se passe dans le cyberespace. Ben-Ze'ev (7) définit ce phénomène detattachment ("détattachement"). Malgré la distance spatio-temporelle, l'utilisateur ressent un sentiment d'attraction et établit une sorte de relation avec son interlocuteur. L'objectif de cette manipulation d'émotions est de couper l'individu de son entourage réel pour qu'il ne ressente plus d'émotions envers ses proches. De même, à travers l'exposition à des contenus violents, l'embrigadeur djihadiste vise à habituer sa cible à la violence et qu'elle n'ait plus peur de mourir. Autrement dit, l'embrigadeur se sert des émotions pour que la cible ne les ressente plus.

Combinaison paradoxale des émotions dans le discours djihadiste

Bien que le lien entre terrorisme et peur soit évident, le discours terroriste djihadiste ne s'articule pas seulement autour de la peur et des autres émotions négatives. Visant à fasciner aussi ses sympathisants, le discours djihadiste recourt également aux émotions positives. Réactions émotionnelles positives et négatives s'articulent donc au sein d'un même discours. Dans certains cas, deux sentiments (8) opposés s'alimentent l'un à l'autre. La haine contre l'ennemi mécréant alimente l'amour envers la communauté djihadiste. Et inversement, l'amour pour la communauté alimente la haine contre l'ennemi. Ce chevauchement d'émotions positives et négatives peut émerger aussi en relation à un événement. Une attaque terroriste menée sur le sol occidental suscitera chez la communauté djihadiste des réactions positives telles que la joie, la fierté et de l'adrénaline. En outre, la même attaque pourra susciter des réactions positives aussi au sein de la communauté visée. Les attentats perpétrés sur le sol français, par exemple, ont réveillé des sentiments de solidarité et d'amour.

Une approche d'analyse des émotions dans le cyberespace

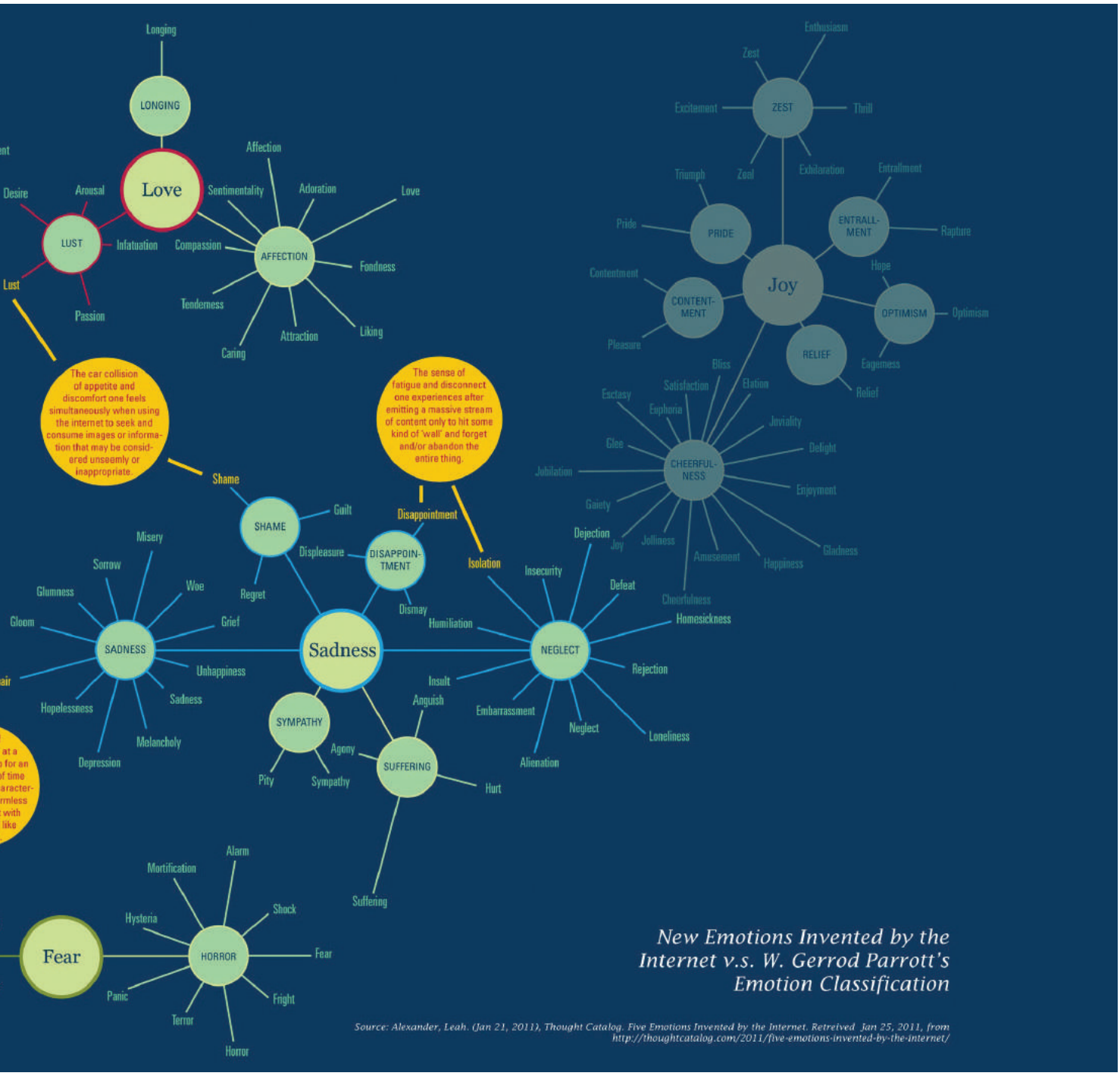
Ce panorama synthétique de l'expression des émotions dans le cyberespace a révélé des éléments qui nécessitent d'être pris en compte lorsque l'on s'apprête à examiner le discours djihadiste diffusé sur Internet. Tout d'abord, il est important d'analyser un texte dans son contexte. Il s'agit donc de considérer le moyen de communication employé et l'impact que ce dernier peut avoir sur le discours, les événements auxquels les interlocuteurs peuvent faire référence, et le point de vue des différents utilisateurs qui participent à la conversation. Plus particulièrement, ce dernier point permet de déterminer si un message exprimant une émotion positive est réellement un contenu positif ou si, au contraire, l'objet de telle émotion constitue un potentiel danger pour la communauté. En outre, il est nécessaire de considérer que notre discours est imprégné de nos impressions même lorsque

l'on n'exprime pas directement nos émotions (9). Par conséquent, afin d'analyser la radicalisation djihadiste à travers l'expression des émotions dans le cyberespace, nous ne pouvons pas limiter l'étude à l'analyse des émotions uniquement négatives. De même, comme nous l'avons montré, il est important d'étudier non seulement l'expression des émotions, mais aussi comment l'énonciateur suscite, à travers son discours, des réactions émotionnelles chez son interlocuteur. ■

Notes :

(1) Kramsch, C. G. (2009). The Multilingual Subject : what foreign language learners say about their experience and why it matters. Oxford University Press.

(2) Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive- scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 8788-8790.
(3) Plantin, C. (2011). Les bonnes raisons des émotions. Peter Lang Publishing Group.
(4) Arndt, H., & Janney, R. W. (1991). Verbal, prosodic, and kinesic emotive contrasts in speech. Journal of pragmatics, 15(6), 521-549.
(5) Di Cesare, D. (2017). Terrore e modernità. Torino : Giulio Einaudi Editore.
(6) Mantovani, G. (2002). Internet haze: why new artifacts can enhance situation ambiguity. Culture and Psychology 8, 307–326.
(7) Ben-Ze'ev, A. (2005). 'Detattachment': the unique nature of online romantic relationships. In Y. Amichai- Hamburger (ed.), The social net: Human behavior in cyberspace, 115–138. New York: Oxford University Press
(8) Contrairement aux émotions, qui ne durent que quelques millisecondes, les sentiments ont une durée plus importante. Ekman (1992) identifie six émotions primaires : joie, peur, colère, surprise, tristesse et dégoût
(9) Shaver, P., Schwartz, J., Kirson, D., & O'connor, C. (1987). Emotion knowledge: further exploration of a prototype approach. Journal of personality and social psychology, 52(6), 1061



Quand l'isolation associée à la désinformation mènent à l'hôpital

Auteur : Octavian Oancea

Cher lecteur,

Aujourd'hui, je préfère vous raconter une histoire vraie. Retirant ma veste d'expert en cyber-sécurité, je vais vous proposer une expérience relevant de mon domaine privé.

L'autre jour, quelque chose de vraiment inhabituel et triste s'est produit. Alors que je vivais et travaillais dans l'auto-confinement imposé par la loi, j'ai reçu un appel d'un ami concernant une personne que nous connaissons tous les deux. Il s'est avéré qu'il se trouvait en grave dépression.

BIO

Octavian est actuellement CEE Channel Business Manager de Trend Micro. Il est titulaire d'une licence et d'une maîtrise de l'Université polytechnique de Bucarest. Il est animé d'une véritable passion pour l'excellence, tant dans sa carrière que dans sa vie privée. En tant que professionnel, il s'avère très compétent pour évaluer les marchés et identifier les opportunités inexploitées en forgeant de nouvelles relations d'affaires. Il a été directeur général et fondateur de McAfee Romania, Avnet Technology Solutions Romania et ZyXEL Communication Romania. Sur le plan personnel, il s'intéresse beaucoup à la musique, à la photographie, aux sports et aux technologies de l'information, et plus particulièrement à la sécurité de l'information.

Nous savions que pendant les dernières années, il était friand de diverses théories de la conspiration et, bien qu'en discutant avec lui, nous ayons essayé de les combattre une à une avec des arguments scientifiques et factuels, nos propos n'ont, en grande mesure, servi à rien.

Ce qui nous a échappé, c'est l'effet que ces années d'exposition à la désinformation peuvent avoir sur l'esprit de quelqu'un. Et nous sommes alors retrouvés abasourdis et sans voix, en observant la réalité, lorsque nous sommes allés rendre visite à notre ami à l'hôpital. Oui, on en est arrivés à ce point là !

Il s'avère que notre pauvre copain a paniqué si fort, en regardant toutes sortes de contenus traitant du Covid-19, truffés d'une pléthore d'inepties autour de la technologie 5G et d'autres pseudo-faits, qu'il s'est retrouvé à bout, au point de ne pas pouvoir dormir pendant plusieurs nuits. L'insomnie, la nervosité ont mis ses limites physiques à épreuve si rude qu'il a craqué. Grâce à un sursaut de bon sens, il a réalisé qu'il avait besoin d'aide et a demandé secours.

En discutant avec lui dans la cour de l'hôpital, il s'est rendu compte à quel point ses décisions de faire confiance à ces théories étaient mauvaises et combien cela lui a fait du tort, mais il a admis qu'il lui était impossible de s'en débarrasser. D'une certaine manière, ces *fake news* alimentaient sa quête de sensationnalisme, et qu'il avait le sentiment d'avoir le privilège d'avoir accès à de telles informations.

Cette expérience nous amène directement au sujet d'aujourd'hui: la désinformation et ses effets sur notre santé. Nous avons tendance à négliger

ce sujet, principalement parce que nous sommes éduqués pour filtrer notre flux d'informations. Dans le domaine de la cyber-sécurité, nous avons de la chance, car notre métier nous permet de mieux repérer les *fake news* et la désinformation, car elles sont étroitement liées à notre routine quotidienne : campagnes de *phishing*, ingénierie sociale et autres.

Et je dois admettre qu'aux nombreux amis qui m'ont demandé comment mieux se protéger dans l'espace numérique, j'ai rapidement trouvé des solutions, enfin... concernant les appareils eux-mêmes - les sécuriser et sécuriser nos comportements humains dans le monde digital. Je n'ai donné que peu de conseils sur la façon de consommer les informations sur ces appareils, et pourtant il semble que, de nos jours, ce soit peut-être le plus grand des problèmes.

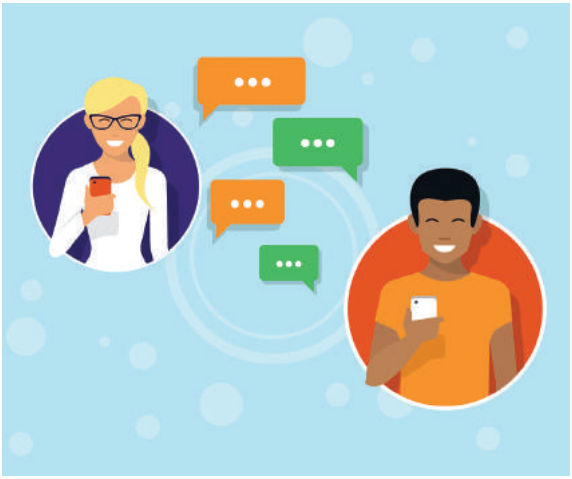
Pensez-y : disons qu'avec un peu de malchance, vous pourriez obtenir une variante de rançongiciel sur l'un de vos appareils. Si vous avez mis en place une bonne sécurité, il y a de fortes chances pour que vous vous en tiriez simplement avec une petite frayeur. Avec un peu plus de malchance, vous pourriez perdre les données de l'appareil attaqué. Vous auriez donc appris "à la dure" à changer vos habitudes cybernétiques, mais à part un peu de frustration, vous accepteriez que ce qui est fait est fait et vous iriez de l'avant. J'ai même rencontré des gens qui ont perdu des sommes d'argent (considérables) à la suite de certaines campagnes ciblées. Ils étaient furieux, mais ils ont réussi à laisser cela derrière eux, à en tirer les leçon et à continuer leur chemin.

Maintenant, revenons sur l'effet de la frustration quotidienne suscitée par l'information que la plupart des citoyens reçoivent, via les réseaux sociaux ou la télévision et replaçons tout cela dans un contexte où la plupart d'entre nous sommes auto-confinés.

Nous ne savons pas grand-chose sur ce virus et nous avons donc peur: pour nos familles, notre santé, nos emplois - autant d'inconnues. De plus, nous avons plus de temps que jamais à consacrer au monde digital. Pensez au cocktail toxique qui se trouve dans le cerveau des "gens de tous les jours". Il n'est pas étonnant que tant de citoyens, sortant de quarantaine*, se soient adressés directement à leurs avocats. (*NdR : auto-isolement imposé avec interdiction de sortir du domicile / de l'hôtel réquisitionné par l'Etat pendant 14 jours, une mesure qui s'applique en Roumanie à toutes les personnes provenant de l'étranger).

Où veux-tu en venir ? – me demanderez-vous.

Compte tenu de ce qui précède, nous devons reconnaître notre rôle dans la société et éduquer les citoyens sur la manière de consommer l'information. L'humanité a déjà été confrontée à de graves crises auparavant, mais nous assistons à un niveau sans précédent de manipulation des médias. La plupart des gens ne savent pas comment gérer ce déluge de "news" et, en particulier en ce moment précis de notre histoire, il est évident que les médias toxiques, légaux (sensationnalisme) comme illégaux (fake news), ont de graves conséquences sur le bien-être et la santé mentale de la population.



Joignez quelques-uns de vos amis les plus proches dès aujourd'hui. Voyez comment ils s'en sortent et, si vous le pouvez, amenez la discussion exactement au point où vous pourrez les aider à filtrer les nouvelles quotidiennes. Commençons ainsi et avec ce simple symbole mondialement connu : ☺.

Avec tous mes vœux de bonne santé ! ■

Sécurité des périmètres, VPN et Zero Trust durant la pandémie de coronavirus

Auteur : Cătălin Pătrașcu

Plusieurs grands titres des médias (1, 2, 3) ont souligné qu'avec la pandémie de coronavirus (SAR-Cov-2), les cyberattaques ont augmenté de façon spectaculaire, les attaquants se concentrant désormais sur l'exploitation de cette situation de crise, un fait qui est également confirmé par les autorités compétentes nationales et internationales (4, 5).

Ce phénomène est lié, d'une part, au fait que la pandémie a attiré pratiquement toute l'attention mondiale, et cet intérêt accru a permis aux malfaiteurs de renforcer considérablement les attaques basées sur des techniques liées à l'ingénierie sociale (*phishing, spear-phishing, landing hole, spam, sram*, etc.).

BIO

Cătălin est un expert chevronné en matière de cyber-sécurité, avec plus de vingt ans d'expérience dans le domaine de la sécurité de l'information. Il a commencé son parcours dans le domaine de la cyber-sécurité au sein du Ministère de la défense de la Roumanie (2010-2012), l'a poursuivi en tant que coordinateur de l'équipe de traitement des incidents au sein de la Cellule nationale de réponse aux incidents de sécurité informatique - CERT-RO (2012-2018). Il est actuellement responsable de la prestation de services de sécurité pour une société qui offre des services de cyber-sécurité dans le monde entier. Il a géré avec succès des projets liés à la cyber-sécurité, planifié et animé des cyber-exercices, géré différents incidents de sécurité à l'échelle nationale et mené diverses études sur des sujets liés à la cyber-sécurité et à la cybercriminalité.

D'autre part, la plupart des gens travaillant maintenant à domicile accèdent à distance aux ressources informatiques de leur employeur (courriels, documents, bases de données, etc.), générant nombre de vulnérabilités pour les entreprises qui se basent encore sur le concept de sécurité périmétrique, celles-ci étant encore – malheureusement – majoritaires à ce jour.

Nous ne parlons pas, cependant, de nouveaux types d'attaques, ni de nouvelles techniques utilisées par les attaquants. La différence est que la pandémie fournit la meilleure des "plates-formes" possibles et le contexte idéal pour les criminels. Par exemple, les attaques de type *watering hole*, basées sur des logiciels malveillants infectant les sites Web utilisés par le groupe cible, ont pour conséquence d'infecter tous ceux qui accèdent à ces sites Web. Aussi, à ce stade, les sites Web qui fournissent des informations en temps réel – comme des cartes interactives – sur la pandémie sont les

cibles idéaux pour des attaques ce de type, une occasion que attaquants ont immédiatement saisi.

Mais revenons au concept de sécurité des périmètres. Traditionnellement, les entreprises sécurisent leur infrastructure en créant des zones virtuelles de réseau, le plus souvent Internet (zone publique, non sécurisée), DMZ (zone généralement dédiée aux serveurs et aux applications) et LAN (réseau interne).

Seulement, en raison de la mobilité accrue des employés et de la nécessité d'accéder aux ressources de l'entreprise où que se trouvent ces derniers, les limites de cette stratégie sont déjà mises en évidence.

La technologie **VPN** est venue comme une bouée de sauvetage provisoire, ce qui signifie en fait que les terminaux situés en dehors du réseau peuvent se connecter via un réseau virtuel au réseau interne de l'entreprise, ayant ainsi accès aux ressources, exactement comme s'ils étaient réellement connectés à réseau vital.

Les logiciels (légaux!) pour hacker des VPN mal configurés © https://white-hattricks.blogspot.com/2019/09/Hack-VPN-Accounts-Download-All-VPN-Hunter-free.html

Cependant, la pandémie a fait littéralement exploser le nombre de connexions VPN et de nombreuses entreprises n'étaient pas prêtes pour cela, ce qui signifie que l'équipement qui a permet ce type de connexion n'a pas été conçu pour que tous les employés puissent se connecter depuis leur domicile.

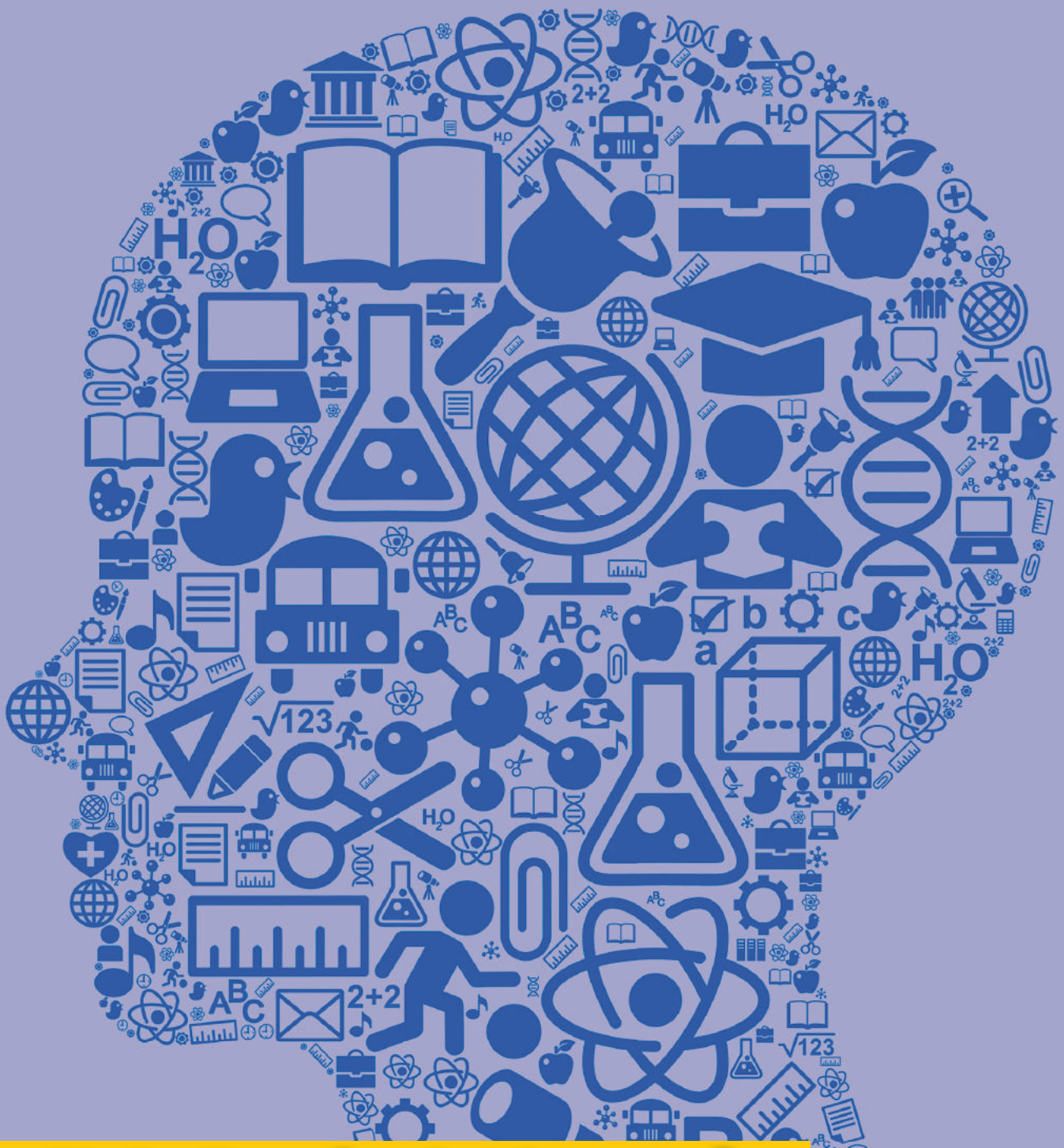
Les entreprises ont dû mettre à niveau le matériel en très peu de temps, ce qui, en plus des coûts financiers, signifie habituellement des interruptions temporaires de service.

Idéalement, il faudrait que l'approche périmétrique et les technologies y relatives, désormais doublées par la technologie VPN, soient remplacées en bloc par un nouveau cadre appelé *Zero Trust* **"confiance zéro"**, qui repose sur un utilisateur, un terminal, une application, ou un processus ayant le même niveau de confiance, où qu'ils soient, l'accès à chacun de ces acteurs humains ou techniques étant accordé de la façon la plus restrictive possible en fonction des besoins de chacun.

De plus, ce cadre est utile non seulement dans le contexte actuel de la pandémie de coronavirus, mais surtout, il s'est avéré être la plus idéale des solutions de base, en symbiose avec l'évolution observée durant ces dernières années, à savoir une augmentation massive de la mobilité et du travail à distance. ■

Notes :

(1) https://euobserver.com/coronavirus/147869
(2) https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
(3) https://securitytoday.com/articles/2020/03/26/world-health-organization-facing-cyber-attacks-during-coronavirus-response.aspx
(4) https://cert.ro/citeste/alerta-campanii-frauduloase-coronavirus
(5) https://www.us-cert.gov/ncas/alerts/aa20-099a



IV. Bréviaire de cyber-défense à user durant (et après) la pandémie

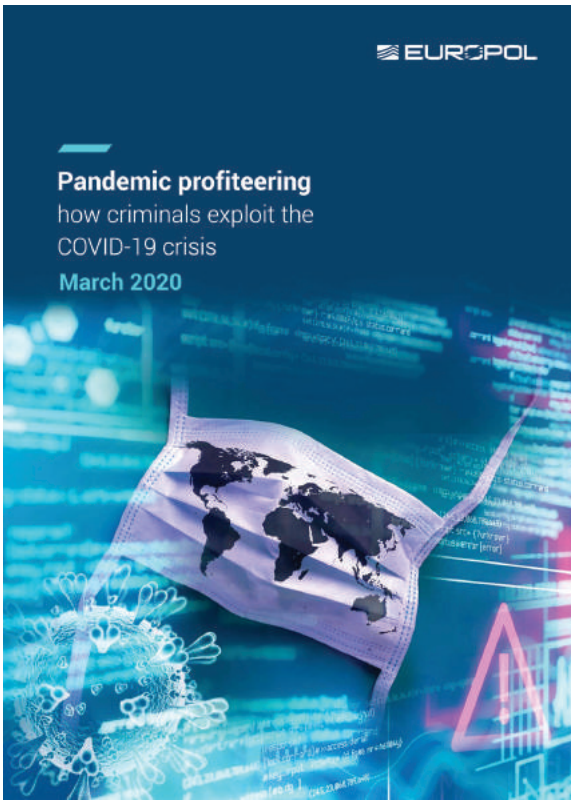
COVID#19 : petit guide international de défense et de protection

Auteur : Laurent Chrzanovski

Une Europe aux organes timides et peu coordonnés, tant dans l'UE que dans les différents pays membres

Malgré l'urgence de faire face au tsunami de cyber-attaques, l'Europe fournit, bien sûr, des informations, mais très peu d'agences centralisées ont créé une section spéciale COVID sur leur page d'accueil. Le CERT-EU (www.cert-europa.eu) par exemple, continue comme si de rien n'était, à offrir tous les détails techniques des attaques détectées et examinées, tout comme l'ENISA (www.enisa.europa.eu). L'agence la plus proactive reste ainsi la cellule EC3 d'EUROPOL, qui a non seulement élaboré un graphique de base éducatif, accessible à tous, a créé une section spéciale sur sa page d'accueil (www.europol.europa.eu), mais a également publié un rapport de grande qualité intitulé *"Pandemic Profiteering : How Criminals Exploit The Covid-19 Crisis"* (16), qui contient de nombreux conseils et exemples utiles.

Si l'on observe en revanche les différents pays européens, on constate un contraste colossal entre l'Espagne et les autres États. À Madrid, il a été décidé de centraliser toutes les informations sur le site web de l'INCIBE (Instituto Nacionál de Ciberseguridad) (www.incibe.es), en créant une énorme bannière sur la page d'accueil consacrée aux attaques liées au COVID#19 (17). Outre les rapports et un flux d'informations actualisé en temps réel, les différents messages vitaux sont également largement diffusés par tous les services de l'Etat - de la police à l'armée en passant par la protection civile et les autorités fiscales - sur leur site web, sous la forme de 30 "pilules" dont le graphisme et la clarté des messages forcent l'admiration.



Quelques-unes des "pilules" espagnoles © INCIBE

BIO

Titulaire d'un doctorat en archéologie romaine obtenu à l'Université de Lausanne, d'un diplôme de recherche postdoctorale en histoire et sociologie de l'Académie roumaine des sciences et d'une habilitation UE à diriger des doctorats en histoire et en sciences connexes, Laurent est professeur (chaire) à l'École doctorale de l'Université de Sibiu et à l'Université de Varsovie (invité permanent). Il donne régulièrement des cours postdoctoraux dans plusieurs grandes universités de l'UE. Il est l'auteur/éditeur de 32 livres, de plus de 150 articles scientifiques et d'autant d'articles grand public. Dans le cadre de la cybersécurité, Laurent Chrzanovski est membre du groupe d'experts de l'UIT. Il a fondé et gère les plateformes annuelles «cybersecurity dialogues», organisées en partenariat avec les plus hautes organisations publiques et privées de chaque écosystème (Roumanie, Italie, Suisse). Dans le même esprit et avec les mêmes partenariats, il est co-fondateur et directeur de la première revue trimestrielle gratuite de prévention de cybersécurité, publiée en roumain dès 2015 et également dans ses versions italienne et anglaise, depuis 2016 et 2017. Ses principaux domaines d'étude sont axés sur la relation entre les comportements humains et le monde numérique, ainsi que sur l'assurance de trouver le juste équilibre entre sécurité et vie privée pour les citoyens en ligne.

A l'opposé, presque tous les autres pays du continent proposent aux citoyens un véritable labyrinthe de sites qui ne renvoient pas les uns aux autres, réduisant ainsi la visibilité de leurs conseils et documents, pourtant très utiles et rédigés avec beaucoup de soin. Si l'on prend l'exemple de l'Italie, la **police des communications** fait quotidiennement le point sur les faits les plus graves (www.commissariatodips.it). Ne sont pas en reste, avec des pages consacrées à COVID-Cybercriminalité, les sites du **Cert de l'Administration publique** (18), de l'**Agence pour l'Italie numérique** (19) du **CertFIN** (20) et de l'**Association italienne des ingénieurs de clinique** (21). Les autres organisations, à l'image du CERT-UE, préfèrent, jusqu'à aujourd'hui, traiter les attaques telles qu'elles se présentent, qu'elles soient liées ou non au COVID# 19 et aux spécificités des modes de vie et de travail désormais imposés à tous les Européens ou presque.

COVID#19 : Un cyber-front sans limites. Des attaques jamais vues auparavant, en diversité et en quantité.

À l'usage de nos lecteurs, nous proposons ici une liste des principaux moyens utilisés par les cybercriminels pour attaquer presque tous les types de personnes et d'entités, *"urbi et orbi"*. Selon Bitdefender, les attaques mondiales de mars 2020 ont connu une augmentation de 500 % par rapport à celles de février... qui étaient déjà très élevées (certains spécialistes avancent le chiffre de de 1500% de plus par rapport à mars 2019).

1. Désinformation massive en cas de panique, avec en cadeau des virus

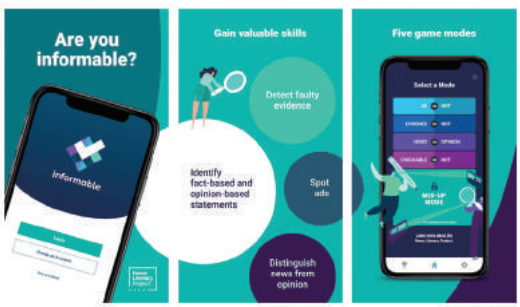
De nombreux pays ont pris des mesures extraordinaires pour censurer les fake news. Ils se heurtent presque toujours au problème que connaissent tous les spécialistes du domaine : les réseaux sociaux et l'extraterritorialité. Le manque de discernement entre un communiqué officiel et une fausse nouvelle, de la part de nombreux citoyens, continue de mettre en évidence *ad eternam* le problème - toujours irrésolu - d'une gestion efficace de la sensibilisation préventive offerte à tous pour reconnaître les *fake news*.

Le faux message du Ministre de l'éducation daté du 19 mars © AFP

Presque partout, les exemples de faux documents officiels, comme les fausses lettres ministérielles à l'image, en Italie, de celle du ministère de l'éducation devenue virale sur les réseaux sociaux - et dénoncée par la ministre Lucia Azzolina (22) - , ne manquent pas.

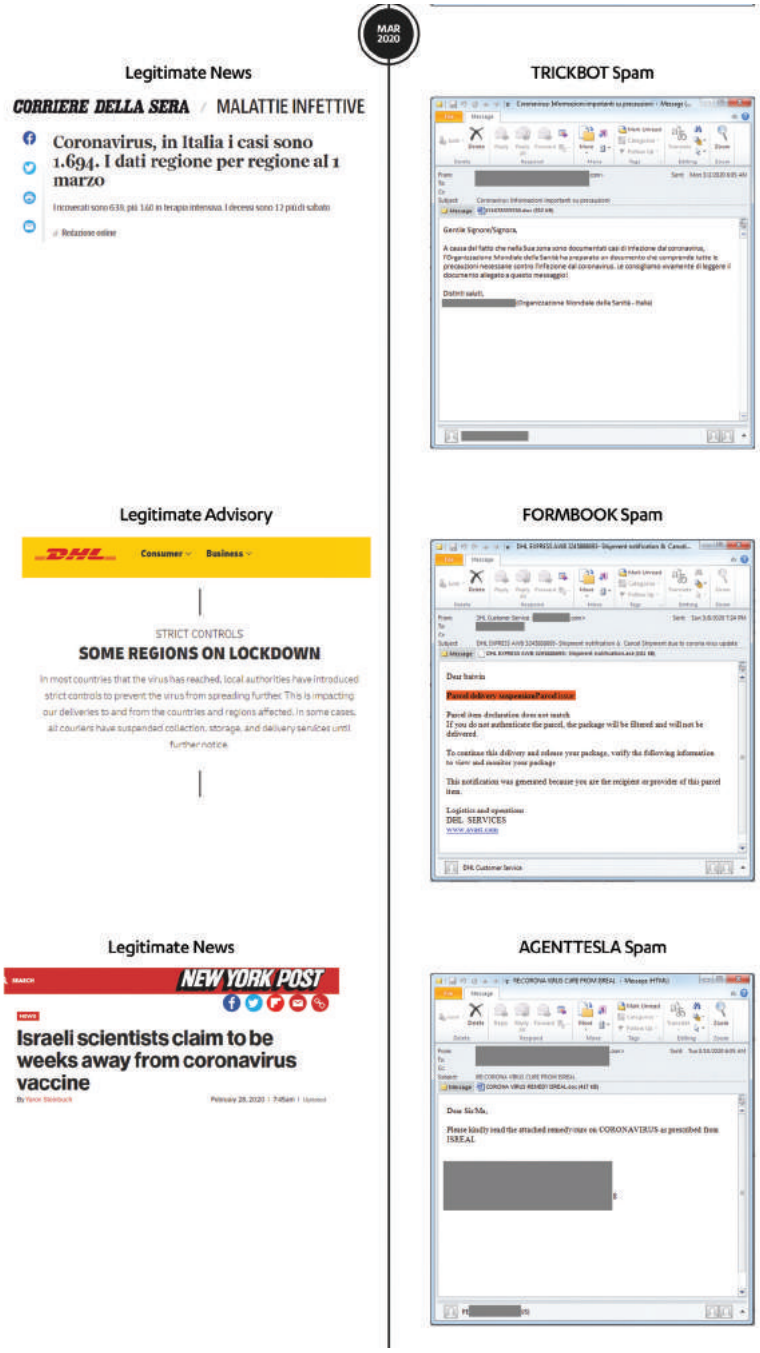
▸▸Apprenez à vous informer correctement !

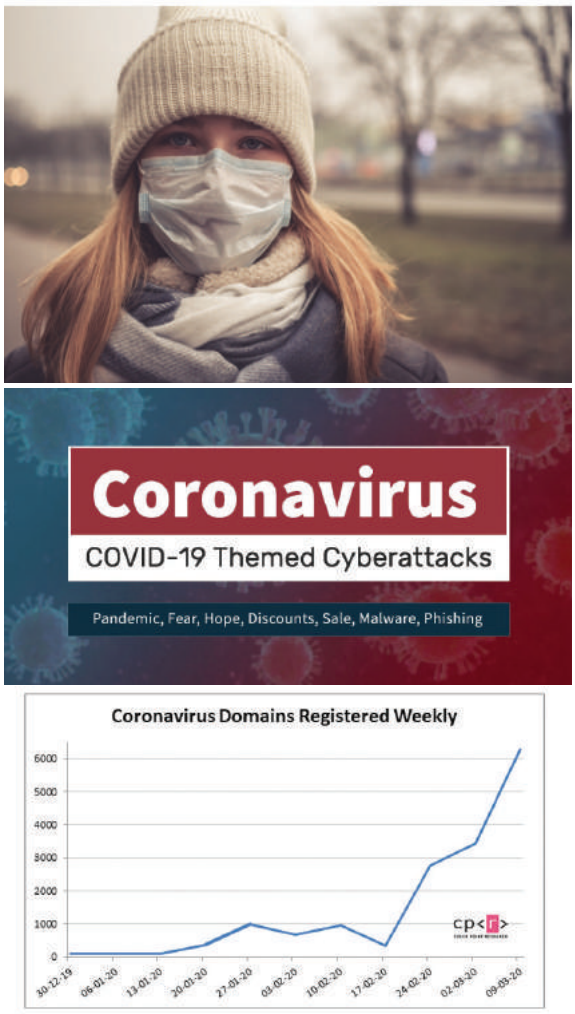
Avec l'urgence de COVID, le projet proactif *News Litteracy* a lancé, pour le public anglophone, une des meilleures initiatives possibles : une application pédagogique directe, intitulée presque ironiquement *Are you informable* ? (litt. Êtes vous encore capable d'être informé ?") (https://newslit.org/coronavirus/.



L'application pour calmer la panique et revenir à des sources fiables © News Litteracy Project

Un élément en plein essor est précisément l'utilisation de ces mêmes faxe news pour cacher de puissants logiciels malveillants, comme l'a révélé un récent rapport d'Adam Pilkey publié par la société F-Secure (voir biblio 13), magistralement illustré et partiellement reproduit ici. Comme on peut le voir dans l'article, il donne force à ses propos par des exemples et les *logiciels malveillants* connexes provenant de pas moins de 12 pays, de l'Asie à l'Europe et aux États-Unis, à considérés comme autant d'exemples. Une autre préoccupation majeure est le nombre de domaines qui font référence au nom officiel ou populaire du virus, tous potentiellement entre les mains de criminels, comme le souligne le rapport de Lakshmanan *(biblio n. 14)*.





A droite : une partie de l'illustration de Pilkey. A gauche : titres de journaux spécialisés © Cyberhub et Montalbano, Threatpost (biblio n. 12) ; nombre de sites liés au nom "Coronavirus" achetés par des criminels ces dernières semaines © Checkpoint, voir Lakshmanan (biblio n. 14).

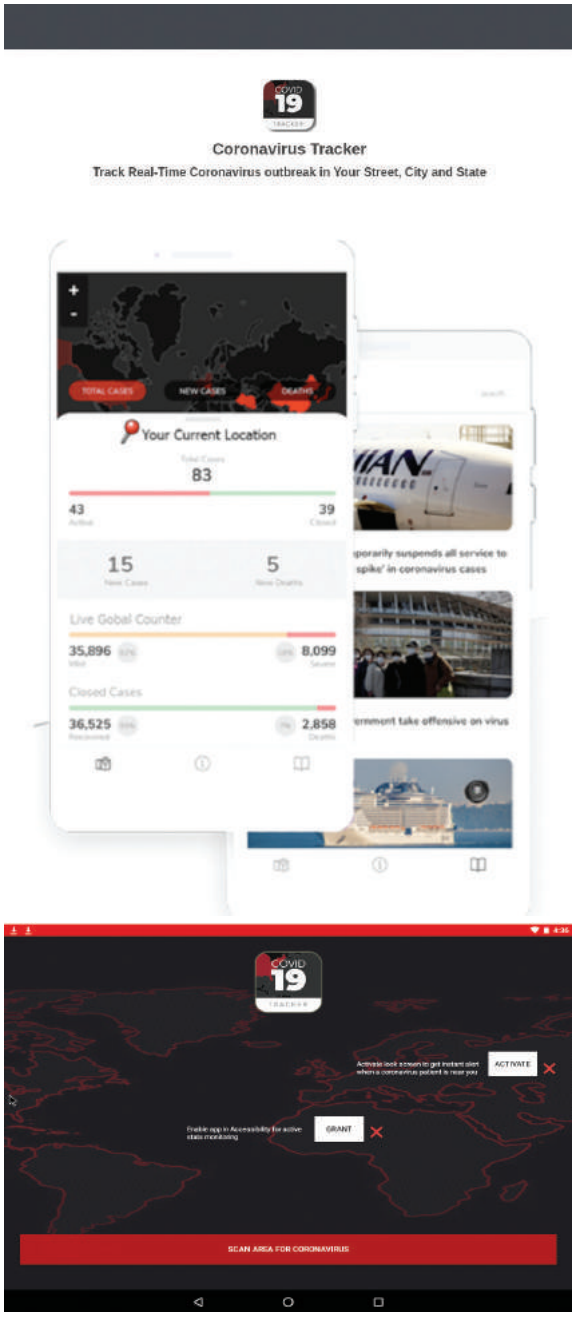
2. Recherche désespérément des informations pour les outils mobiles : les applications criminelles consacrées au Covid#19

Au nombre des fausses nouvelles envoyées par courriel, escroqueries ou liens malveillants postés sur les réseaux sociaux, s'ajoutent des dizaines de fausses applications créées chaque semaine pour "informer" l'utilisateur sur la situation mondiale, nationale et fournir des "informations utiles".

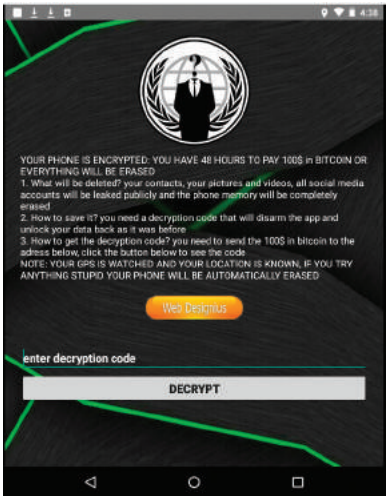
Presque tous destinés aux smartphones équipés de système Android, ils donnent du fil à retordre à tous les spécialistes de sécurité. Bien que rejetées par les différents "stores" natifs des fabricants de smartphones,

elles sont téléchargées directement sur Internet par les utilisateurs. Si la plupart de ces app se contentent de copier des parties plus ou moins importantes du contenu du smartphone de la victime, certaines d'entre elles prennent carrément le contrôle aussi bien du microphone que des les caméras vidéo/photo du smartphone atteint.

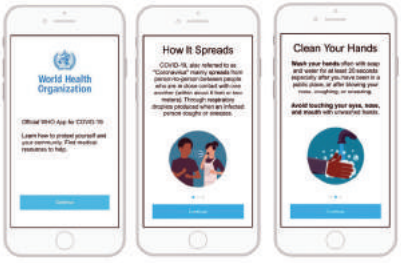
Pour l'instant, la plus diabolique de ces applications est sans doute **"Covid 19 Tracker"**, découvert le 10 mars dernier, car il s'agit non seulement d'un spyware très puissant, mais aussi d'un logiciel de rançon. Quelques heures après son activation, il bloque le smartphone avec un crypto-ransomware et demande 100 dollars en bitcoin pour le débloquer, comme l'explique Tarik Saleh (23).



"Covid 19 tracker" : publicité, visuel et... chantage © Saleh, Domaintools



"Covid 19 tracker" : publicité, visuel et... chantage © Saleh, Domaintools



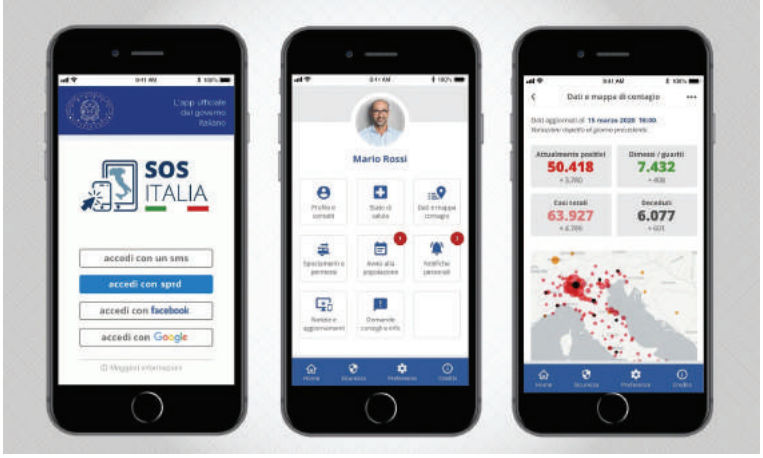
L'interface de l'application MyHealth de l'OMS *selon le prototype donné aux médias © New York Post*

⏩TÉLÉCHARGER les applications garanties par les États, ÉVITEZ l'utilisation des applications des GAFAM

Face à l'énorme quantité d'applications dédiées au virus, l'Organisation mondiale de la santé lancera, début avril, sa propre application, gratuite et disponible dans toutes les langues du monde, appelée *"WHO MyHealth"* (24).

Entre-temps, en Italie, deux initiatives sont prêtes. La première application, à des fins de diffusion sanitaire et scientifique, est destinée à rassurer, conseiller, faciliter l'autodiagnostic des premiers symptômes du virus et suivre les contagions. Il est le résultat du travail d'un groupe scientifique d'excellence, et attend maintenant la validation finale par le ministère de la santé (25).

La seconde, qui vise à la collaboration des citoyens dans la gestion de la crise et facilite la rédaction des formulaires de déplacement hors domicile, est au contraire développée par l'Association italienne pour la révolution numérique avec SOS Italia dans le cadre du projet gouvernemental *"Innova per l'Italia"* (26), propose une application qui a pour premier objectif la simplification de la gestion des pandémies, grâce à un système qui intègre un outil d'autodiagnostic, un compte rendu des dernières nouvelles et des communications officielles, une carte de contagion et un système de gestion de l'auto-certification basé sur les codes QR qui simplifie le travail des services répressifs (27).



Le prototype d'interface de l'application "Sos Italia" © La Stampa

Les applications des GAFAM, toujours la même extraterritorialité, toujours les mêmes pratiques : vos données deviennent leur propriété, ad *eternam*. Aussi, dans ce domaine, il est de notre devoir d'encourager prudence et réflexion avant de prendre la décision de télécharger et d'utiliser l'une des applications officielles des GAFAM et les sociétés qu'elles possèdent.

Cela vaut également pour la plupart des applications payantes qui ont vu le jour dans le sillage de ce nouveau marché. Vérifiez obligatoirement quels paramètres et quelles informations de votre smartphone seront obligatoirement accessibles pour ces app *"pour un fonctionnement optimal"* avant de les télécharger !

Comme pour les réseaux sociaux, vous accepterez en un clic un contrat très long qui explique que toutes vos données **peuvent / seront enregistrées (sans limite de temps) "pour améliorer nos produits"**, comme nous le lisons, pour donner un exemple, dans la *politique de confidentialité* de l'application "COVID-19 Screening Tool" d'Apple (https://www.apple.com/legal/privacy/en-ww/).

3. Un cœur d'or? Ne laissez pas les criminels profiter de votre générosité!

Sur les pages web et les comptes de réseaux sociaux de toutes les polices d'Europe, il ne se passe pas un jour sans qu'une annonce d'urgence soit affichée sur de fausses collectes de fonds, comme, pour l'Italie, celles de la police des communications (28).

La plus grave de ces fausses collectes a visé précisément l'Agence mondiale responsable de la gestion de la crise, l'Organisation mondiale de la santé (OMS). Des millions d'e-mails de phishing ont été envoyés, dans presque toutes les langues du monde, appelant à des dons et copiant des logos ainsi que des parties des descriptions du *"Fonds de réponse de solidarité COVID-19"*, avec de faux numéros de compte bancaire, souvent assorties à des demandes des données personnelles, parfois accompagnées, cerise sur le gâteau, de pièces jointes comprenant des logiciels malveillants. La réaction officielle de l'organe des Nations unies explique bien la gravité de l'incident (29) :

World Health Organization

Beware of criminals pretending to be WHO

Criminals are disguising them selves as WHO to steal money or sensitive information. If you are contacted by a person or organization that appears to be from WHO, verify their authenticity before responding.

The World Health Organization will:

- never ask for your username or password to access safety information
- never email attachments you didn't ask for
- never ask you to visit a link outside of www.who.int
- never charge money to apply for a job, register for a conference, or reserve a hotel
- never conduct lotteries or offer prizes, grants, certificates or funding through email.

The only call for donations WHO has issue dis the COVID-19 Solidarity Response Fund, which is linked to below. Anyother appeal for funding or donations that appears to be from WHO is a scam.

⏩Utilisez uniquement les informations fournies par les sites web officiels.

Le seul conseil, en cette période plus que jamais, est de ne jamais écouter les propositions de cadeaux reçues par courrier électronique. Une fois que vous avez choisi l'organisation ou l'ONG à laquelle vous souhaitez contribuer par un geste en espèces, vous devez vérifier sur le site web original de l'organisation de votre choix quels sont les modes de paiement, les coordonnées et conditions exactes et les références bancaires correctes du bénéficiaire.

4. Vous avez peur ? Attention aux médicaments, masques et autres produits sanitaires en vente en ligne

Sur tous les sites comportant des "annonces", on assiste à une déferlante de publicités incitant à l'achat d'"antiviraux" miraculeux, de masques protecteurs, et de toute une panoplie de moyens destinés à "prévenir la contagion".

Une grande partie des escroqueries - dont certaines sont accompagnées de puissants virus (30) - reçues par courrier électronique profitent de la peur des citoyens et de leur volonté de se protéger: elles touchent ainsi le maillon le plus faible d'une rationalité que nous avons tous tendance à perdre lorsque notre vie ou celle de nos proches est en jeu.

IL FAUT RAPPELER QUE POUR LE MOMENT IL N'EXISTE NI VACCIN NI REMÈDE UNIVERSELLEMENT RECONNU POUR FAIRE FACE AU COVID#19.

Les traitements - à l'**hôpital et uniquement sur place** - qui ont permis le rétablissement de nombreux patients qui ne souffraient pas d'antécédents médicaux graves sont en fait différents d'un pays à l'autre et souvent d'un hôpital à l'autre. Il faut souligner que certains produits encensés par la presse, comme la *chloroquine,* ne sont que des composants partiels des "cocktails pharmaceutiques" développés par les hôpitaux. En tant que tels, ils ne doivent jamais être utilisés en automédication - leur achat est illégal, et leur utilisation sans surveillance médicale a déjà causé de nombreux décès aux États-Unis.

Il est très dangereux d'acheter en ligne sur des sites qui dissimulent bien leur situation géographique réelle. Le moindre des maux, comme dans le cas des fausses polices d'assurance proposant une couverture COVID#19 (31), est que vous ne recevez jamais rien après votre paiement.

Dans le pire des cas, la commande que vous avez achetée arrive chez vous, accompagnée de boîtes et

Histoires d'Internet, p. 19 © Confédération suisse

surtout de médicaments contrefaits, qui sont au mieux de la pâte à farine, au pire un mélange de substances qui peuvent vous emmener directement à l'hôpital, comme l'illustre bien, ci-dessous, une page de la bande dessinée du *Groupe suisse de prévention de la criminalité* (32).

⏩ Utilisez uniquement les sites web originaux de pharmacies ou de boutiques en ligne que vous connaissez déjà.

Pour être en conformité avec vos autorités nationales, n'achetez pas de médicaments provenant d'autres pays, y compris de l'Union Européenne. Les exigences de prescription pour chaque médicament sont très différentes d'un pays à l'autre, tout comme les dosages.

Il en va de même pour l'achat de masques faciaux, de désinfectants médicaux et d'autres produits de santé. La meilleure solution est de vous rendre physiquement à votre pharmacie locale et d'y commander ce dont vous avez besoin.

Attention maximale aux messages *"antivirus care"* faisant référence au site antivirus-covid (différents domaines): une fois que vous ouvrez la page web, elle déclenche un malware très puissant appelé BlackNet sur votre PC (33). Si votre PC est infecté, contactez immédiatement la police.

5. Enfermés à domicile ? Faites attention à vos enfants !

Une attention particulière doit être accordée aux mineurs. Avec les écoles fermées, les cybercriminels multiplient les nouveaux jeux cachant très souvent des logiciels malveillants; de même, on assiste à une vague de tentatives de demande d'amitié sur les réseaux sociaux (à des fins de grooming, pédophilie etc.), signalées par la plupart des polices (34).

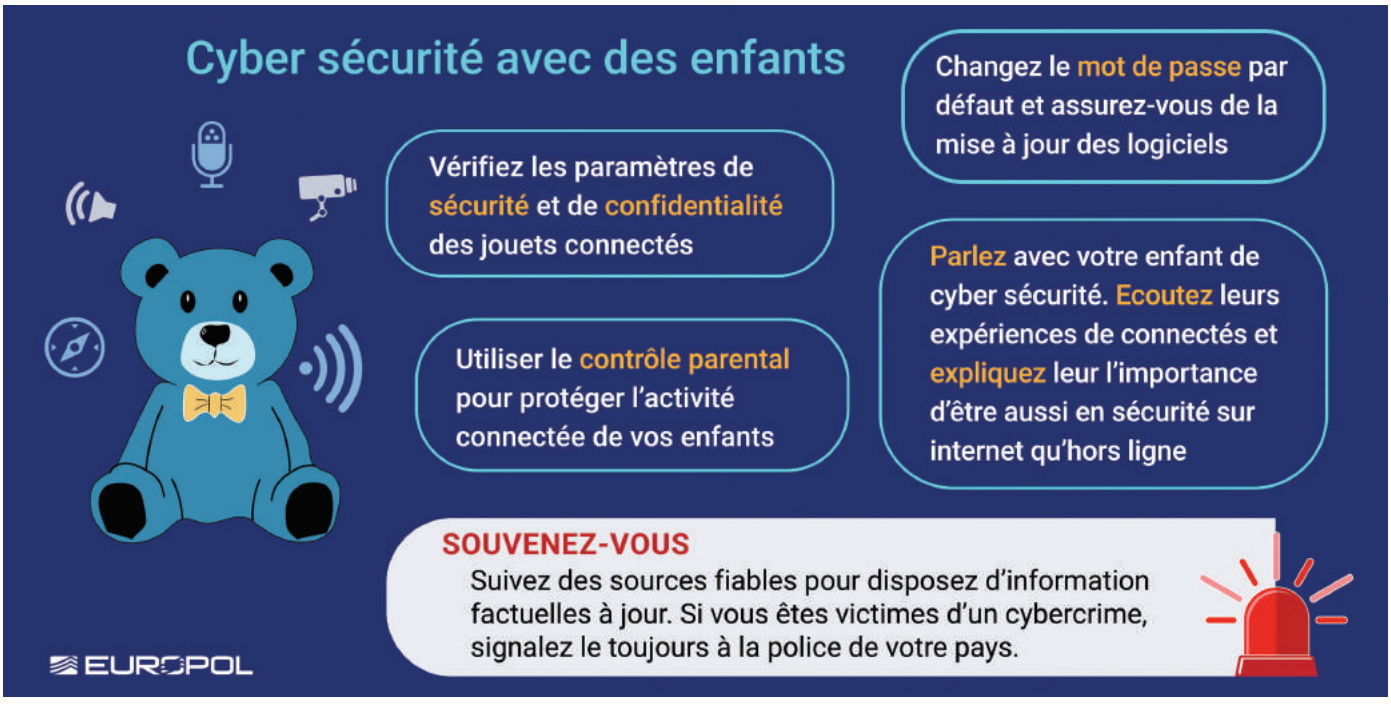
⏩ Achetez uniquement les jeux originaux proposés par les différents "app stores" des producteurs de Smarphone et par les magasins autorisés à vendre des licences de jeux PC/Xbox en ligne.

Une panoplie de mesures à prendre en compte, en fonction de l'âge des mineurs, a été magistralement rédigée par le PPP anglais GetsafeOnline, avec des tutoriels réalisés sous forme de courts clips vidéo faciles à comprendre et adaptés à la situation actuelle *"Assurer la sécurité des enfants en ligne pendant l'épidémie de coronavirus"* (35).

6. Enfermés à domicile ? Attention à vos moments de plaisir et de shopping !

Nous assistons à une attaque généralisée des plateformes de streaming vidéo et de jeux gratuits - un puissant "zero-day" a même interrompu *GooglePlay* pendant une heure - et on assiste à la multiplication d' escroqueries qui renvoient à des sites criminels proposant des mois entiers de films et de jeux gratuits, avec... demande de carte de crédit pour s'inscrire.

Les pires armes contre les plus faibles sont les torrents de courriels de phishing avec de fausses offres commerciales de toutes sortes, qui augmentent de façon exponentielle jour après jour. Bien qu'elles restent plus faciles à détecter car elles sont généralement pleines d'erreurs - dans les langues "mineures" - ou de phrases génériques, certaines sont particulièrement réussies. La méfiance de l'utilisateur est parfois mise à rude épreuve, comme nous le voyons ici dans un cas roumain rapporté par le CERT-RO (36). Si le message est truffé d'erreurs, l'ergonomie du courriel, le positionnement des logos de la grande chaîne de supermarchés allemande et, surtout, le nom du site piège ont été particulièrement bien étudiés: l'adresse est celle de la multinationale (Kaufland.com) à laquelle on a toutefois ajouté "-bon" (cadeau) et, surtout, révélateur du faux: le domaine final du site (.club).



Le faux site web imitant celui des supermarchés Kaufland © CERT-RO

⏩N'achetez rien de ce qui vous est proposé par e-mail en cliquant sur un lien intégré

Vous connaissez parfaitement les sites des magasins dont vous êtes client et où vous avez un compte. Par mesure de précaution, ne cliquez pas sur les offres, même légitimes, de ces mêmes magasins: vous les retrouverez une fois que vous vous serez connecté au site officiel.

7. Enfermés à domicile ? Méfiez-vous de toute offre bancaire / financière !

Dans presque tous les pays européens, il existe une proportion massive de phishing / hameçonnage liée au monde financier. On y lit des offres incroyables comme des crédits élevés à taux d'intérêt zéro, un moratoire sur les hypothèques, le remboursement de gros pourcentages des sommes dépensées à condition d'utiliser ce "nouvel instrument" etc..., comme l'ont très bien résumé la police des communications italienne (37) et, dans le graphique ci-dessous, Europol.

⏩N'achetez rien de ce qui vous est proposé par e-mail en cliquant sur le lien intégré

Surveillez également **vos comptes bancaires**. Vérifiez souvent le solde de votre compte via la banque en ligne. Pour les propriétaires de **Bitcoin**, n'effectuez que les transactions absolument nécessaires: un logiciel de rançon très puissant et complexe, spécialement conçu pour les mouvements de Bitcoin, sévit en ce moment (38).

Le graphique de l'article de Haig © Cointelegraph

8. Travailler à domicile ? Attention à tous les objets connectés !

Beaucoup d'entreprises n'étaient pas prêtes à faire travailler la majorité de leurs employés à domicile. Les protocoles de vidéoconférence, d'accès aux données, mais aussi la résilience des systèmes d'interaction entre le téléphone portable et l'ordinateur portable privé de l'employé et l'infrastructure informatique centrale de l'entreprise (et de son cloud) sont assiégés. Il suffit, pour exemple, de mentionner l'exploit réussi par les pirates informatiques, qui ont trouvé une faille dans les robustes VPN des iPhones, aujourd'hui comblée par Apple.

En outre, dans la "vieille Europe", les réseaux fixes - à l'exclusion des zones à fibres optiques - sont en train de s'effondrer suite à leur sur-sollicitation, dans de nombreuses régions, tandis que la vitesse réellement disponible des réseaux mobiles varie d'une position à l'autre, même dans un même voisinage.

Cela représente évidemment le paradis que les cybercriminels attendent depuis longtemps, non seulement pour saturer encore plus les réseaux, mais aussi pour y introduire des logiciels malveillants et des *"zero days"* de toutes sortes, ainsi que des escroqueries et même des faux appels téléphoniques prétendant être des membres de la direction de la société où travaille tel employé ou des représentants d'autres sociétés / clients / fournisseurs.

⏩ Assurez-vous de bénéficier de la meilleure des protections

a) Installez et mettez à jour tous les antivirus / protections et actualisez régulièrement les systèmes d'exploitation de tous vos appareils.

b) Couvrir la caméra vidéo / les caméras vidéo et les microphones des ordinateurs portables et des téléphones mobiles une fois la téléconférence professionnelle terminée : de nombreux systèmes et protocoles de téléconférence ont été piratés: les entreprises ont réagi avec des correctifs - souvent non installés par les PME - qui ont à leur tour été piratés à nouveau.

c) Conseils pour les smartphones, les tablettes et les PC : pour l'instant, les meilleurs conseils pour sécuriser votre "bureau à domicile" se trouvent, en italien, sur le site de CertFin (cf. 20) et, pour les téléphones portables et les tablettes, sur la page des services de renseignement allemands (39). Conseil : téléchargez les documents et saisissez les textes sur www.deepl.com, le meilleur traducteur en ligne du moment pour les langues de circulation majeures.

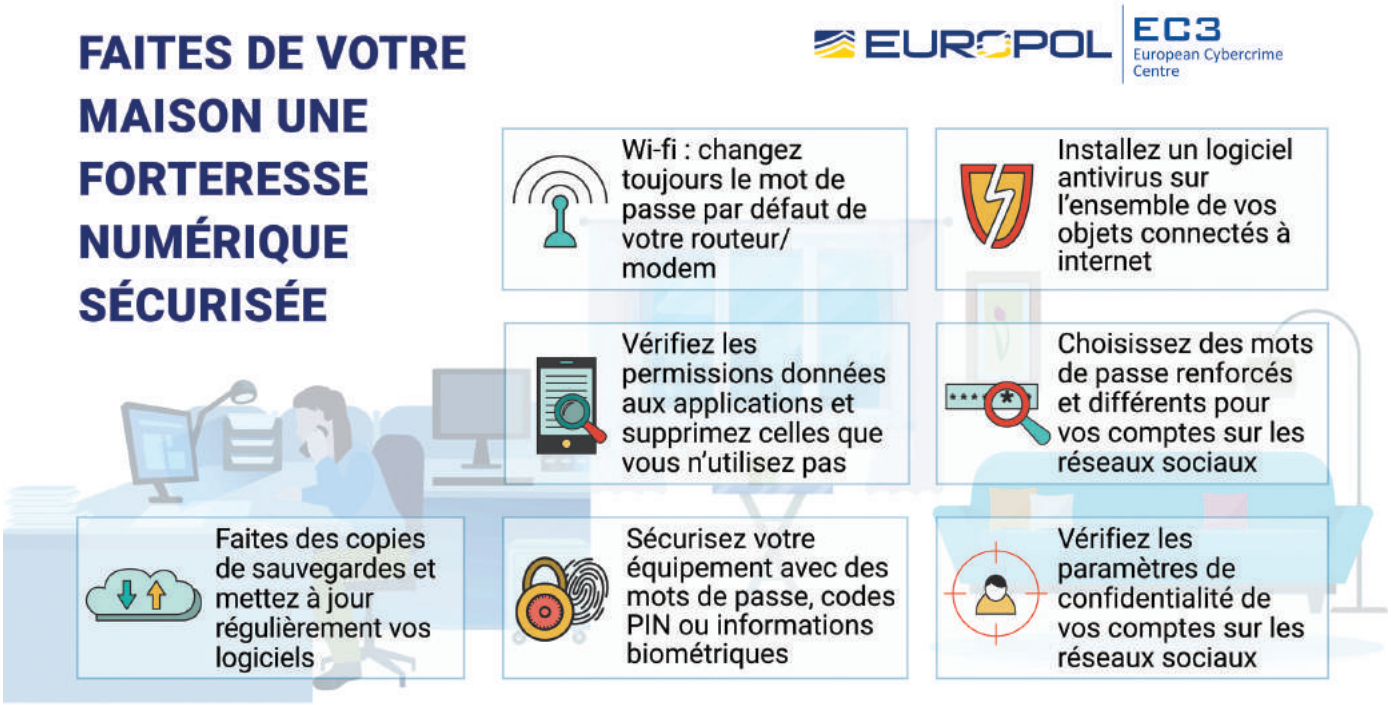
Les lignes directrices (pdf) du Centre canadien pour la cybersécurité (40) et celles de l'IVCAEW (Institut des comptables agréés d'Angleterre et du Pays de Galles) (41) sont très utiles pour une hygiène numérique complète, surtout pour les indépendants, mais aussi pour les simples employés.

Pour les entreprises et la vérification de l'efficacité du système VPN, il est important de consulter l'excellent rapport du Department of Homeland Security qui détaille à la fois les menaces et les solutions (42), ainsi que toutes les recommandations de Staysafeonline, catégorie "Entreprises" (n.10).

9. Médecin, spécialiste médical, directeur d'hôpital ? Vous êtes la cible la plus recherchée !

Il est inutile d'entrer ici dans les détails des innombrables attaques qui visent les établissements de soins et les médecins, et en particulier les outils de télémédecine. Comme nous l'avons déjà expliqué à maintes reprises, la fiche de santé d'un patient vaut cent fois plus au marché noir que les données d'une carte de crédit.

Attention, il n'y a pas que des attaques super sophistiquées : des médecins aux infirmières en passant par tous les employés, toute personne travaillant



dans l'écosystème d'un hôpital est en proie à un nombre exponentiel d'escroqueries, de phishing et autres tentatives de toilettage plus important que les professionnels des autres secteurs (43).

Informez-vous auprès des meilleurs

Comme le système médical au Canada et aux États-Unis d'Amérique est essentiellement privé, les

directives, les alertes et les conseils sont suivis sur les sites gouvernementaux et privés dans ces deux pays (au Canada, tous les documents sont également en variante francophone).

Nous recommandons donc à tous ceux qui travaillent dans le monde médical – et en particulier des responsables de l'infrastructure numérique – de se rendre quotidiennement sur (exemples sélectionnés) : https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations ; https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19?utm_source=hp_slideshowtm_medium=webtm_campaign=dhsgov ; www.healthcareitnews.com ; https://healthitsecurity.com/

Vers où allons-nous ?

Pour terminer sur une note optimiste, nous espérons que les citoyens et les gouvernements tireront les leçons de ce qui se passe. Comme l'a écrit Yuval Noah Harari (n°5), *"L'humanité doit faire un choix. Allons-nous suivre le chemin de la désunion ou adopterons-nous le chemin de la solidarité mondiale ? Si nous choisissons la désunion, cela ne fera pas que prolonger la crise, mais conduira probablement à des catastrophes encore plus graves à l'avenir. Si nous choisissons la solidarité mondiale, ce sera une victoire non seulement contre le coronavirus, mais aussi contre toutes les futures épidémies et crises qui pourraient frapper l'humanité au 21e siècle."*

Il appartient maintenant à chacun d'entre nous de faire dès maintenant les bons choix et de montrer l'exemple en matière de maturité numérique mais aussi de solidarité internationale. ■

Références bibliographiques :

(1) Giorgio Agamben, Riflessioni sulla peste, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste) (passage cité: traduction de l'auteur)

(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/ (passage cité: traduction de l'auteur)

(3) Michel Onfray, Berezina, in Les Observateurs, 17.03.2020 (https://lesobservateurs.ch/2020/03/17/michel-onfray-berezina/)

(4) Slavoj Žižek, TRIBUNE. Surveiller et punir? Oh oui, s'il vous plaît! in Le Nouvel Observateur, 18.03.2020 (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)

(5) Yuval Noah Harari, Il mondo, dopo il Coronavirus, in Ottimisti e Razionali, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/) (passage cité: traduction de l'auteur)

(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

(7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

(8) https://www.csa.gov.sg/singcert

(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html

(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/

(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049

(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

(14) Ravie Lakshmanan : Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

(15) Salvatore Lombardo : L'allarme: Coronavirus, in aumento attacchi cyber, phishing e malspam: consigli per difendersi, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

(16) Europol REPORT : PANDEMIC PROFITEERING : HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS (pdf) https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

(17) Subdomenio COVID dell'INCIBE (Instituto nacional de Ciberseguridad) https://www.incibe.es/cibercovid19

(18) Cert Pubblica Amministrazione, pagina COVID: https://www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/

(19) Agenzia per l'Italia Digitale, pagina COVID: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/27/coronavirus-difendersi-malware-truffe-online

(20) CertFin, pagina COVID: https://www.certfin.it/newsroom/rendi-la-tua-casa-una-cyber-fortezza/

(21) Associazione italiana ingegneri clinici, pagina COVID: http://www.aiic.it/covid19/

(22) Polizia delle Comunicazioni : Coronavirus: Il Ministro Lucia Azzolina denuncia falso documento del Ministero Dell'Istruzione, 21.03.2020 https://www.commissariatodips.it/notizie/articolo/coronavirus-il-ministro-lucia-azzolina-denuncia-falso-documento-del-ministero-dellistruzione/index.html

(23) Tarik Saleh, CovidLock : Mobile Coronavirus Tracking App Coughs Up Ransomware, in Domaintools, 13.03.2020 – con ulteriore link contenente la descrizione tecnica completa del malware https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#

(24) Kyle Bradshaw, World Health Organization to launch COVID-19 tips app for Android, iOS, in 9to5Google, 26.03.2020 https://ww.9to5google.com/2020/03/26/world-health-organization-covid-19-app/#

(25) Elena Tebano, Coronavirus, pronta la app italiana per tracciare i contagi : "Così possiamo fermare l'epidemia", in Corriere della Sera, 20.03.2019 https://www.corriere.it/tecnologia/20_marzo_18/coronavirus-pronta-app-italiana-tracciare-contagi-cosi-possiamo-fermare-l-epidemia-c6c31218-6919-11ea-913c-55c2df06d574.shtml?refresh_ce-cp

(26) https://innovaperlitalia.agid.gov.it/home/

(27) Andrea Nepori, SOS Italia, ecco come potrebbe essere l'app per il monitoraggio dell'epidemia, in La Stampa, 26.03.2020 https://www.lastampa.it/tecnologia/news/2020/03/25/news/sos-italia-ecco-come-potrebbe-essere-l-app-per-il-monitoraggio-dell-epidemia-1.38636482

(28) Polizia delle Comunicazioni : Coronavirus: attenzione alle false campagne di raccolta fondi! https://www.commissariatodips.it/notizie/articolo/coronavirus-attenzione-alle-false-campagne-di-raccolta-fondi/index.html

(29) https://www.who.int/about/communications/cyber-security

(30) Polizia delle Comunicazioni : Coronavirus: BlackNET: RAT distribuito tramite falso "Corona Antivirus" https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(31) Polizia delle Comunicazioni: Coronavirus : false proposte assicurative per la copertura da COVID-19 https://www.commissariatodips.it/notizie/articolo/coronavirus-false-proposte-assicurative-per-la-copertura-da-covid-19/index.html

(32) Storie di Internet. Ufficio federale delle comunicazioni UFCOM Ufficio federale del consumo UFDC Incaricato federale della protezione dei dati e della trasparenza IFPDT Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI Consultabile e scaricabile onlile su: https://www.websters.swiss/it/

(33) Polizia delle Comunicazioni: BlackNET : RAT distribuito tramite falso "Corona Antivirus" https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(34) Polizia delle Comunicazioni : Coronavirus: rischio adescamento minori online https://www.commissariatodips.it/notizie/articolo/coronavirus-rischio-adescamento-minori-online/index.html

(35) Keeping children safe online during the Coronavirus outbreak https://www.getsafeonline.org/news/keeping-children-safe-online-during-the-coronavirus-outbreak/

(36) Continuă valul de campanii de tip scam. Atacatorii se folosesc acum de imaginea Mega Image https://cert.ro/citeste/alerta-scam-kaufland-ikea

(37) Polizia delle Comunicazioni : Coronavirus: smishing con falsi messaggi di istituti di credito https://www.commissariatodips.it/notizie/articolo/coronavirus-smishing-con-falsi-messaggi-di-istituti-di-credito/index.html

(38) Samuel Haig, 'CovidLock' Exploits Coronavirus Fears With Bitcoin Ransomware, in Cointelegraph, 14.03.2020 https://cointelegraph.com/news/covidlock-exploits-coronavirus-fears-with-bitcoin-ransomware

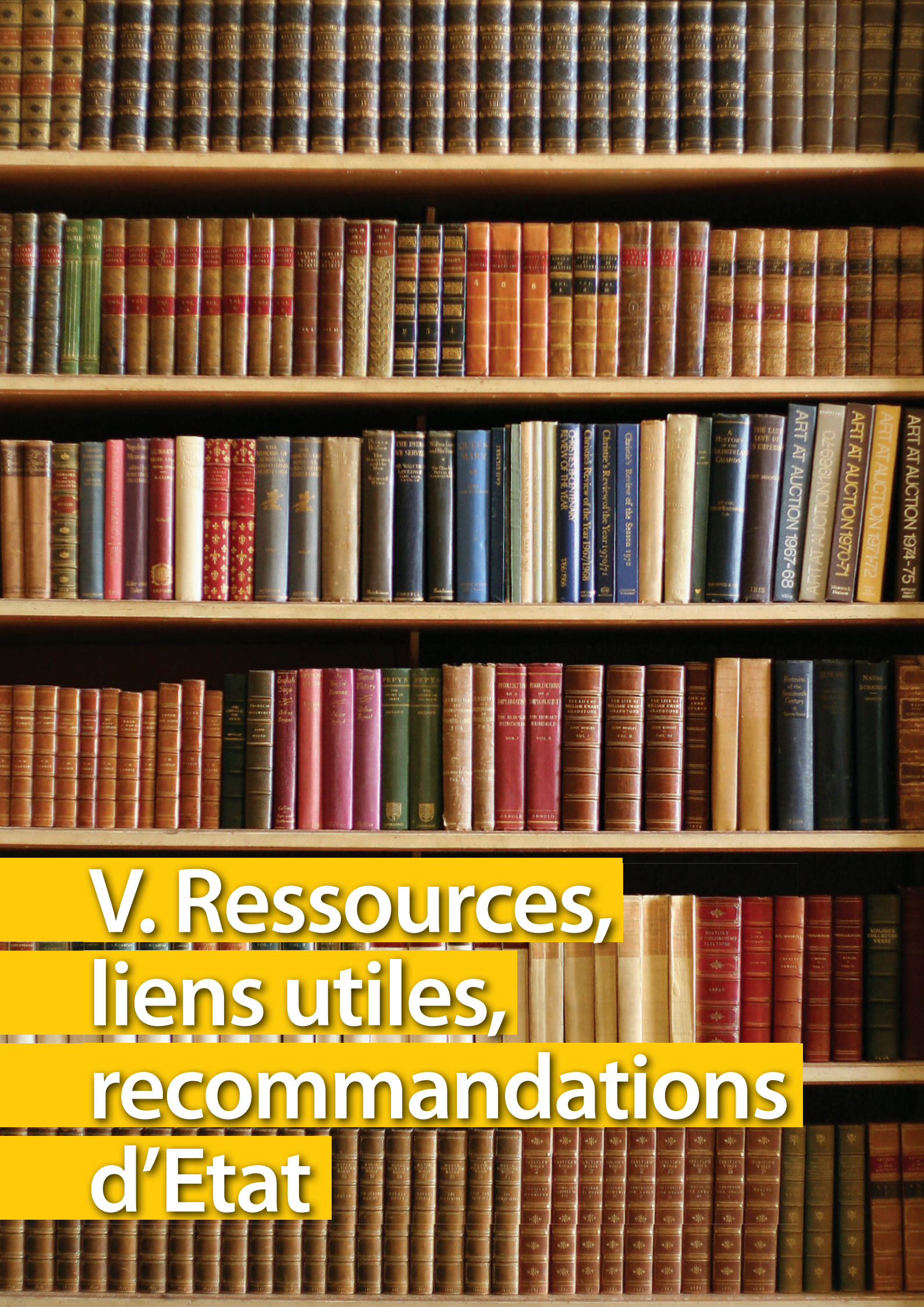
(39) BSI-BUND, Smartphone und Tablet effektiv schützen https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

(40) Canadian Centre for Cyber Security, Cyber Hygiene for COVID-19 https://cyber.gc.ca/sites/default/files/publications/Publication-COVID-19-e.pdf

(41) IVCAEW (Institute of Chartered Accountants in England and Wales), Coronavirus guide : cyber hygiene and data https://www.icaew.com/-/media/corporate/files/technical/information-technology/tech-faculty/coronavirus-guide-cyber-hygiene-and-data.ashx

(42) CISA (U.S. Department of Homeland Security) : Alert (AA20-073A) Enterprise VPN Security https://www.us-cert.gov/ncas/alerts/aa20-073a

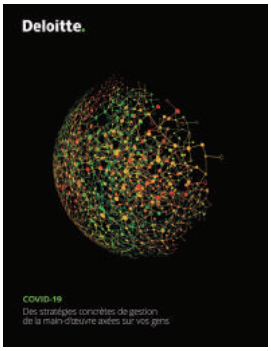
(43) Gareth Corfield, Health workers are top of phishers' target lists thanks to data value, in The Register, 16.03.2020 https://www.theregister.co.uk/2020/03/16/proofpoint_interview/

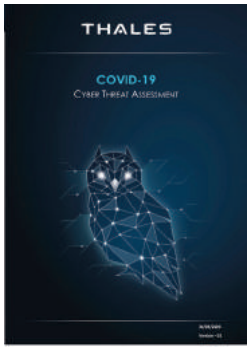


V. Ressources, liens utiles, recommandations d'Etat

Bibliographie

Les derniers rapports complets à ce jour en langue française :





Deloitte, COVID-19 - *Des stratégies concrètes de gestion de la main-d'œuvre axées sur vos gens* (Avril 2020)
(https://www2.deloitte.com/ca/fr/pages/finance/articles/covid-19-practical-workforce-strategies-that-put-your-people-first.html#)
Thalès, *Le télétravail en période de crise : Cyber Threat Assessment* (03.04.2020)
Thalès, *COVID-19 - Cyber Threat Assessment* (24.03.2020)
(les deux volumes sont sur : www.thalesgroup.com/fr/marches-specifiques/systemes-dinformation-critiques-et-cybersecurite/news/le-covid-19-une-nouvelle)

Les sites des autorités compétentes de votre pays :

Confédération Suisse

MELANI - Centrale d'enregistrement et d'analyse pour la sûreté de l'information :
https://www.melani.admin.ch/melani/fr/home.html
Victime d'une attaque/Incident :
www.melani.admin.ch/melani/fr/home/meldeformular.html
Hameçonnage : www.antiphishing.ch

République Française

ANSSI - Agence Nationale de la sécurité des systèmes d'information :
www.ssi.gouv.fr
CNIL - Commission Nationale de l'Informatique et des Libertés :
www.cnil.fr
Cybermalveillance - Assistance et prévention du risque numérique :
www.cybermalveillance.gouv.fr
Témoin de pratiques illégales sur Internet, mais aussi de contenus illégaux, sites d'escroqueries :
www.internet-signalement.gouv.fr
Spams : www.signal-spam.fr
Hameçonnage : www.phishing-initiative.com

Royaume du Maroc

Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) :
www.dgssi.gov.ma/fr
Déclaration d'incidents : MaCERT :
www.dgssi.gov.ma/fr/declaration-d-incidents.html

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

De très nombreuse informations et les images ci-après sont à découvrir sur : https://www.cybermalveillance.gouv.fr/

Coronavirus (COVID-19)

LES PRINCIPAUX RISQUES ET CYBERMENACES LIÉS AU TÉLÉTRAVAIL

L'hameçonnage (*phishing*)

Les rançongiciels (*ransomware*)

Le vol de données

Les faux ordres de virement (FOVI/BEC)

Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Coronavirus (COVID-19)

LES PRINCIPAUX RISQUES ET CYBERMENACES LIÉS AU TÉLÉTRAVAIL

L'hameçonnage (*phishing*)

Les rançongiciels (*ransomware*)

Le vol de données

Les faux ordres de virement (FOVI/BEC)

Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Coronavirus (COVID-19)

LES PRINCIPAUX RISQUES ET CYBERMENACES LIÉS AU TÉLÉTRAVAIL

L'hameçonnage (*phishing*)

Les rançongiciels (*ransomware*)

Le vol de données

Les faux ordres de virement (FOVI/BEC)

Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

Télétravail: Sécuriser son accès à distance

NCSC

PDF original à l'adresse : https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff.html

Introduction

Etant donné l'utilisation accrue des solutions d'accès à distance pour le télétravail, il est opportun de rappeler les bonnes pratiques afin de minimiser le risque lié à ces technologies. Nous sommes convaincus que ce dernier augmente avec l'accroissement des différentes connexions à distance. Des attaquants sont informés de cette situation et tentent, par différents moyens, de gagner accès au réseau des organisations :

- Des tentatives de phishing (qu'elles soient classiques pour l'obtention de mots de passe ou en temps réel dans les cas d'authentification à deux facteurs)
- Attaques contre les mots de passe (attaque de dictionnaire, password spaying ou encore des attaques de brute force)
- Attaques contre les systèmes de gateways non-patché
- Via des maliciel (qui restent souvent non détectés si une tunnellisation de l'ensemble du trafic n›est pas en place).

Contremesures

Considérations quant à la capacité

La mise en place du télétravail peut amener à une augmentation importante des besoins en bande passante. Il est conseillé d'en discuter avec votre fournisseur de télécommunication et votre équipe interne. Cependant, cette augmentation à elle seule n'est pas suffisante. En effet les appareil dits *downstream* tels que les pare-feu, les systèmes anti-intrusion mais aussi les switches et les serveurs pourraient devenir surchargés si leurs capacités ne sont pas elles aussi adaptées.

Mesures contre les maliciels et le phishing

- Toujours utiliser une authentification forte, c›est-à-dire avec au moins **deux facteurs d'authentification** pour vos utilisateurs. La meilleure option serait un facteur matériel tel une clé USB ou une smartcard ou encore un system de OTP *(«One Time Pass-word»)* matériel tel que RSA ou encore MobilleID. Si cela n'est pas possible, un facteur logiciel tel qu'un token OTP avec par exemple Google Authenticator est aussi recommandé
- Mettre en oeuvre et faire respecter les **bonnes pratiques en matière de mots de passe**. Il faut notamment veiller à ce que les mots de passe ne soient pas réutilisés pour différents services et que les utilisateurs n'utilisent pas de séquences (p. ex. xyz2018, xyz2019, xyz2020)
- **Surveiller les logs des accès à distance** pour identifier toute anomalie (p.ex. des adresses IP suspectes, venant de l'étranger alors que votre force de travail est basée en Suisse, des adresses venant de sorties TOR *(«Exit-Nodes»)*, de services VPN et de manière générale venant de réseaux de fournisseurs d'hébergement)

- **Appliquer un tunnel VPN** pour tous les appareils afin de garantir la sécurité des communications et maintenir une visibilité des connexions en direction de l'Internet. Gardez à l'esprit que cette mesure augmentera significativement vos besoins en bande passante
- **Informez vos utilisateurs des dangers** du télétravail et fournissez-leur un **point de contact** unique en cas d'activité suspecte
- Ayez des **plans d'analyse forensique** en place, notamment si les collaborateurs sont autorisés à utiliser leurs appareils pour accéder aux ressources de l'entreprise.
- Assurez-vous que tous les **appareils** d'accès à distance soient **à jour** et définissez **un plan de mise-à-jour d'urgence** *(«emergency patch roll-out»)* en cas de vulnérabilité critique
- Assurez-vous que les appareils puissent être mis à jour sans être physiquement sur place, de préférence en dehors de heures de travail, et avec la bande passante disponible
- Assurez-vous que les utilisateurs de télétravail n'interconnectent pas leur **réseau privé** (du domicile) avec celui de l'entreprise
- Planifiez la remise à niveau et le remote staging d'appareils infectés, p.ex. via une lignes DSL/fibre dédiée.

En plus de ces recommandations, nous vous signalons les documents relatifs à la protection contre les rançongiciels ciblés que nous avons publiés récemment :

- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes
- https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/si-cherheitsrisiko-durch-ransomware.html
- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/as-sets/blocked-filetypes.txt

Sécurité des données

- Assurez-vous que vous avez des **sauvegardes hors-ligne** en cas de rançongiciel
- Assurez-vous que des solutions de sauvegarde soient en place et efficaces si les utilisateurs **enregistrent des données importantes localement**
- Si l'usage des appareils personnels **(BYOD)** augmente, assurez-vous que vous avez des **lignes directrices de base pour ces appareils**, que les données appartenant à votre organisation puissent être enregistrées de manière sûre (par exemple dans un container chiffré) et que ces dernières puissent être effacées efficacement si par exemple l'utilisateur veut revendre son appareil. Pour rappel, les données enregistrées sur des SSD non-chiffrés requièrent un effort supplémentaire pour être effacées.

Sensibilisation

- Mettez en arrêt toutes les **campagnes de sensibilisation** au phishing afin de réduire les perturbations
- Informez vos utilisateurs concernant les **risques additionnels** et demandez-leur de signaler tout courriel ou site web suspect à votre helpdesk
- Assurez-vous que votre **helpdesk est suffisamment équipé** en ressources
- Formez vos utilisateurs à la **sécurisation des réseaux WiFi**
- Informez vos utilisateurs des **moyens de contacter le helpdesk** et dites leur comment celui-ci peut les contacter afin d'éviter les fraudes au soutien («support scam»): https://www.melani.admin.ch/melani/fr/home/themen/fake_support.html
- Mettez en place une méthode d'authentification simple en cas de réinitialisation des mots de passe.

Divers

- Documentez tous les changements durant la situation d'urgence afin de pouvoir revenir à la normale lorsque la situation le permet
- Assurez-vous que les tâches administratives qui requièrent des privilèges élevés soient exécutées depuis des appareil sécurisés qui ne peuvent pas accéder à Internet en même temps. Utilisez des instances de terminal de serveur dédiées si possible
- Si vous observez des tentatives de phishing ou des activités de maliciels, annoncez-les sur www.antiphishing.ch .
- Renseignez-vous sur l'état de la menace cyber actuelle uniquement par des sources sûres tels que : www.ncsc.ch, www.govcert.ch, twitter.com/GovCERT_CH, www.bsi.bund.de/DE/Home/home_node.html, www.ssi.gouv.fr
- Facilitez les demandes de fonctionnalités et d'outils *(«feature and tool request»)* à votre service desk. Si vous ne pouvez pas offrir une solution interne, il est recommandé d'offrir des instructions quant à des solutions tierces afin de minimiser les solutions de rechanges individuelles qui sont impossibles à surveiller.

Résumé

La gestion de risque et la sécurité opérationnelle devraient s'adapter rapidement à la nouvelle surface d'attaque actuelle. Des contre-mesures appropriées devraient être implémentées notamment pour les risques considérés comme critiques. Nous recommandons d'éviter des changements complexes dans la situation actuelle, mais plutôt de réduire les risques en augmentant les la capacité de détection. Si vous avez des questions, n'hésitez pas à nous contacter sur outreach[at]ncsc.ch.

ROYAUME DU MAROC
.....
ADMINISTRATION
DE LA DEFENSE NATIONALE
.....
Direction Générale de la
Sécurité des Systèmes
d'Information

المملكة المغربية
.....
إدارة الدفاع الوطني
.....
المديرية العامة لأمن نظم المعلومات

NOTE D'INFORMATION N° 24100304/20

OBJET : RECOMMANDATIONS DE CYBERSECURITE LIEES AU TELETRAVAIL

La crise sanitaire mondiale du COVID-19 a nécessité la mise en place de mesures de confinement et de limitation des déplacements aux seuls motifs indispensables. Face à cette situation exceptionnelle et inédite, les administrations, entreprises ou collectivités, désignés ci-après entités, qui en avaient la possibilité ont dû mettre en place le télétravail pour préserver les activités essentielles que ce mode de fonctionnement peut permettre.

Cependant, une mise en œuvre non-maîtrisée du télétravail peut augmenter les risques de sécurité pour les entités qui y recourent. Elle peut même mettre en danger leur activité face à une cybercriminalité qui redouble d'efforts au cours des dernières années.

Dans la suite de la note d'information diffusée en date du 20 mars 2020 auprès des Responsables de la Sécurité des Systèmes d'Information (RSSI), la présente note a été élaborée par la Direction Générale de la Sécurité des Systèmes d'Information pour décrire les mesures de sécurité à prendre afin de mieux maîtriser les risques liés au télétravail.

A. PRINCIPAUX RISQUES ET CYBERMENACES LIES AU TELETRAVAIL

Dans ce contexte inédit caractérisé par le recours au télétravail, les entités sont plus exposées à des risques et attaques informatiques. Ces attaques ont pour principaux objectifs :

- **Vol ou altération de données :** Les attaquants tirent profit des mesures de sécurité réduites en dehors des locaux de l'entité pour accéder aux données présentes sur les postes de travail. En effet, à domicile, les postes de travail sont directement exposés au réseau Internet sans protection appropriée (absence de filtrage des flux, présence d'autres équipements sur le même réseau, usage du poste à des fins non professionnelles).
- **Compromission de l'activité :** En ces temps de crise sanitaire, l'activité des entités est davantage tributaire de leurs systèmes d'information. Les attaquants chercheront par tous les moyens à porter atteinte au bon fonctionnement de ces systèmes, notamment à travers des attaques de déni de service. A ce titre, les services en ligne et les plateformes d'accès distant sont les plus visés par ce type d'attaques.

Pour arriver à leurs fins, les principaux moyens et vecteurs d'attaques utilisés sont :

- **L'hameçonnage (phishing)** : Il s'agit de messages frauduleux (email, SMS, chat…) visant à dérober des informations confidentielles (mots de passe, données sensibles de l'entité, informations personnelles ou bancaires) en usurpant l'identité d'un tiers de confiance ou infecter la machine par des codes malveillants (Virus, Ransomware, programme espion,..). Cette technique profite désormais d'une part de l'engouement autour de l'information relative à la pandémie COVID-19 et d'autre part de l'utilisation de la messagerie électronique comme moyen principal de communication entre collaborateurs.
- **Contournement des mécanismes d'accès aux systèmes d'information :** L'accès distant en l'absence de mesures de sécurité appropriées, augmente les possibilités d'accès aux systèmes d'information offertes aux attaquants. Cet accès, peut se faire directement en exploitant des insuffisances sur les systèmes et applications exposés sur Internet, ou indirectement en passant à travers un poste utilisateur compromis utilisé comme point de rebond.

B. MESURES DE PROTECTION LIEES AU TELETRAVAIL

Pour faire face aux risques précités, il est recommandé de mettre en œuvre les mesures de cybersécurité ci-après et d'attirer l'attention du RSSI pour veiller à leur application :

1. **Utiliser des moyens et équipements appropriés pour le télétravail** : Il est fortement recommandé de privilégier autant que possible l'utilisation de moyens, mis à disposition, sécurisés et maîtrisés par l'entité (dotés d'Antivirus, Firewall, cryptage des disques…) et de renforcer la sécurité d'accès aux systèmes d'information sensibles.
2. **Limiter les accès distants** : L'ouverture des accès extérieurs ou distants doit être réservée aux personnes et services indispensables, et faire strictement l'objet d'un filtrage au niveau du pare-feu. Ces accès doivent s'appuyer sur des privilèges adéquats et se limiter aux besoins des utilisateurs. Il convient aussi de cloisonner les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver.
3. **Sécuriser les accès distants** : Les connexions distantes aux systèmes d'information internes doivent systématiquement s'effectuer via un réseau privé virtuel (VPN). La mise en place d'une double authentification est à privilégier pour se prémunir de l'usurpation de l'identité.
4. **Renforcer la politique de mots de passe** : Les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. Dans ce contexte, Il convient aussi de réduire la durée de changement des mots de passes et implémenter des mécanismes pour contrecarrer des attaques par force brute. Au moindre doute ou même en prévention, il faut changer les mots de passe et activer la double authentification chaque fois que cela est possible.

5. **Veiller au respect du déploiement des mises à jour de sécurité** : Tous les équipements et systèmes et en particulier ceux qui sont exposés au réseau Internet (postes nomades, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité…) doivent systématiquement et immédiatement bénéficier des mises à jour de sécurité. En effet, un défaut de mise à jour d'un seul équipement est souvent la cause d'une intrusion dans le réseau des entités.

6. **Veiller à la sauvegarde des données** : Ne disposant pas forcément des mécanismes de sauvegarde automatiques déployés au niveau central des entités, les télétravailleurs doivent être sensibilisés sur l'importance de sauvegarder eux même régulièrement leurs données afin de faire face à d'éventuelles pertes de données suite à une cyberattaque (Ransomware par exemple).

7. **Superviser l'activité des accès externes et systèmes sensibles** : Cette supervision doit permettre à l'entité de pouvoir détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou élévation des privilèges d'un utilisateur connu, ou encore un volume inhabituel de téléchargement d'informations…

8. **Activer la journalisation au niveau de l'infrastructure de télétravail :** La journalisation est souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque. Aussi, il convient d'activer la journalisation notamment au niveau des postes nomades, des équipements périmétriques et des services exposés.

9. **Respecter les règles de sécurité au niveau des plateformes collaboratives**: L'usage des plateformes en Cloud pour l'échange d'informations professionnelles (Visio conférence, Partage de documents, messagerie, etc..) doit se faire en veillant à ne pas partager des données sensibles. En tout cas et autant que faire se peut, il est recommandé de recourir à des connexions VPN et à des mécanismes d'authentification forte.

10. **Sensibiliser et apporter un soutien aux télétravailleurs :** Il s'agit de Donner aux télétravailleurs des consignes claires sur ce qu'ils peuvent faire ou ne pas faire et les sensibiliser aux risques de sécurité liés au télétravail. Il convient d'attirer leur attention notamment sur :
    - L'usage exclusif des équipements de télétravail à des fins professionnelles ;
    - L'usage du protocole sécurisé (WPA2) et de mots de passes robustes pour protéger le réseau wifi à domicile ;
    - La déclaration systématique de tout incident ou événement suspect au RSSI de son entité.

Pour toute éventuelle assistance ou complément d'informations, veuillez contacter la DGSSI sur l'adresse électronique suivante : **contact@dgssi.gov.ma**.

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

PRATIQUES EXEMPLAIRES EN CYBERSÉCURITÉ POUR LA COVID-19

Le Centre pour la cybersécurité a constaté que des auteurs malveillants se servent de plus en plus du coronavirus (COVID-19) pour mener des campagnes d'hameçonnage et d'escroquerie liées à des maliciels.

L'Agence de la santé publique du Canada dirige la réponse à la COVID-19 en collaboration avec les responsables et les organismes de la santé publique d'un bout à l'autre du Canada. Pour obtenir les renseignements les plus récents sur la COVID-19, veuillez consulter la page Web du gouvernement du Canada concernant la mise à jour sur l'éclosion.

MÉFIEZ-VOUS DES TROMPERIES

À mesure que l'inquiétude du public à l'égard de la COVID-19 s'accroît, le nombre de tentatives d'hameçonnage faisant référence au virus augmente. L'hameçonnage consiste à envoyer des courriels de masse qui semblent provenir d'une source légitime, mais qui contiennent une pièce jointe infectée ou un lien malveillant. Les courriels sont rédigés de manière à inciter les destinataires à ouvrir une pièce jointe ou à cliquer sur un lien pour permettre aux auteurs de menaces d'obtenir des justificatifs d'identité personnels ou d'accéder sans autorisation à un système informatique. Dans certains cas récents, des auteurs malveillants se sont fait passer pour divers organismes de santé dans leurs tentatives d'hameçonnage.

Les auteurs de cybermenace saisissent rapidement l'occasion de profiter d'événements fortement médiatisés, surtout si ces événements soulèvent des inquiétudes ou des préoccupations.

COMMENT VOUS PROTÉGER

Voici quelques mesures à prendre afin de protéger votre appareil contre les maliciels :

Courriels malveillants :

- Assurez-vous que l'adresse ou la pièce jointe est liée au contenu du courriel.
- Assurez-vous de connaître l'expéditeur du courriel.
- Vérifiez s'il y a des coquilles.
- Utilisez un logiciel antivirus ou antimaliciel sur vos ordinateurs.

Pièces jointes malveillantes :

- Assurez-vous que l'adresse courriel de l'expéditeur comprend un nom d'utilisateur et un nom de domaine valides.
- Méfiez-vous si le ton de l'expéditeur est urgent.
- Si vous ne vous attendiez pas à recevoir une pièce jointe, vérifiez auprès de l'expéditeur.

Sites Web malveillants :

- Assurez-vous que les URL sont bien épelées.
- Tapez l'URL directement dans la barre de recherche au lieu de cliquer sur le lien fourni.
- Si vous devez cliquer sur un hyperlien, pointez votre curseur sur le lien pour vérifier qu'il vous dirigera bel et bien vers le site Web indiqué.

4 MOYENS PRATIQUES DE RENFORCER VOTRE CYBERSÉCURITÉ

- Utilisez des mots et des phrases de passe uniques et complexes
- Mettez à jour vos ordinateurs, vos applications et vos appareils mobiles
- Stockez vos données de façon sécurisée et sachez comment récupérer les copies de sauvegarde
- Sécurisez vos comptes de médias sociaux et de courriel

Êtes-vous prêt?

Mesures de sécurité des TI visant à protéger votre organisation

Une publication

web for business
swiss webacademy

Rédaction :
Laurent Chrzanovski et
Romulus Maier (†)

ISSN 2559 - 1789
ISSN-L 2559 - 1789

Adresse :
Şcoala de Înot nr.18,
550005, Sibiu, Roumanie
https://swissacademy.eu/
https://cybersecurity-dialogues.org

Page spéciale pour télécharger ce numéro :
https://swissacademy.eu/cybercovid/

Congrès partenaires

CHARENTE-MARITIME CYBER SÉCURITÉ — CMCS-CONNECT.FR —

CYBERSECURITY PUBLIC - PRIVATE DIALOGUES — CYBERSECURITY-DIALOGUES.ORG —

FIC — FORUM-FIC.COM —

Stanchion Payment Solutions

Global Payment Specialists

Our experience in complex payments environments and our international perspective of client engagements enable us to offer a range of solutions, services and products to integrate, improve, optimise and secure your payments systems.

Please contact us at *engage@stanchionpayments.com* for further details on our security and payment health-check services.

Visit our website: *stanchionpayments.com/insights/brochures/* to download free brochures on security and securing your payments systems.

STANCHION

Engage | Innovate | Solve | Secure

www.stanchionpayments.com