Présentation du rapport sur la cybersécurité durant la crise sanitaire

Mercredi 10 juin 2020

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 & cybermalveillance : l'autre guerre du Covid-19 »

Rachel Mazuir interviendra sur les deux derniers 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 notre parlement.

Suite à la communication de notre rapport, des représentants religieux nous ont également alerté sur les désinformations qui les ont atteints.

Pour information, le régime communiste chinois ne s'en prend pas aux seuls Ouigours musulmans. Il fermé l'année dernière plus de 5500 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 donc recommandé la mise en place d'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 de respecter les 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.

Je transmets la parole à mon collègue Rachel Mazuir.

Je souhaite rendre hommage à notre administrateur Jean-Marc Virieux, qui fait valoir ses droits à la retraite.
Je regretterai la rigueur de son travail et ses multiples qualités.

Présentation du rapport sur la cybersécurité durant la crise sanitaire
Mercredi 10 juin 2020

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.

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, 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) avec des conséquences sur la gestion de la crise (remontées des informations vers Santé publique France, services funéraires…).

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 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, déjà 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.