



DESINFORMATION, CYBERATTAQUES ET CYBERMALVEILLANCE : « L'AUTRE GUERRE DU COVID 19 »

La crise sanitaire, course au « tout digital », a considérablement accru l'exposition au risque informatique. Elle s'accompagne d'un accroissement des « fausses nouvelles » (fake news) aux effets potentiellement délétères, accompagnant parfois les campagnes d'influence de certaines puissances étrangères. Elle met à l'épreuve les systèmes d'information des établissements de santé, cibles qui doivent être mieux protégées. Elle force à une utilisation massive et rapide du télétravail. Cette bascule en urgence vers le « tout digital » accentue le risque d'actes de cyber malveillance.

Communication de MM. Olivier CADIC et Rachel MAZUIR, sénateurs, rapporteurs pour le programme 129 de la loi de finances (SGDSN, ANSSI et Cybersécurité), pour la commission des affaires étrangères et de la défense du Sénat

Pendant le confinement lié à la crise sanitaire, les rapporteurs de la commission des affaires étrangères, de la défense et des forces armées poursuivent leurs travaux en télétravail. Cette communication écrite vise à en rendre compte. Elle sera soumise à l'approbation de la commission lors de sa plus prochaine réunion plénière.

Les situations de crises sanitaires sont propices à la diffusion massive de fausses nouvelles qui peuvent être dangereuses pour la santé et perturber la mise en place des politiques publiques. La crise du Covid 19 montre de façon plus inquiétante le déploiement de stratégies d'influence ambiguës, voire agressives de puissances étrangères comme la Chine, pouvant utiliser des informations inexactes ou tronquées afin de valoriser de son modèle social comme clef du succès de la lutte contre la pandémie et son caractère indispensable pour apporter les produits sanitaires nécessaires, critiquer ouvertement les mesures mises en œuvre par les autres Etats et faire pression sur tous ceux qui dévoilent les objectifs de cette communication. Une guerre de la communication a été enclenchée, destinée à réécrire l'histoire et à dénigrer les démocraties pour préparer la reconfiguration du paysage géopolitique de l'après-crise.

Les systèmes d'information des acteurs de la santé doivent être mieux protégés : on y observe une concentration de cyber-attaques (18 en un an, d'après l'ANSSI), fruit d'un sous-investissement chronique en dépense de sécurité informatique.

La crise sanitaire a précipité 8 millions de Français vers le télétravail, contre 5,2 millions en télétravail partiel auparavant. Des compromis ont été faits avec la sécurité des réseaux. Les cyberattaquants ont tout de suite exploité l'inquiétude en multipliant les opérations d'hameçonnage¹. Les sites de vente en ligne proposant médicaments, masques, gels hydro-alcooliques et autres produits de santé² ont

¹ Diffusion de messages contenant des liens ou des pièces jointes corrompues afin de recueillir des données personnelles ou s'introduire dans les systèmes d'exploitation des ordinateurs

² Le 31 mars, l'OMS a mis en garde sur l'existence de sites web non enregistrés commercialisant des produits soi-disant efficaces contre la COVID-19 et susceptibles d'être falsifiés

proliféré, avec pour objectif, outre une escroquerie à la vente, de récupérer des numéros de cartes bancaires. Désormais les attaques par « rançongiciel » (déblocage contre rançon des systèmes d'information d'une entreprise) se développent.



La situation est particulièrement propice au développement de l'espionnage économique, même s'il reste à ce stade difficile à déceler.

Les rapporteurs concluent leur étude par plusieurs recommandations concrètes :

- *Mettre en œuvre une force de réaction cyber afin de répondre aux fausses informations dans le domaine sanitaire et aux attaques contre les valeurs démocratiques et pour lutter contre les campagnes de désinformation ou d'influence de certains acteurs étrangers.*
- *Investir dans la sécurité informatique des acteurs de la santé ;*
- *Lancer sans tarder une campagne de communication à grande échelle pour promouvoir la plateforme « cybermalveillance.fr » et diffuser les « gestes barrière numériques » ;*
- *Initier une communication régulière, au travers des médias, d'un top 10 des cyber-crimes constatés sur le territoire ;*
- *Unifier la chaîne de recueil et de traitement des plaintes en ligne, aujourd'hui de la compétence des autorités de police et de gendarmerie locales ;*

I. Un contexte propice à la multiplication des « fausses informations » et des stratégies d'influence

► **« Fake news » : une stratégie française qui repose avant tout sur le dialogue avec les grandes plateformes d'Internet**

La crise sanitaire aussi a vu se multiplier la diffusion des fausses informations, dans le climat propice d'isolement et de grande anxiété. Ces fausses informations relèvent majoritairement de la bêtise ordinaire, mais peuvent avoir des conséquences graves, lorsqu'elles touchent à la santé publique³, au complotisme, voire à la fraude. D'autres, enfin, procèdent **d'intentions malveillantes visant à déstabiliser l'action publique ou à développer des stratégies d'influence**. Il est donc important pour les autorités publiques de suivre cette situation et de combattre ses effets.

Les autorités publiques ont mis en place une stratégie différenciée de réponse et d'entrave. La situation est suivie au niveau interministériel. **L'Ambassadeur du numérique**, qui a pour mission de garantir la sécurité internationale du cyberspace, à travers la promotion de la stabilité et de la sécurité internationale dans le cyberspace et la régulation des contenus diffusés sur internet, est un des principaux acteurs.

³ par exemple une rumeur selon laquelle la consommation de cocaïne immuniserait contre le Covid 19 ou en Iran la consommation d'alcool avec de nombreux cas d'intoxication mortels au méthanol

Dans un système démocratique fondé sur la liberté d'expression et la liberté de la presse, la stratégie qui consiste d'abord à distinguer ce qui relève de la liberté d'opinion des fausses informations, diffusées plus ou moins intentionnellement. Il s'agit ensuite d'une action de responsabilisation des diffuseurs, pouvant déboucher sur un encadrement juridique.

S'agissant des fausses informations concernant la santé publique, le secrétaire d'État au numérique, comme d'ailleurs la Commission européenne, **dialoguent avec les principales plateformes** en les incitant à jouer les régulateurs dans un esprit civique, en enlevant systématiquement les messages dangereux⁴ et en mettant en avant les messages des sources référencées (institutions, organes de presse).



Jean-Marc, agissez maintenant pour ralentir la propagation du coronavirus (COVID-19)

Sur certaines on voit s'afficher des bandeaux qui pointent vers une actualité Covid 19 référencée et vérifiée (voir ci-contre).

Dans le même esprit, les autorités publiques ont souhaité **développer une politique de communication claire et transparente** en distinguant, la communication institutionnelle⁵ et la communication politique⁶ et **rendre accessibles toutes les données selon le principe de l'open data** sans cacher les difficultés rencontrées à faire remonter certaines informations et améliorant progressivement le dispositif afin d'éviter un débat sur la réalité des informations diffusées, ce qui n'empêche pas un débat public intense sur les réponses apportées à la crise. **Les autorités publiques devraient préparer de façon plus intense la déclinaison de l'expertise scientifique dans des contenus en ligne fiables et didactiques.**

Le développement d'une réglementation appropriée (élections, lutte contre le harcèlement, lutte contre le terrorisme) a permis d'établir un dialogue avec les responsables opérationnels des grandes plateformes, mais en l'absence d'une véritable transparence sur les algorithmes qui permettent de pousser telle information vers tel utilisateur, ce qui permettrait d'avoir une régulation plus efficace, ce dialogue reste imparfait.

► Une action diplomatique cohérente et réactive nécessaire face aux stratégies d'influence parfois fondées sur la désinformation

Sur le plan international, nous assistons au développement d'une **stratégie d'influence particulièrement active de la Chine**, tendant à occulter ses erreurs dans la gestion initiale de l'épidémie⁷, sous un « narratif » vantant l'efficacité du modèle chinois de surveillance généralisée et le bienfondé de son organisation sociale pour réduire l'épidémie. La Chine insiste également sur sa générosité par la mobilisation de ses capacités industrielles recouvrées au service des autres États, pour les aider à surmonter la crise, démontrant de façon de moins en moins implicite son caractère de « puissance indispensable ».

Cette stratégie se déploie ouvertement sur internet et les réseaux sociaux, avec l'utilisation de méthodes sophistiquées qui vont au-delà de la simple propagande allant jusqu'à la diffusion fréquente de fausses informations, tronquées ou manipulées⁸. Dans un contexte où

⁴ Les principales plateformes sont assez actives. Elles sont même allées jusqu'à effacer des messages du président du Brésil qui contrevenaient aux prescriptions des autorités de santé.

⁵ Exemple point de presse quotidien et très factuel du directeur général de la santé, le Professeur Salomon.

⁶ Portée par le Président de la République, le Premier ministre et le ministre de la santé et de solidarités.

⁷ Allant parfois jusqu'à contester le lieu d'apparition du virus (

<https://twitter.com/AmbassadeChine/status/1242011628608118786>) ou à occulter l'aide reçue de l'Europe

⁸ <http://www.amb-chine.fr/fra/zfzj/t1768712.htm> : « Or, dans le même temps, en Occident, on a vu des politiciens s'entredéchirer pour récupérer des voix ; préconiser l'immunisation de groupe, abandonnant ainsi leurs citoyens

la critique de cette stratégie est parfois difficile, du fait de la dépendance de la plupart des États aux produits de santé fabriqués en Chine ; elle fait l'objet de ripostes plutôt agressives des autorités chinoises⁹.



La Russie et les médias « patriotes » qui la soutiennent, sont moins actifs dans le contexte de la crise sanitaire. Ils n'en continuent pas moins d'utiliser toutes les opportunités pour susciter des sentiments de défiance à l'égard de l'Union européenne. En revanche, ils **se montrent actifs en Afrique** pour dénigrer la présence française et critiquer ses initiatives. Se diffusent également sur ce continent des rumeurs et fausses informations attribuant la responsabilité de l'épidémie ou ses conséquences aux Français et aux Occidentaux, plus généralement.

Tant que cette situation ne porte pas atteinte à la sécurité nationale, les autorités françaises réagissent par les canaux diplomatiques habituels et par des prises de positions publiques¹⁰. **Ainsi, le ministre de l'Europe et des affaires étrangères, M. Jean-Yves Le Drian a-t-il convoqué l'ambassadeur de Chine pour lui signifier sa "désapprobation" vis-à-vis de "certains propos récents" critiquant la réponse occidentale à la pandémie de nouveau coronavirus**¹¹, publiés sur le site de l'ambassade ou sur son compte Twitter.

Elles soutiennent aussi les initiatives prises par certains médias et ONG pour identifier et dénoncer les fausses informations en mettant des outils à la disposition des chercheurs et des journalistes¹².

Il est clair qu'une **guerre de la communication a été enclenchée**, destinée à réécrire l'histoire et à dénigrer les démocraties pour préparer la reconfiguration du paysage géopolitique de l'après-crise. Dans cette bataille des opinions, **les démocraties européennes ne doivent pas se montrer naïves**. Elles doivent au contraire accroître la défense et la promotion de leurs valeurs en renforçant leur vigilance et en se dotant d'instruments efficaces.

Nous recommandons la mise en place une force de réaction cyber afin de répondre aux fausses informations dans le domaine sanitaire, aux attaques contre les valeurs

seuls face à l'hécatombe virale; s'entre dérober des fournitures médicales ; revendre à des structures privées les équipements achetés avec l'argent public pour s'enrichir personnellement ; on a fait signer aux pensionnaires des maisons de retraite des attestations de « Renonciation aux soins d'urgence »; les personnels soignants des EHPADs ont abandonné leurs postes du jour au lendemain, ont déserté collectivement, laissant mourir leurs pensionnaires de faim et de maladie... ».

⁹ N'hésitant pas à prendre à partie certains chercheurs ou parlementaires français et les médias qui relaient leurs opinions ou à faire pression sur des hauts fonctionnaires allemands pour qu'ils diffusent des positions favorables à la Chine AFP 14 avril 2020 14:28. « Les autorités taiwanaises, soutenues par plus de 80 parlementaires français dans une déclaration co-signée, ont même utilisé le mot « nègre » pour s'en prendre à lui (le directeur de l'OMS ndr). Je ne comprends toujours pas ce qui a pu passer par la tête de tous ces élus français.» <http://www.amb-chine.fr/fra/zfzj/t1768712.htm>

¹⁰ Le 24 mars, le Haut représentant de l'Union européenne pour les affaires étrangères et la politique de sécurité Josep Borrell s'est inquiété de la "bataille mondiale des narratifs" et "des luttes d'influence" en cours via la "distorsion" des faits et la "politique de générosité" chinoise. Le 29 mars, la secrétaire d'Etat aux Affaires européennes, Amélie de Monchalain, a reproché à la Chine, mais aussi à la Russie, "d'instrumentaliser" leur aide internationale et de la "mettre en scène 30 Mars 2020, 16h00, AFP

¹¹ <https://www.diplomatie.gouv.fr/fr/dossiers-pays/chine/evenements/article/communiqu%C3%A9-de-jean-yves-le-drian-14-04-20>

¹² ex : <https://disinfo.quaidorsay.fr/fr/>, qui, en source ouverte, fournit des outils permettant l'identification des émetteurs, de voir s'ils sont soutenus par une usine de robots...

démocratiques et pour lutter contre les campagnes de désinformation ou d'influence de certains acteurs étrangers.

II. L'INDISPENSABLE PROTECTION DES SYSTÈMES D'INFORMATION DU SECTEUR DE LA SANTÉ

► Une fragilité structurelle, fruit d'un sous-investissement chronique

Déjà dans un récent rapport en décembre dernier,¹³ nous avons noté que le ministère de la santé et des solidarités et ses opérateurs principaux avaient subi, **en 2018, 8 attaques cyber nécessitant l'intervention de l'ANSSI, dont 2 qualifiées de « majeures »**. L'année 2019 a confirmé cette fragilité avec les attaques récentes par rançongiciels du CHU de Montpellier au printemps, de 120 établissements privés du groupe Ramsay-Générale de santé, en août, et du CHU de Rouen en novembre. **Au total, en 2019, l'ANSSI a répertorié 18 attaques par rançongiciels contre ce secteur d'activité¹⁴. Cette densité d'attaques résulte d'un sous-investissement chronique en sécurité informatique.** Sous la contrainte budgétaire, le développement des applications a été privilégié à la sécurité informatique laissant les établissements à la merci d'attaquants pour lesquelles les entités, dont la rupture d'activité aurait un impact social important, sont des cibles intéressantes.

► Des attaques sporadiques mais de faible intensité depuis le début de la crise sanitaire

Dans un communiqué de presse, plusieurs groupes de *hackers* ont indiqué qu'ils suspendaient provisoirement leurs attaques contre les établissements de santé.

Pour autant, l'ANSSI a relevé des attaques par déni de service contre l'AP-HP (Paris) le 22 mars dernier¹⁵ et contre l'AP-HM (Marseille) sans grands dommages, et une attaque par rançongiciel contre l'établissement public de santé de Lomagne (Gers).

À l'étranger, des attaques ont touché le CHU de Brno (République tchèque), l'OMS, le département fédéral de la santé des Etats-Unis et l'agence de santé de l'Illinois.

Enfin des attaques, a priori sans lien avec la crise, perturbent certains services publics locaux (région de Marseille, communes du Morbihan)¹⁶ avec des conséquences sur la gestion de la crise (remontées des informations de l'état-civil vers Santé publique France, services funéraires...).

► Une remise à niveau très partielle et une vigilance renforcée

Depuis l'automne dernier, l'ANSSI a développé une procédure d'intervention d'urgence auprès des quinze principaux CHU pour renforcer leur niveau de protection tout en recherchant un effet de levier de ces établissements chefs de file sur les quelque 3000 établissements du secteur de santé. Elle n'est plus en mesure de poursuivre cette action actuellement car les DSI des hôpitaux sont totalement mobilisées pour assurer le fonctionnement des installations nécessaires à la lutte contre le Covid 19.

¹³ <http://www.senat.fr/rap/a19-142-9/a19-142-9-syn.pdf>

¹⁴ <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf>

¹⁵ consistant à générer une grande quantité de connexions simultanées pour surcharger les serveurs.

¹⁶ <https://www.ssi.gouv.fr/actualite/lanssi-sensibilise-et-transmet-des-recommandations-de-securite-a-destination-des-collectivites-territoriales/>, https://l'expansion.lexpress.fr/high-tech/cyberattaques-de-nouvelles-mairies-ranconnees-a-l-heure-du-coronavirus_2122763.html

Paradoxalement, l'hétérogénéité actuelle du parc hospitalier pourrait éviter une contamination massive d'un établissement à un autre mais **on ne pourra se dispenser à terme d'augmenter le niveau de la cybersécurité de tout ce secteur et d'y consacrer des moyens importants.**

L'ANSSI a aussi renforcé sa vigilance sur le système de santé et les secteurs périphériques : environnement des établissements hospitaliers, certaines industries pharmaceutiques, acteurs de plus petite taille et nouveaux entrants comme les entreprises ou les laboratoires de recherche impliqués dans la fabrication de produits (masques....) ou la recherche (tests, vaccins, médicaments) moins coutumiers de cybersécurité.

Nous relevons une **grande fluidité dans l'échange d'informations et de solutions au sein de l'Union européenne**, par exemple après l'attaque contre l'hôpital de Brno. La coopération entre les agences fonctionne et les initiatives de la Commission portent aussi leurs fruits.

III. Une entrée massive et rapide dans le « tout digital » qui a accru l'exposition aux attaques

► Une explosion parfois mal maîtrisée des usages du numérique

En quelques jours, **8 millions de Français ont basculé la totalité de leur activité en télétravail**, contre 5,2 millions qui y avaient recours plus ou moins partiellement. Rares sont les organisations qui avaient pu anticiper un basculement de cette ampleur ou l'envisager de façon cohérente et intégrée à un plan de continuité d'activité. **La bascule a été effectuée dans l'urgence, parfois avec les moyens du bord**, avec les ordinateurs personnels des salariés et par l'utilisation de plateformes existantes non sécurisées (visio-conférences notamment)¹⁷.

Bien souvent, la sécurité informatique a été sacrifiée à l'efficacité immédiate. En ont découlé une élongation des réseaux informatiques des organisations dans un environnement moins maîtrisé et donc une dégradation assumée de leur résilience. De la même façon, les mesures de confinement ont conduit à un développement important de l'usage de l'internet et des réseaux sociaux pour toutes sortes d'activités (enseignement à distance, usages culturels, relations personnelles).

En Espagne, Telefonica évoque ainsi une *"augmentation de trafic de près de 40%"*¹⁸, Telecom Italia, *"une augmentation de plus de 70 % du trafic Internet sur [le] réseau fixe* ». Le 20 mars, le PDG d'Orange Stéphane Richard estimait que, rien qu'en France, *"Le télétravail a été multiplié par 7, les visioconférences par 2, et le trafic WhatsApp par 5"*¹⁹. Ajouté au risque de relâchement de l'attention dans cette période d'anxiété, ce basculement peut avoir des conséquences graves alors que, tendanciellement, la cybercriminalité progresse de 10% par an²⁰.

► Un risque avéré de renforcement de la cybermalveillance

¹⁷ Voir les débats sur la sécurité de certaines plateformes de visioconférence sur l'Internet

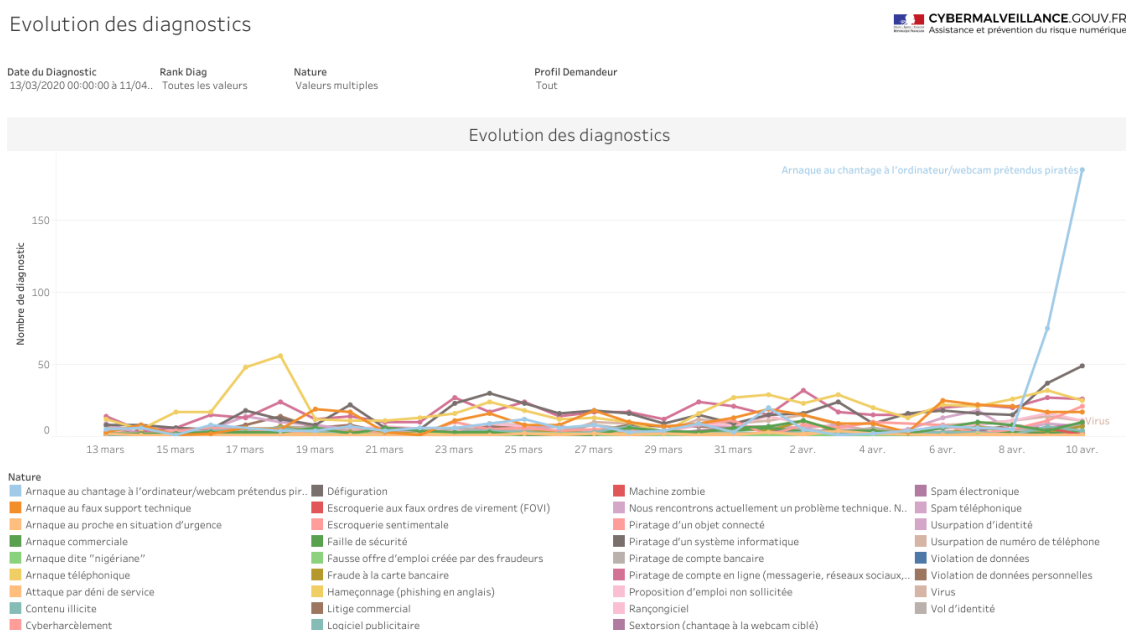
¹⁸ L'utilisation des téléphones portables a augmenté d'environ 50% pour la voix et de 25% pour les données. « Le trafic provenant d'outils de messagerie instantanée a été multiplié par 5 et celui lié aux outils de travail à distance par 4. »

¹⁹ Interview donnée à RTL

²⁰ Selon la neuvième étude annuelle sur le coût de la cybercriminalité publiée en 2019 par Accenture et le Ponemon Institute, la cybercriminalité augmente de plus de 10% par an.

- *L'explosion de la petite criminalité sur Internet*

De façon générale, les cyberattaquants exploitent l'inquiétude. Très vite, tant le GIP ACYMA²¹ que la Gendarmerie nationale²² observent une explosion de la petite criminalité qui profite de la situation de vulnérabilité pour monter de **nombreuses opérations d'hameçonnage²³**. **Se multiplient les sites de vente en ligne, plus ou moins fictifs, proposant médicaments, masques, gels hydro-alcooliques et autres produits de santé²⁴**, dont certains ont pour objectif, outre une escroquerie à la vente, de récupérer des numéros de cartes bancaires. Des alertes identiques ont été lancées par les agences américaine et britannique de cybersécurité.



Depuis trois semaines, conséquence de ces actions d'hameçonnage, le GIP ACYMA assiste à une croissance d'attaques effectives, notamment par « **rançongiciels** »²⁵. Il s'attend à une vague plus importante avec des **risques de paralysie des systèmes informatiques** de PME, déjà éprouvées par la crise, voire de collectivités territoriales, perturbant des services indispensables en période de crise sanitaire.

- *Une probabilité forte d'actions d'espionnage économique*

S'agissant des menaces de plus haute intensité, l'ANSSI observe une situation plus calme mais analyse, sur la base de signaux faibles, que **les actions d'espionnage progressent**, profitant de la dégradation de la sécurité des systèmes d'information. Les effets n'en seront perçus que dans plusieurs mois. Cette hypothèse est confirmée par une étude récente du groupe Thalès²⁶ à partir de renseignements recueillis dans les pays d'Asie, voisins de la Chine, confrontés à la crise dès février.

²¹ Dispositif d'assistance aux victimes de la cybercriminalité

²² Qui gère la plateforme SIGNAL-SPAM <https://www.signal-spam.fr/>

²³ Diffusion de messages contenant des liens ou des pièces jointes corrompues afin de recueillir des données personnelles ou s'introduire dans les systèmes d'exploitation des ordinateurs

²⁴ Le 31 mars, l'OMS a mis en garde sur l'existence de sites web non enregistrés commercialisant des produits soi-disant efficaces contre la COVID-19 et susceptibles d'être falsifiés

²⁵ Blocage des systèmes d'information qui ne peut être réactivé qu'après versement d'une rançon. Et plus récemment une explosion des tentatives d'escroqueries crypto-porno.

²⁶ <https://www.lefigaro.fr/flash-eco/covid-19-les-cyberattaques-d-origine-etatique-en-hausse-avertit-thales-20200330>

► Une prise de conscience insuffisante ; un traitement des infractions à unifier

Nous avons pu constater lors de nos auditions que les acteurs publics concernés étaient pleinement mobilisés.

Les acteurs concernés se sont mobilisés pour renforcer les mesures de prévention, notamment via le site cybermalveillance.gouv.fr

L'ANSSI et le GIP ACYMA ont dû adapter leurs organisations. Le renforcement des mesures de prévention est une priorité. Dès le 16 mars, « cybermalveillance.gouv.fr » a publié une recommandation²⁷ bien relayée entraînant une multiplication par 10 des consultations journalières (de 1500 à 15000 avec un pic à 22 000)²⁸.



Des actions d'effacement, afin de rendre inaccessibles les liens vers les sites à visée frauduleuses, peuvent aussi être demandées aux entreprises qui attribuent les noms de domaine. Le 23 mars, un nouvel article²⁹ a été publié sur le site « cybermalveillance.fr » pour formuler des recommandations aux entreprises et aux usagers en télétravail.

Toutefois, nous pensons qu'il faut amplifier l'effort de communication pour diffuser la nécessité de « gestes barrière numériques ».

Ces messages devraient être relayés plus régulièrement et plus intensément. En effet, cette actualité est restée marginale, dans la presse, par rapport aux informations sur la situation sanitaire ou les mesures de sauvegarde économiques et sociales et le risque est grand que certaines entreprises qui subissent de plein fouet la crise ne puissent se relever si une attaque cyber les affecte, de surcroît. Pour ce faire, le renforcement des moyens du GIP ACYMA pour conduire une campagne de communication de cette ampleur est nécessaire.

Nous recommandons la mise en place rapide d'une campagne ciblée de promotion de la plateforme « cybermalveillance » via les organisations en contact quotidien avec les entreprises : banques, assurances, organisations patronales, chambres de commerce et d'industries, presse professionnelle, et certains réseaux sociaux : LinkedIn, Viadéo...

A plus long terme, il faut s'engager vers le renforcement par chaque entreprise des budgets réservés à la sécurité informatique.

Nous préconisons d'initier la communication régulière, au travers des médias, d'un top 10 des cyber-crimes constatés sur le territoire afin d'aider à la prise de conscience générale des menaces qui pèsent sur la population et les entreprises.

²⁷ <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite>

²⁸ Elle a été lue plus de 150 000 fois au cours des deux semaines suivants sa publication.

²⁹ <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail>, cet article a été lu 35 000 fois dans la semaine suivant sa publication.

Enfin, les outils d'entrave et de répression de la cybercriminalité doivent être simplifiés. L'unification de la chaîne de recueil et de traitement des plaintes en ligne nous apparaît nécessaire et urgente ; elle demeure, sauf évocation par la section spécialisée du parquet de Paris, la compétence des autorités de police et de gendarmerie locales, alors que les faits procèdent de mêmes auteurs et de mêmes modes opératoires sur tout le territoire.

<p>Commission des affaires étrangères, de la défense et des forces armées http://www.senat.fr/commission/etr/index.html 15 rue de Vaugirard 75006 Paris - secretariat-affetra@senat.fr</p>	
 <p>M. Christian Cambon, Président Sénateur du Val-de-Marne (Groupe Les Républicains)</p>	
<p>Les rapporteurs pour avis sur le programme 129 « Coordination du travail gouvernemental »</p>	
 <p>M. Olivier Cadic (Union centriste - sénateur des Français établis hors de France)</p>	 <p>M. Rachel Mazuir (Socialiste - sénateur de l'Ain)</p>