# N° 502

# SÉNAT

SESSION ORDINAIRE DE 2019-2020

Enregistré à la Présidence du Sénat le 10 juin 2020

# RAPPORT D'INFORMATION

FAIT

*au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le suivi de la* **cybermenace** *pendant la* **crise sanitaire***,*

Par MM. Olivier CADIC et Rachel MAZUIR,

Sénateurs

*(1) Cette commission est composée de :* M. Christian Cambon*, président ;* MM. Pascal Allizard, Bernard Cazeau, Olivier Cigolotti, Robert del Picchia, Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini*, vice-présidents ;* Mme Joëlle Garriaud-Maylam, M. Philippe Paul, Mme Marie-Françoise Perol-Dumont, M. Olivier Cadic*, secrétaires ;* MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Alain Cazabonne, Pierre Charon, Mme Hélène Conway-Mouret, MM. Édouard Courtial, René Danesi, Gilbert-Luc Devinaz, Jean-Paul Émorine, Bernard Fournier, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Claude Haut, Mme Gisèle Jourda, MM. Jean-Louis Lagourgue, Robert Laufoaulu, Ronan Le Gleut, Jacques Le Nay, Rachel Mazuir, François Patriat, Gérard Poadja, Ladislas Poniatowski, Mmes Christine Prunaud, Isabelle Raimond-Pavero, MM. Stéphane Ravier, Hugues Saury, Bruno Sido, Rachid Temal, Raymond Vall, André Vallini, Yannick Vaugrenard, Jean-Pierre Vial, Richard Yung.

# S O M M A I R E

Pages

***Rapport de suivi de la cybermenace pendant la crise sanitaire de***
***MM. Olivier Cadic et Rachel Mazuir***

*Avertissement : Pendant le confinement lié à la crise sanitaire du coronavirus, les sénateurs rapporteurs de la commission des affaires étrangères, de la défense et des forces armées ont poursuivi activement leur travail d'information et de contrôle du Gouvernement, via des entretiens en téléconférence, destinés à mesurer l'impact de la crise sanitaire sur les secteurs dont ils avaient la charge, et à proposer des mesures pour y faire face.*

*Publié d'abord sous forme de communication écrite le 16 avril 2020, ce rapport d'information a été adopté par la commission des affaires étrangères et de la défense, lors de sa réunion plénière du 10 juin 2020.*

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

(Situation au 16 avril 2020)

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.

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 ambigües, 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'hameçonnage[1]. Les sites de vente en ligne proposant médicaments, masques, gels hydro-alcooliques et autres produits de santé[2] ont proliféré, avec pour objectif, outre une escroquerie à la vente, de récupérer des numéros de cartes bancaires.

---

[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*

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.**

**Ce rapport formule 5 recommandations concrètes :**

**❶ 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.**

**❷ Investir dans la sécurité informatique des acteurs de la santé ;**

**❸ Lancer sans tarder une campagne de communication à grande échelle pour promouvoir la plateforme « cybermalveillance.fr» et diffuser les « gestes barrière numériques » ;**

**❹ Initier une communication régulière, au travers des médias, d'un top 10 des cyber-crimes constatés sur le territoire ;**

**❺ 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

### ► Lutte contre les « 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 publique[1], au complotisme, voire à la fraude. D'autres, enfin, procèdent

[1] *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*

**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 cyberespace, à travers la promotion de la stabilité et de la sécurité internationale dans le cyberespace et la régulation des contenus diffusés sur internet, est un des principaux acteurs.

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 dangereux 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 institutionnelle[1] et la communication politique[2] 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 règlementation 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

[1] *Exemple point de presse quotidien et très factuel du directeur général de la santé, le Professeur Salomon.*
[2] *Portée par le Président de la République, le Premier ministre et le ministre de la santé et de solidarités.*

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'épidémie[1], 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 manipulées[2]. Dans un contexte où 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 chinoises[3].


**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

---

1 *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*

2 *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 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… ».*

3 *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 ndlr). 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*

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 publiques[1]. **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**[2], 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 journalistes[3].

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

---

[1] *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 Monchalin, 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*

[2] *https://www.diplomatie.gouv.fr/fr/dossiers-pays/chine/evenements/article/communique-de-jean-yves-le-drian-14-04-20*

[3] *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…*

## 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,[1] nous avions 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'activité**[2]. **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 dernier[3] 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)[4] avec des conséquences sur la gestion de la crise** (remontées des informations de l'état-civil vers Santé publique France, services funéraires…).

---

[1] http://www.senat.fr/rap/a19-142-9/a19-142-9-syn.pdf

[2] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

[3] *consistant à générer une grande quantité de connexions simultanées pour surcharger les serveurs.*

[4] https://www.ssi.gouv.fr/actualite/lanssi-sensibilise-et-transmet-des-recommandations-de-securite-a-destination-des-collectivites-territoriales/, https://lexpansion.lexpress.fr/high-tech/cyberattaques-de-nouvelles-mairies-ranconnees-a-l-heure-du-coronavirus_2122763.html

**► 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.

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)[1].

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

[1] *Voir les débats sur la sécurité de certaines plateformes de visioconférence sur l'Internet*

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%*"[1], 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*"[2]. 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 an[3].

### ► Un risque avéré de renforcement de la cybermalveillance

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

De façon générale, les cyberattaquants exploitent l'inquiétude. Très vite, tant le GIP ACYMA[4] que la Gendarmerie nationale[5] observent une explosion de la petite criminalité qui profite de la situation de vulnérabilité pour monter de **nombreuses opérations d'hameçonnage[6]. Se multiplient les sites de vente en ligne, plus ou moins fictifs, proposant médicaments, masques, gels hydro-alcooliques et autres produits de santé**[7], 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.

---

[1] *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. »*

[2] *Interview donnée à RTL*

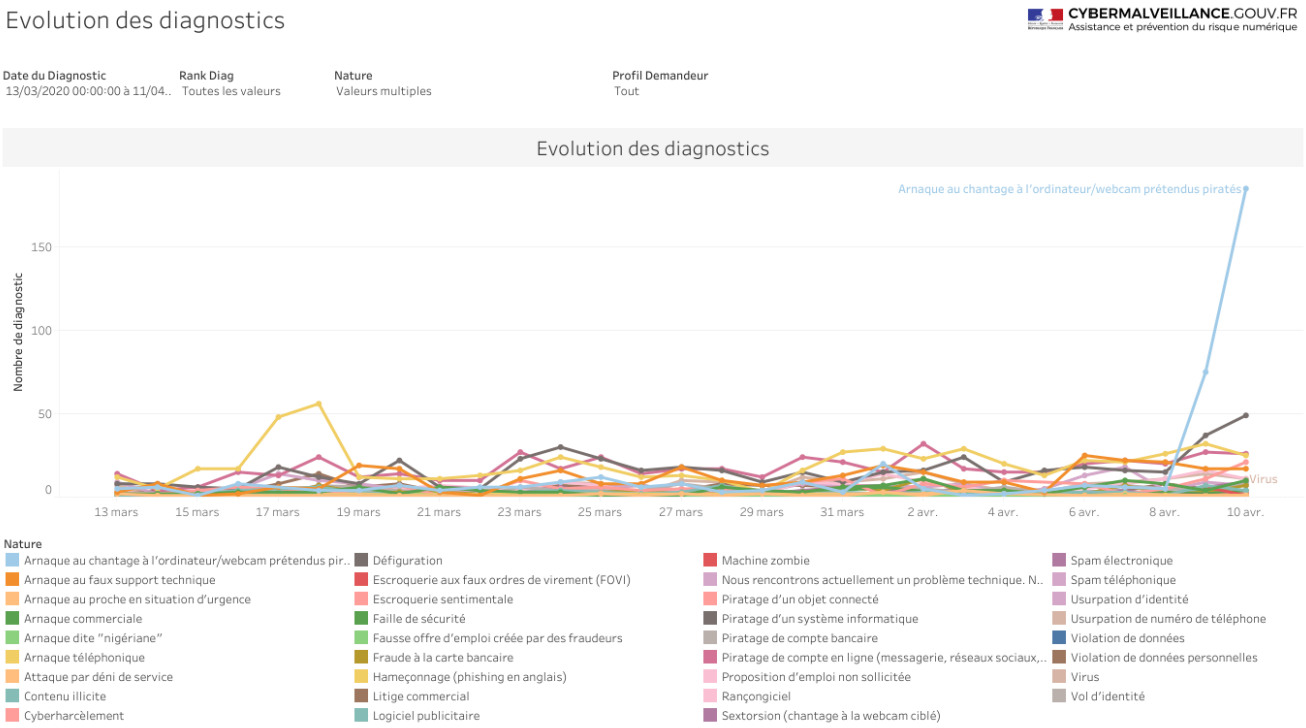
[3] *Selon la neuvième étude annuelle sur le coût de la cybercriminalité publiée en 2019 par Accenture et le Ponemon Institute, la cybercriminalité augmente de plus de 10% par an.*

[4] Dispositif d'assistance aux victimes de la cybercriminalité

[5] *Qui gère la plateforme SIGNAL-SPAM https://www.signal-spam.fr/*

[6] *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*

[7] *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*




Depuis trois semaines, conséquence de ces actions d'hameçonnage, le GIP ACYMA assiste à une croissance d'attaques effectives, notamment par **« rançongiciels »**[1]. 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 Thalès[2] à partir de renseignements recueillis dans les pays d'Asie, voisins de la Chine, confrontés à la crise dès février.

[1] *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.*

[2] *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 cybermaveillance.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 recommandation[1] bien relayée entraînant une multiplication par 10 des consultations journalières (de 1500 à 15000 avec un pic à 22 000)[2].



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 article[3] 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 surcroit. Pour ce faire, le renforcement des moyens du GIP ACYMA pour conduire une campagne de communication de cette ampleur est nécessaire.

---

[1] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite

[2] *Elle a été lue plus de 150 000 fois au cours des deux semaines suivants sa publication.*

[3] 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.*

**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.

**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.

# EXAMEN EN COMMISSION

*Réunie le mercredi 10 juin 2020, la commission des affaires étrangères, de la défense et des forces armées, présidée par M. Christian Cambon, président, a procédé à l'examen du rapport d'information de MM. Olivier Cadic et Rachel Mazuir.*

**M. Olivier Cadic. –** La commission nous a demandé de suivre l'évolution des cybermenaces dans le contexte de la crise sanitaire et des mesures de confinement qui en ont été les conséquences. Nous vous avons transmis le document intitulé « Désinformation, cyberattaques et cybermalveillance : l'autre guerre du covid-19 ». Rachel Mazuir interviendra sur les deux premiers aspects. Je vais, pour ma part, traiter la désinformation qui nous a conduit à recommander de mettre en place une force de réaction cyber afin de lutter contre les campagnes de désinformation ou d'influence de certains acteurs étrangers.

La crise sanitaire a vu se multiplier la diffusion des fausses informations, dans le climat propice d'isolement et de grande anxiété. Celles-ci relèvent majoritairement de la bêtise ordinaire, mais peuvent avoir des conséquences graves, lorsqu'elles touchent à la santé publique, au complotisme, voire à la fraude. D'autres procèdent d'intentions malveillantes visant à déstabiliser l'action publique ou à développer des stratégies d'influence.

La situation est suivie au niveau interministériel. Les autorités publiques ont mis en place une stratégie de réponse et d'entrave.

Dans un système démocratique libéral, la stratégie distingue ce qui relève de la liberté d'opinion des fausses informations diffusées plus ou moins intentionnellement et vise à responsabiliser des diffuseurs, voire à mettre en place un encadrement juridique.

Pour le traitement des infox concernant la santé publique, le dialogue avec les principales plateformes, a permis de retirer les fausses nouvelles ou de promouvoir l'information crédible. Nos autorités ont soutenu 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 journalistes.

Plus inquiétant, nous avons assisté au développement d'une stratégie d'influence particulièrement active de la Chine, sur internet et les réseaux sociaux. Le gouvernement chinois a cherché à occulter ses erreurs dans la gestion initiale de l'épidémie, sous un « narratif » vantant l'efficacité du modèle chinois et sa générosité au service des autres États pour surmonter la crise. Les autorités chinoises sont allées jusqu'à la diffusion

fréquente de fausses informations, tronquées ou manipulées. Cela a conduit le Ministre de l'Europe et des affaires étrangères à convoquer l'ambassadeur de Chine pour lui signifier sa désapprobation. Nous constatons que l'ambassade de Chine n'a pas retiré ces informations de son site dont certaines constituent des attaques directes envers des collègues parlementaires.

Suite à la communication de notre rapport, des représentants religieux nous ont également alertés sur les désinformations qui les ont atteints. Pour information le régime communiste chinois ne s'en prend pas qu'aux Ouïghours musulmans, il a fermé l'année dernière plus de 5 500 églises et institutions religieuses chrétiennes.

Il est clair qu'une guerre de la communication a été enclenchée, destinée à réécrire l'histoire et à dénigrer les démocraties. Une reconfiguration du paysage géopolitique de l'après-crise se prépare. 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.

Voilà pourquoi nous avons recommandé la mise en place une force de réaction cyber afin lutter contre les campagnes de désinformation ou d'influence d'états totalitaires ou autoritaires qui s'en prennent aux démocraties et relativisent l'intérêt du respect des droits de l'Homme. Cela nous a valu un fort intérêt, manifesté par les médias mais aussi par les experts. Nous souhaiterions pouvoir poursuivre nos travaux sur cette question afin de préciser les contours de cette force, qui de notre point de vue, doit aller au-delà des réponses étatiques conventionnelles pour être efficace.

**M. Rachel Mazuir. –** Dans notre dernier rapport nous avions noté la fragilité de la sécurité des systèmes d'information du ministère de la santé et de ses opérateurs qui ont subi 18 attaques en 2019. On se souvient de celle visant le CHU de Rouen en novembre. Sous contrainte budgétaire, le développement des applications a été privilégié à la sécurité 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 et faciles.

Plusieurs groupes de hackers ont indiqué qu'ils suspendaient leurs attaques contre les établissements de santé pendant la crise. Pour autant, l'ANSSI a relevé des attaques contre l'AP-HP (Paris) et contre l'AP-HM (Marseille) sans grands dommages, il faut le reconnaître, et une attaque par rançongiciel contre l'établissement public de santé de Lomagne (Gers) cher à notre collègue Raymond Vall. Enfin des attaques, ont perturbé certains services publics locaux (région de Marseille, communes du Morbihan).

Depuis l'automne dernier, l'ANSSI a développé une procédure d'intervention d'urgence dans les CHU mais elle a dû la suspendre car les DSI étaient totalement mobilisées pour assurer le fonctionnement des installations nécessaires à la lutte contre le Covid 19.

Pendant la crise, l'ANSSI a aussi renforcé sa vigilance sur les secteurs périphériques impliqués dans la fabrication de produits (masques….) ou la recherche (tests, vaccins, médicaments).

Parallèlement, l'entrée massive et rapide dans le « tout digital » a accru l'exposition aux attaques. 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 qui a souvent été effectué avec les moyens du bord. La sécurité informatique a été sacrifiée à l'efficacité immédiate. 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). Selon le PDG d'Orange, rien qu'en France, le télétravail a été multiplié par 7, les visioconférences par 2, et le trafic WhatsApp par 5.

De façon générale, les cyberattaquants exploitent l'inquiétude. Très vite, une explosion de la petite criminalité – les grandes entreprises elles étaient déjà protégées, et des opérations d'hameçonnage a été observée. Des sites de vente en ligne, plus ou moins fictifs, proposant médicaments, masques, et autres produits de santé se sont multiplié ; certains ayant pour objectif, de récupérer des numéros de cartes bancaires. Des alertes identiques ont été lancées par les agences américaine et britannique de cybersécurité.

Puis, avec un léger décalage, le GIP ACYMA a assisté à une croissance d'attaques effectives, notamment par « rançongiciels ». Il s'attend à une vague plus importante avec des risques de paralysie des systèmes informatiques de PME, qui souvent sont peu protégées et ont déjà été éprouvées par la crise.

L'ANSSI analyse, sur la base de signaux faibles, que les actions d'espionnage progressent. Les effets n'en seront perçus que dans plusieurs mois. Cette hypothèse est confirmée par une étude du groupe Thalès sur la situation en Asie.

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

Toutefois, nous pensons qu'il faut amplifier l'effort de communication pour diffuser les « gestes barrière numériques » et, pour ce faire, renforcer des moyens du GIP ACYMA. Le directeur général de la plateforme, qui a relayé largement notre rapport, nous a indiqué avoir pu, grâce à cette recommandation, obtenir de France Télévisions des espaces publicitaires gratuits pour diffuser ses messages de vigilance.

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

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 est nécessaire. Je ferai un commentaire personnel : depuis le temps que nous écrivons des rapports, vous devez avoir l'impression que nous faisons beaucoup de constats. Nous faisons le constat que l'ANSSI est un excellent gendarme mais ce n'est, à mon avis, pas suffisant. Il va falloir développer une autre façon de faire avec des propositions plus offensives. On ne peut pas continuer à jouer aux gendarmes, j'ai le sentiment qu'il faudrait aller au-delà.

**M. Christian Cambon, président. –** Notre collègue Michel Boutant fait également un travail important sur ce sujet. Je pense qu'aucune institution n'était prête à faire face à la crise covid-19, qui était certes inattendue mais qui aurait pu être précédée ou suivie d'une autre crise – je pense à un incident nucléaire majeur en région parisienne, par exemple, empêchant les pouvoirs publics parisiens de travailler. Nous avons dû inventer un nouveau système de télétravail, avec des difficultés, sur la qualité des transmissions par exemple. Il est nécessaire que l'on s'attache à cette question et que l'on protège notamment les parlementaires et les informations qu'ils manient. La dématérialisation systématique comporte des dangers pour les entreprises également. On peut penser aux sous-traitants auprès de nos grands groupes d'industrie de défense avec qui les échanges d'informations vont s'intensifier du fait des nouvelles règles de téléconférence. Il y a donc une sensibilité sur les secrets industriels, les savoir-faire et les bonnes pratiques.

Je rappelle la décision du Bureau de la commission d'inclure, pour l'ensemble des différents programmes budgétaires que suit la commission, une vigilance particulière sur les conséquences à tirer de la crise du Covid-19. Cette crise va changer très profondément nos manières de penser et nos manières de travailler.

**Mme Hélène Conway-Mouret. –** Pensez-vous qu'il y ait une prise de conscience collective sur la situation que vous avez décrite, qui est inquiétante à tous les niveaux ? Cette menace cyber est existentielle pour notre démocratie puisqu'elle peut aller – et nous en savons quelque chose avec l'utilisation du vote électronique pour les français de l'étranger-, jusqu'à la remise en cause de la sincérité d'un scrutin qui peut être altéré si un système est hacké. Deuxième question, nous avons tous déploré ne pas avoir accès à un système européen et encore moins français avec la possibilité de partages de données protégées des puissances étrangères. Avez-vous le sentiment qu'il y ait une volonté d'aider au développement de tels outils en France ou au niveau européen ? Jusqu'à présent nous avons davantage été dans la réaction que dans la prévention, nous laissant un temps de retard qui nous expose.

**M. Olivier Cadic. –** Oui, la prise de conscience de la menace est de plus en plus forte. La plateforme cybermalveillance.gouv.com est un outil important. Des personnes qui ne sont pas conscientes au départ de la menace, peuvent être dévalisées sans sortir de chez elles et ne pas savoir vers quelle institution se tourner. De nouveaux réflexes se mettent en place. Le site cybermalveillance.gouv.com délivre l'information pour chacun puisse savoir comment réagir, notamment comment déposer sa plainte. Nous avons été heureux qu'à la suite de ce rapport, le site cybermalveillance ait pu avoir des espaces publicitaires gratuits sur France Télévision.

Le besoin d'un outil souverain est fort. Dès que nous avons publié notre rapport, des experts nous ont contactés pour nous signifier leur plein accord avec cette analyse. La difficulté tient à sa mise en œuvre car la force de réaction cyber existe dans le domaine militaire mais nous ne sommes pas armés dans le domaine civil. C'est la démocratie au sens large qui est attaquée et nous ne pouvons donc faire un outil uniquement gouvernemental. Le gouvernement tout seul ne peut pas répondre à tout. Le Parlement peut se saisir de ce dossier et réfléchir aux contours de cette force afin de formuler des propositions.

**M. Rachel Mazuir. –** Il y a des progrès autour d'un cœur de gens qui s'intéressent au sujet mais cela n'est pas encore tout à fait passé dans le grand public. Le site cybermalveillance a néanmoins vu sa fréquentation exploser, ce qui nous satisfait.

**M. Christian Cambon, président.** - Soyons aussi attentifs à nos propres comportements.

**M. Robert del Picchia. –** L'introduction de la 5G va avoir des conséquences en matière de cybersécurité et pourrait potentiellement introduire de nouvelles vulnérabilités. Monaco a déjà accepté la 5G et d'autres pays pourraient franchir le pas. L'Etat va en débattre et nous devrions en débattre aussi.

**M. Pascal Allizard. –** J'adhère complètement aux propos de Robert del Picchia. Je voudrais simplement rappeler qu'il était convenu dans le texte 5G que nous avons voté ici, il y a un an, au mois de juin, une clause de revoyure. L'objectif était de maîtriser le déploiement de la 5G. Les Européens doivent rattraper leur retard technologique. Nous avions décidé qu'il faudrait retravailler ce texte 18 à 24 mois après. Notre commission pourrait prendre l'initiative sur le sujet.

**M. Christian Cambon, président. –** Tout à fait !

**M. Gilbert Roger. –** Je voudrais rappeler à nos rapporteurs le peu d'enthousiasme de nos opérateurs à installer la fibre dans toutes les communes de France. Or nous avons vu notre dépendance à ces installations.

*La commission autorise la publication du présent rapport d'information, adopté à l'unanimité.*

# LISTE DES PERSONNES AUDITIONNÉES

**M. Guillaume Poupard**, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI)

**M. Jérôme Nottin**, directeur général du GIP ACYMA

**M. Henri Verdier**, Ambassadeur du numérique, ministère de l'Europe et des Affaires étrangères