ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

# Compte rendu

## Commission de la défense nationale et des forces armées

— Audition, à huis clos, de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Mercredi
27 mai 2020
Séance de 9 heures

Compte rendu n° 54

SESSION ORDINAIRE DE **2019-2020**

**Présidence de Mme Françoise Dumas,** *présidente*

ASSEMBLÉE NATIONALE

*La séance est ouverte à neuf heures.*

**Mme la présidente Françoise Dumas**. Un grand merci, Guillaume Poupard, pour votre présence aujourd'hui avec nous. Vous êtes directeur général de l'Agence nationale de la sécurité des systèmes d'information, une agence créée en 2009 et rattaché à la secrétaire générale de la défense et de la sécurité nationale. Le rôle de cette agence, si je vous ai bien lu car je vous cite, est « *de faciliter une prise en compte coordonnée, ambitieuse et volontariste des questions de cybersécurité en France* ».

Votre audition s'imposait naturellement au regard de la crise que nous traversons aujourd'hui. Celle-ci est bien sûr sanitaire, et par contrecoup économique et sociale, mais elle comporte également une autre dimension, moins évidente, moins médiatisée, mais tout aussi essentielle à prendre en compte : la dimension cyber.

Cette crise a en effet accru l'exposition de nos concitoyens aux cyberattaques. Elle renforce le risque sur les systèmes d'information de nos établissements de santé, de nos collectivités territoriales ou encore de nos entreprises, notamment à l'aune du recours massif et rapide au télétravail.

C'est dans ce contexte inédit que notre commission a souhaité vous entendre, tout en ayant conscience que le format de cette audition par visioconférence rend le présent exercice délicat, y compris en termes de cybersécurité.

Nous attendons de vous, M. le directeur général, que vous nous dressiez un panorama de l'état de la menace cyber et de son évolution sur les particuliers et sur les entreprises depuis le début de la crise.

Nous sommes intéressés à avoir des renseignements plus précis sur les établissements de santé qui étaient déjà des cibles privilégiées des cyberattaquants avant la crise. En témoigne par exemple la cyberattaque qui a frappé le CHU de Rouen en novembre 2019 et que vous avez décrite dans votre récent rapport sur l'état de la menace rançongiciel, un terme que j'ai appris grâce à vos travaux et qui désigne l'utilisation d'un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent. Ce type d'attaque a été lancé il y a peu à l'encontre de l'établissement de santé de Lomagne, dans le Gers. Estimez-vous, M. le directeur général, que nos établissements de santé investissent suffisamment pour assurer leur sécurité informatique et les considérez-vous suffisamment armés pour répondre seuls aux cyberattaques dont ils sont la cible ?

J'en profite pour saluer l'action de l'ANSSI en faveur des collectivités territoriales également de plus en plus touchées par les cyberattaques. Et je signale le guide sur leur sécurité numérique que vous avez publié en mars dernier.

Nous aimerions également vous entendre sur le risque d'accroissement du cyberespionnage en cette période de crise. Alors que les acteurs profitant de l'actualité pour mener leurs attaques étaient initialement des cybercriminels isolés, il semblerait que l'on ait affaire de plus en plus à des groupes parrainés par des États qui mènent leurs campagnes d'espionnage en direction des institutions publiques mais également de nos entreprises stratégiques et de notre base industrielle et technologique de défense. De plus, les instituts de recherche et les laboratoires universitaires font également l'objet de ces opérations de

cyberespionnage dans le cadre de la recherche mondiale d'un vaccin contre le COVID-19, comme le FBI en a récemment accusé la Chine. Estimez-vous cette menace sérieuse et quelles seraient vos préconisations pour s'en prémunir plus efficacement ?

Nous savons par ailleurs que l'ANSSI travaille en étroite collaboration avec plusieurs services, auxquels elle a pu apporter son expertise dans le cadre de cette crise, comme ce fut le cas auprès de l'Institut national de recherche en sciences et technologies du numérique pour l'application StopCovid. Pourriez-vous évoquer avec nous cette coopération spécifique, et plus généralement les coopérations qui sont les vôtres avec d'autres organismes.

Enfin, vous pourriez nous dire un mot sur l'évolution organisationnelle de l'ANSSI ainsi qu'à ses méthodes de travail. En particulier, quels sont les enjeux et les conséquences pour l'ANSSI de la récente réforme qui aboutira à la création au 1er juillet 2020 de l'Opérateur des systèmes d'information interministériels classifiés, à partir de la fusion de la sous-direction numérique de l'ANSSI avec le centre de transmissions gouvernemental ?

**M. Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information.** Le numérique innerve l'ensemble de notre société et des attaquants de nature très différente tentent d'en tirer parti. Ainsi, de nombreux petits criminels profitent de la crise pour escroquer nos concitoyens, profitant du fait que beaucoup utilisent désormais des outils numériques. Le nombre des mails malveillants et des escroqueries sur le thème de la crise sanitaire a explosé. La lutte contre cette petite criminalité sans effet majeur sur la sécurité nationale passe par la prévention et la pédagogie en direction du grand public. C'est le rôle du groupement d'intérêt public ACYMA, qui développe la plateforme cybermalveillance.gouv.fr sur laquelle figurent des conseils élémentaires mais indispensables ainsi qu'un moyen d'accéder facilement à tout un écosystème de prestataires privés à même d'aider les victimes.

Les rançongiciels, ou ransomwares, nous préoccupent davantage. Pour arnaquer de grandes structures ou de grandes entreprises disposant de moyens importants, des groupes cybercriminels très organisés pénètrent les réseaux de leurs victimes, chiffrent des données pour les rendre inaccessibles afin d'exiger des rançons dont le montant va croissant et se chiffre parfois en millions d'euros. Difficiles à appréhender, la parade face à ces attaques consiste essentiellement à élever des protections pour éviter qu'ils atteignent le cœur des réseaux. Une nouvelle tendance, particulièrement originale et préoccupante, voient ces groupes, ne pas se contenter de bloquer l'accès aux données mais également les voler pour menacer de les publier et ainsi faire chanter leurs victimes.

Ainsi, depuis le début de l'année, nous collaborons avec Bouygues Construction qui a été victime d'une telle attaque. Plus tôt, en novembre 2019, le CHU de Rouen a également été touché par une cyberattaque par rançongiciel, obligeant les personnels soignants à travailler plusieurs jours sans aucun outil numérique. Cela montre que les établissements de santé, aujourd'hui fortement numérisés avec des moyens bureautiques mais également équipements professionnels tels que du matériel d'imagerie et d'analyse biomédicales, peuvent être la cible d'attaquants sans aucune éthique. Enfin, les collectivités locales sont également des victimes de choix : la communauté de communes de Marseille a par exemple été touchée la veille du premier tour des élections municipales, entraînant le dysfonctionnement de nombreuses applications. Seul le travail formidable du personnel a permis la tenue du scrutin dans des conditions normales.

Contrairement à nos craintes, de telles attaques ne se sont pas multipliées pendant la crise. Les petits attaquants ont continué leurs actions – le site de Lomagne a par exemple été touché comme vous le rappeliez – mais aucune vague massive sur les CHU n'a été observée. Étonnamment, certains des cyberattaquants les plus connus ont publié un communiqué indiquant qu'ils ne s'en prendraient plus aux établissements hospitaliers durant la crise sanitaire, et ils s'y sont tenus.

D'autres attaques sont lancées par des États ou des groupes dont on soupçonne qu'ils sont liés à des États. Il n'est pas absurde d'imaginer aujourd'hui que ce type d'attaques vise notamment un sujet aussi stratégique que la recherche mondiale sur le vaccin ainsi que l'organisation des États pour assurer la continuité des fonctions critiques. Les industries pharmaceutiques et les instituts de recherche sont des cibles de choix pour les grands services de renseignement. Il est important de se rappeler que nous n'avons pas d'amis dans ce domaine et que nous pouvons donc être ciblés par nos alliés comme par nos ennemis.

Nous sommes également très attentifs aux attaques numériques visant le fonctionnement physique de systèmes à des fins de sabotage mais, depuis le début de la crise, leur nombre a plutôt décru. Les instigateurs ont-ils autre chose à faire ou se sont-ils rabattus vers des opérations d'espionnage, l'heure n'étant pas à la provocation diplomatique ? Il est trop tôt pour le dire.

Le développement du télétravail par des outils non maîtrisés a par ailleurs généré de nouveaux risques majeurs. Les outils de visioconférence non européens tels que Zoom par exemple, peu sécurisés et régis par des réglementations non-européennes comme le Cloud Act, sont inadaptés aux échanges sensibles. La crise aura eu pour effet de forcer de nombreux collaborateurs à travailler à distance avec des outils plus ou moins adaptés. Il est encore trop tôt pour tirer totalement les enseignements de cette crise mais il est déjà certain qu'il ne faudra pas attendre la prochaine pour développer des outils d'un niveau de sécurité raisonnable et relevant du seul droit européen.

Dans son rôle d'autorité nationale de sécurité des systèmes d'information, l'ANSSI s'est intéressée à la cybersécurité de tous les projets relatifs à la gestion de la crise sanitaire. INRIA s'est vu confier le développement de l'application StopCovid. J'ai déjà indiqué devant l'office parlementaire d'évaluation des choix scientifiques et technologiques que le développement de ce genre d'outil, lié à une situation de crise, devait être opéré avec sérieux et esprit de responsabilité. Dévoyée par l'État ou par des attaquants, une telle application pourrait avoir des conséquences dramatiques.

La coopération avec INRIA et plusieurs industriels rassemblés dans un consortium a été exemplaire. Les recommandations en matière de sécurité issues de la Commission nationale de l'informatique et des libertés (CNIL) et du Conseil national du numérique ont été suivies par les développeurs avec soin. Confier le pilotage du projet StopCovid à l'institut qui compte les meilleurs experts français en matière de sécurité et de protection de la vie privée était rassurant. Le lancement de l'application est sur le point d'être débattu par l'Assemblée nationale et le Sénat. Un tel dispositif, s'il fait sens, doit rester exceptionnel, transparent et très encadré.

Notons par ailleurs que des acteurs privés sont tentés de faire ce travail à la place de l'État. Nous avons eu d'intéressants débats avec Apple et Google pour définir le rôle de

chacun. Ces géants du numérique, engagés dans un développement commercial à tout-va, cherchent bien naturellement à pousser leur avantage. À l'État de dire que ce sujet régalien ne concerne pas les acteurs privés. S'il ne s'y oppose pas, les géants développeront encore leurs compétences et leurs services dans le domaine de la santé, avec des intérêts divergents par rapport au modèle défendu par l'État. D'autres projets sécuritaires plus lourds, tels que les systèmes non anonymes de gestion de l'épidémie et des malades, qui collectent les résultats des tests et outillent les brigades d'enquêtes sanitaires nous ont également occupés. Faute de sécurisation adéquate, des attaquants chercheront immanquablement à voler ces données médicales de valeur. En 2018, Singapour a ainsi été victime d'une telle attaque. Les données de santé d'une majorité de la population singapourienne ont été dérobées. Cela a également eu un impact politique puisque le premier dossier médical dérobé était celui du Premier ministre. Un autre exemple similaire est celui de la Norvège où les données de santé de la moitié de la population ont également été volées.

Des questions de souveraineté interviennent dans notre capacité à gérer des données et à organiser la crise. C'est pourquoi l'État et des industriels français ou européens coopèrent actuellement en vue de développer des systèmes capables de traiter massivement des données sans recourir à des industriels américains comme Palantir. Nous avons montré que nous savions développer des technologies souveraines, maîtrisées, de confiance, avec des acteurs industriels accoutumés à travailler avec le ministère des armées et la direction générale de l'armement (DGA), acteurs auxquels seul s'applique le droit français et européen.

Au 1er juillet sera créé l'opérateur des systèmes d'information interministériels classifiés (OSIIC), issu de la fusion de la sous-direction numérique de l'ANSSI, qui développe des systèmes très sécurisés au profit de l'administration et des plus hautes autorités de l'État, avec le centre de transmissions gouvernemental, en charge des communications des plus hautes autorités. Cette évolution très positive permettra à cet opérateur de se concentrer en tous lieux et en tout temps sur la sécurité des outils et sur l'aspect opérationnel des communications les plus sensibles de nos autorités, et à l'ANSSI de se concentrer sur les questions de cybersécurité et de cyberdéfense tout en préservant une forte proximité entre les deux entités.

Malgré la baisse d'effectifs immédiate liée à cette fusion, la croissance de l'ANSSI reste ambitieuse. Elle est ainsi passée de 100 personnels lors de sa création, il y a dix ans, à 600. Les gouvernements successifs ont permis à l'ANSSI de croître afin de développer un dispositif de cybersécurité robuste et performant en coopération avec les différents partenaires nationaux. Nous avons formalisé une coopération étroite avec les grands services de l'État qui font du cyber. Sous la présidence de la secrétaire générale de la défense et de la sécurité nationale, le centre de coordination des crises cyber, dit C4, se réunit tous les mois pour traiter d'enjeux cyber avec les ministères concernés. Le sujet est également régulièrement traité en conseil de défense et de sécurité nationale afin d'effectuer les principaux arbitrages en matière de stratégie et de doctrine et ainsi permettre la bonne coordination des actions des services de l'État dans ce domaine. L'ANSSI, dont l'action est purement défensive, joue pleinement un rôle de coordination interministérielle. Bien qu'armés face à ces menaces croissantes, nous restons toujours modestes sachant que, dans ce domaine, l'avantage reste à l'attaque.

**Mme Patricia Mirallès**. Les enjeux de cyberdéfense revêtent une dimension économique évidente. La lutte contre la cybercriminalité touche de près à l'espionnage

industriel. Les législations étrangères entravent-elles parfois votre action ? Si oui, comment y remédier ?

**M. Charles de La Verpillière**. La crise nous a fait prendre conscience de l'engagement d'une « guerre froide » entre la Chine, la Russie et les États-Unis. Dans ce contexte, la sécurité des systèmes informatiques est cruciale, non seulement pour les outils numériques mais aussi à l'égard des infrastructures. La question de l'intervention de Huawei dans les réseaux est-elle tranchée ?

**M. Fabien Lainé**. L'Assemblée nationale a rapidement répondu au besoin d'assurer les auditions grâce aux outils numériques. Pour tenir ses réunions à huis clos, notre commission ne peut recourir à l'application Zoom qui ne garantit pas la protection des données et la solution Orange fonctionne avec du matériel Huawei. Quels dispositifs sont de nature à assurer une communication sécurisée entre le Parlement et l'exécutif ? Une harmonisation des systèmes de communication numérique entre l'ensemble des ministères serait-elle pertinente ?

**M. Jean-Christophe Lagarde**. Vous l'avez dit, dans le domaine de l'espionnage, nous n'avons pas d'amis. La dépendance de la France à de nombreuses technologies extérieures comme celle de Huawei représente-t-elle une menace pour la sécurité de nos réseaux ? À l'Assemblée nationale, les 577 députés doivent pouvoir discuter et voter au moyen d'une technologie souveraine, sans risque de piratage. Cet objectif est-il techniquement réaliste ?

**M. Guillaume Poupard**. L'industrie de défense a été la première ciblée par les attaques, il y a dix ans. L'industrie de l'armement, l'industrie spatiale, la BITD sont ciblées par de l'espionnage de haut niveau. Depuis dix ans, nous collaborons avec nos industriels et les services du ministère des armées en charge de la sécurité industrielle afin de les protéger efficacement. L'avantage revenant souvent aux attaquants, la lutte doit être renouvelée sans cesse. Le cas d'Airbus montre ainsi la nécessité de sécuriser l'ensemble de l'écosystème. Depuis longtemps, les industriels ne travaillent plus seuls mais avec un écosystème très dense et varié de PME, de grands groupes, voire des acteurs étrangers. Les attaquants ne s'y trompent pas et ils commencent par s'en prendre aux sous-traitants pour remonter au cœur des réseaux de leur cible par le biais d'accès légitimes. Dès 2013, la France a été le premier pays au monde à adopter une réglementation stricte sur la sécurité des opérateurs d'importance vitale. Cela nous permet d'imposer une prise en compte complète de la cybersécurité dans l'industrie de l'armement et dans nombre d'autres secteurs comme l'énergie, les transports ou les télécoms, jugés critiques pour la sécurité nationale.

Certains de ces groupes, ni français ni européens mais mondiaux, doivent gérer des réglementations différentes d'un pays à l'autre. Nous sommes intervenus auprès de la Commission européenne pour que l'esprit des règles applicables en France soit érigé en principe européen. C'est l'esprit de la directive NIS (Network and Information System Security) relative à la sécurité des réseaux, fortement inspirée par l'Allemagne et la France. Au-delà de l'Europe, nous invitons les grands industriels à recloisonner les réseaux, car si le même réseau « à plat » est déployé dans le monde entier, y compris dans des pays à risque, il est impossible d'en protéger le cœur.

Bien que non déclarée, la guerre cyber, froide ou chaude, est forte entre ennemis et alliés. Dans ce contexte, deux cercles se dessinent, le premier englobant les nations capables d'assurer leur souveraineté numérique, c'est-à-dire les États-Unis, la Chine, la Russie et Israël, et un second avec les pays en quête de protection par le biais de l'OTAN ou d'autres alliances. Ainsi que dans d'autres domaines de défense comme la dissuasion – et on notera que les pays cités sont également des puissances nucléaires – nous avons les moyens d'appartenir au premier cercle. L'enjeu pour la France est de jouer dans le cercle des grands, grâce à une volonté politique constante de souveraineté prenant appui sur une base industrielle forte. Nous nous employons avec les États membres de l'UE intéressés et la Commission européenne à combiner une souveraineté nationale avec une autonomie stratégique européenne.

S'agissant des infrastructures, certains équipementiers et acteurs non européens – vous avez cité Huawei – sont plus à risque que d'autres. Au regard de l'exigence de souveraineté, une loi vise à contrôler le déploiement des équipements au sein des réseaux 5G. L'État doit avoir son mot à dire sur le déploiement de ce type d'équipement. L'enjeu est de permettre le développement des réseaux 5G dans des conditions économiques acceptables pour les opérateurs, sans renoncer à notre souveraineté ni à la sécurité à long terme des réseaux. Cela concerne toutes les infrastructures numériques comme les *datacenters* ou encore les câbles. Nous ne pourrons être souverains sans une certaine maîtrise de ces infrastructures.

L'expérience militaire a montré que la souveraineté technologique ne consiste pas à faire tout nous-mêmes – la DGA ne réalise pas des systèmes d'armes composés exclusivement de composants français – mais à concevoir une architecture sûre et maîtrisée, puis à distinguer, parmi les différentes briques élémentaires, celles qui doivent être développées en confiance par la BITD et celles acquises sur étagère. La difficulté, c'est de réaliser l'architecture ménageant une maîtrise suffisante. Dans le domaine des télécoms, la question est de savoir ce que nous devons maîtriser et ce que nous pouvons acheter, y compris à Huawei.

Force est de reconnaître que nous n'étions pas prêts à répondre au besoin de visioconférence révélé par la crise. Des solutions qui fonctionnent ne sont pas sûres, d'autres garantissant la sécurité manquent de fonctionnalité, mais je suis convaincu qu'il est possible, même si cela a nécessairement un coût, de développer des outils à la fois maîtrisés et fonctionnels. Pour les plus hautes autorités de l'État, nous avons développé depuis plusieurs années un réseau de visioconférence sécurisé au niveau confidentiel défense qui s'est avéré bien utile et grâce auquel des conseils de défense et des conseils des ministres se sont tenus. Il serait certainement possible d'organiser des auditions à huis clos sécurisées à l'Assemblée nationale, mais cela exigera une volonté et des moyens. Si elle est sollicitée, l'ANSSI aidera volontiers à garantir la sécurité d'un tel système.

Nous ne sommes pas capables de tout faire, mais nous sommes capables de progresser sur la ligne de crête qui doit nous permettre de nous maintenir dans le premier cercle des pays souverains. Mais pour cela il faut renoncer aux solutions internationales faciles d'emploi et d'accès, et souvent moins coûteuses, au moins au début… Si, lors de la construction de la dissuasion, on avait choisi le meilleur rapport qualité/prix à court terme, nous n'aurions certainement pas développé toutes les industries dont nous bénéficions aujourd'hui.

**M. Joaquim Pueyo**. Plusieurs pays européens envisagent le développement de la technologie pour suivre et prévenir les malades. La France veut une application sans GAFAM, tandis que l'Allemagne travaille avec ces entreprises et la Commission européenne dialogue avec elles. L'impossibilité de relier ces systèmes ne risque-t-elle pas de porter atteinte à la stratégie française ?

**M. Alexis Corbière**. À quel niveau évaluez-vous le risque de fuite de données, inhérent à tout dispositif numérique, pour l'application StopCovid ?

Le 10 mai, le port iranien de Bandar Abbas a subi une cyberattaque. Les bâtiments militaires français ont-ils essuyé ce type d'offensive dans les derniers mois ?

**M. Pierre Venteau**. En janvier 2020, l'ANSSI a publié un guide de la réglementation de la sécurité numérique à destination des collectivités territoriales. Toutefois, à en croire un sondage, le risque cyber reste mal compris et sous-estimé par deux tiers des personnels des collectivités territoriales. Un partenariat en vue d'assurer la formation de nos fonctionnaires territoriaux aux enjeux de la cybersécurité et d'améliorer notre culture du risque numérique est-il envisageable ?

**M. Thibault Bazin**. En 2018, une mission d'information sur la cyberdéfense relevait l'insuffisance de cyber-conscience de nos concitoyens, le besoin de produits antivirus et antimalware souverains et d'un cloud sous juridiction française. Dispose-t-on des moyens nécessaires pour développer des solutions entièrement françaises ? Sommes-nous montés en puissance en matière de cyber-offensive et de cyber-riposte afin d'aveugler nos adversaires sur les théâtres d'opérations ? A-t-on recruté les talents espérés ? Sommes-nous attaqués plutôt par des Français ou par des étrangers, plutôt par des États ou par des organisations non étatiques voire économiques ?

**M. Christophe Lejeune**. Durant le confinement, l'ANSSI a-t-elle été en capacité d'instaurer le télétravail pour ses collaborateurs, en garantissant une communication stable, fine et à l'abri de malveillance ? Si oui, pourriez-vous nous en faire profiter ?

**Mme Monica Michel**. Les cybercriminels ont profité de la crise pour augmenter leur activité en direction des collectivités territoriales, encouragés par le millefeuille territorial qui complique la sécurisation et par le manque de moyens des petites structures. Consciente de cette vulnérabilité, l'ANSSI a mis en place des délégués régionaux. Les élus et fonctionnaires territoriaux ont-ils pris en main les instruments de protection mis à leur disposition par les services de l'État ?

**M. Nicolas Meizonnet**. Nous avons parlé des risques d'ingérence de la Chine au travers du déploiement de la 5G. Afin de garantir l'autonomie stratégique européenne du numérique, quelles contraintes pouvons-nous imposer à un équipementier comme Huawei ?

**M. Stéphane Baudu**. Lors de la dernière édition du forum international de la cybersécurité, vous avez appelé au développement d'une souveraineté européenne. L'Union européenne s'est emparée du sujet en créant l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Dans le cadre de la collaboration avec cette institution, observez-vous depuis la crise sanitaire une prise de conscience des pays européens pour réduire leur vulnérabilité partagée ? Quels leviers envisagez-vous d'activer pour stimuler les ambitions européennes ?

**Mme Sereine Mauborgne**. Nombre de salariés travaillant encore de chez eux à l'aide d'appareils peu sécurisés, des observateurs s'inquiètent de leur grande vulnérabilité lors du retour dans les entreprises. Comment mieux assurer la sécurité informatique du télétravail ?

**M. Jacques Marilossian**. L'ANSSI a édité des recommandations relatives au nomadisme numérique. Depuis la crise du covid, le développement du télétravail a accru les risques de cyberattaques et la saturation des accès sécurisés. Des entreprises de la BITD ont-elles été victimes de telles attaques ? Quelles sont vos recommandations pour ces entreprises dans le cadre du nomadisme numérique ?

**M. Guillaume Poupard**. L'application StopCovid pourrait faire craindre un risque de dérive vers une surveillance de masse, alors qu'il s'agit d'une application minimaliste, pseudonymisée, qui ne traite que les données strictement nécessaires. Dans le même temps, il ne faudrait pas que certains puissent reconstituer les réseaux d'interaction sociale, afin de savoir qui croise qui et d'obtenir des données relevant de la vie privée. L'objet du développement du protocole et de son implémentation était de minimiser la surface d'attaque et d'en garantir la sécurité. Les points de fragilité au sein de l'architecture ont été réduits et des audits ont été réalisés. Le fonctionnement de l'application et du système est ouvert et publié par INRIA. Nous lançons un « *bug bounty* », c'est-à-dire que nous demandons à la communauté des hackers d'éprouver par eux-mêmes le niveau de sécurité. En suivant les recommandations de l'ANSSI, de la CNIL et des experts, tout aura été fait pour minimiser les risques et maximiser l'intérêt de l'usage de cette application. Cela étant, le traçage des contacts ne doit pas devenir une activité normale hors temps de crise.

Il n'y a pas eu de front européen pour une stratégie unique. Les discussions ont été sabotées par certains pour empêcher une entente des États membres. Après avoir envisagé un modèle similaire au nôtre, l'Allemagne a changé d'avis et je n'exclus pas qu'elle change de nouveau. La stratégie de la France n'exclut pas les GAFAM, puisque cette application fonctionne grâce à des systèmes d'exploitation Apple et Google (Android). En revanche, la France a fait le choix résolu de ne pas confier aux GAFAM la santé de ses concitoyens. Nous ne devons pas nous décharger sur ces entreprises privées américaines des responsabilités régaliennes de la santé publique, du suivi épidémiologique ou de choix stratégiques pour la gestion de la crise sanitaire. Force est de constater que l'absence de coordination européenne empêchera de fait l'échange de données, les systèmes étant incompatibles.

StopCovid, médiatiquement visible, ne doit pas être l'arbre qui cache la forêt des systèmes plus critiques par nature non anonymisables et contenant un très grand nombre d'informations. Il est indispensable d'assurer la sécurisation de ces bases de données de santé vis à vis d'un attaquant de haut niveau, leur valeur étant bien plus élevée que les rares données traitées par l'application StopCovid.

L'attaque dans le détroit d'Ormuz est une mesure de rétorsion d'un pays de la région en réponse à une attaque par un autre pays du Moyen Orient. Au-delà de l'espionnage omniprésent, cette région particulièrement active dans le domaine cyber est depuis des années le lieu de cyberattaques parmi les plus violentes. Toutefois la géographie du cyberespace ne se confond pas nécessairement avec la géographie physique et un navire français doté de systèmes indépendants ne peut être contaminé uniquement du fait de sa présence dans la zone.

Le haut niveau de sécurité de nos systèmes d'armes est une priorité du ministère des armées et de la DGA. Les militaires ont été les premiers en France à prendre en compte cette menace et ils se sont rapidement structurés pour y faire face. La BITD traite également le sujet depuis une dizaine d'années et les grands industriels de l'armement progressent sans cesse sur le cyber.

Je dois bien avouer que je ne suis pas serein pour la sécurité des collectivités territoriales. Ce que nous avons vécu à Marseille montre que les collectivités sont des cibles critiques. Les atteintes portées à ces collectivités peuvent avoir de graves conséquences sur la vie quotidienne ou la sécurité des citoyens. Si nous savons traiter les grandes entreprises, nous savons beaucoup moins le faire pour les PME, ce que beaucoup de collectivités sont du point de vue informatique. Nous devrons y réfléchir avec le ministère de la cohésion des territoires.

Parmi les pistes d'amélioration, je suis par exemple étonné de voir chacun développer de son côté des outils sécurisés destinés à répondre à des besoins identiques. La concentration du développement de ces outils bénéficierait à tout le monde.

Depuis plus d'un an, un conseil de défense a donné priorité à la cybersécurité des hôpitaux. L'attaque contre le CHU de Rouen a conforté cette orientation. Il s'agit de sensibiliser, de déployer des moyens et d'homogénéiser les solutions.

Depuis 2018, la prise de conscience cyber a progressé, mais cela reste encore insuffisant. Le sujet est cependant pris au sérieux par les décideurs. Je l'observe de plus en plus lors de mes rencontres avec les comités exécutifs de grandes entreprises françaises où des acteurs majeurs comme les PDG, les directeurs juridiques et financiers, de nombreux responsables dont le métier n'est a priori pas le cyber, ont manifestement compris l'importance de ce sujet pour leur entreprise.

Le développement d'une conscience collective reste d'actualité. Depuis un an, une coopération étroite est établie avec l'Éducation nationale et dès la rentrée prochaine une initiation à la sécurité numérique sera dispensée au lycée.

Nous n'avons toujours pas d'antivirus souverain pour le grand public, mais un progrès a été réalisé dans le domaine du cloud. Nous ne sommes pas condamnés à utiliser des solutions américaines ou chinoises. Des sociétés comme OVH ou Outscale conçoivent des solutions robustes et sûres. La question de savoir comment amener de solutions telles qu'Office 365 sur des clouds maîtrisés fait l'objet de discussions avec Bercy.

La lutte informatique active ne relève pas des attributions de l'ANSSI, le modèle français séparant clairement l'attaque et la défense. J'ai le sentiment toutefois que les moyens sont là et que cette capacité progresse.

Les ressources humaines restent la priorité. La richesse cyber repose intégralement sur les femmes et les hommes. Nous recrutons à un très bon niveau, mais l'écart entre les besoins et le nombre de personnes capables de les remplir continue à se creuser. Afin de faire travailler ensemble public et privé et de tirer le maximum des expertises de chacun, un campus cyber sera lancé en 2021 en région parisienne.

Tout le monde nous attaque. Les petits attaquants prennent de gros risques et la justice n'a plus aucune mansuétude pour ce genre de crime. Le crime organisé opère dans des zones

de non-droit où les attaquants sont très mobiles. Des États continuent à nous attaquer, et j'ai l'intuition que les grands États vont chercher à empêcher les petits à développer leurs capacités cyber, d'où l'intérêt d'être dans le premier cercle.

L'ANSSI a réussi à sécuriser ses flux et à faire du télétravail, parce que nos agents sont équipés de produits conçus par des informaticiens pour des informaticiens. Toutefois, pour l'activité classifiée, les agents sont venus travailler sur place. Cette solution dégradée est difficilement reproductible pour d'autres entités comme l'Assemblée mais certains outils peuvent ponctuellement bénéficier à d'autres entités.

Les petites attaques contre l'AP-HP n'ont pas eu d'effet opérationnel, mais ont révélé un besoin majeur de moyens pour hisser les différentes structures au juste niveau de sécurité, car l'investissement en matière de cybersécurité est souvent insuffisant.

On ne doit pas opposer souveraineté européenne et souveraineté nationale, qui se complètent. C'est l'objet de discussions franches avec les autres États membres et la Commission européenne. Nous avons besoin de l'Europe pour avoir une cybersécurité efficace et l'Europe a besoin notamment de la France et de l'Allemagne pour la développer à l'échelle européenne. Comme il n'est pas question de renoncer à notre souveraineté, nous insistons systématiquement sur la nécessité pour chaque État de développer ses capacités et pour l'ENISA de les faire travailler ensemble en réseau. Une volonté politique forte est indispensable à la construction d'une autonomie stratégique européenne.

L'ANSSI a identifié un risque de vulnérabilité lors du retour au travail. Beaucoup ont travaillé chez eux, dans le meilleur des cas avec des outils confiés par leur employeur, mais pour ceux qui ont utilisé leurs ordinateurs personnels, le risque est plus élevé. Cela pose la question du BYOD (« bring your own device ») : selon ce principe, pour faire des économies, les personnels sont invités à travailler avec leurs propres moyens informatiques. Comme il est impossible de protéger un réseau constitué d'une multitude d'équipements non maîtrisés, on peut craindre que des attaques ne passent par ces équipements pour atteindre le cœur des réseaux informatiques.

Nous faisons depuis longtemps de strictes recommandations sur le nomadisme, notamment pour éviter l'usage trop répandu d'équipements personnels. L'organisation du travail devra être repensée.

Quant aux attaques contre la BITD, je ne peux entrer dans le détail. Pendant la crise, les attaques aux fins de rançonnage et d'espionnage ont continué. Il ne faut jamais baisser la garde.

**Mme la présidente Françoise Dumas**. Merci pour la clarté et la richesse de vos propos. Vous avez évoqué la nécessité de l'homogénéité de la protection des équipements et d'une résilience commune au regard des inégalités d'acculturation. Nous entendons diffuser les initiatives en ce sens, être des transmetteurs d'alerte et des vecteurs de sensibilisation dans nos territoires. Nous serons à vos côtés pour poursuivre la protection de notre République et le chantier de l'autonomie stratégique européenne.

*

* *

*La séance est levée à dix heures cinquante.*

*

* *

**Membres présents ou excusés**

*Présents.* - M. Xavier Batut, M. Stéphane Baudu, M. Thibault Bazin, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. Philippe Chalumeau, M. Alexis Corbière, Mme Marianne Dubois, Mme Françoise Dumas, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Claude de Ganay, Mme Séverine Gipson, M. Fabien Gouttefarde, M. Jean-Michel Jacques, M. Loïc Kervran, Mme Anissa Khedher, M. Jean-Christophe Lagarde, M. Fabien Lainé, M. Jean-Charles Larsonneur, M. Didier Le Gac, M. Christophe Lejeune, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Nicolas Meizonnet, Mme Monica Michel, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Florence Morlighem, M. Jean-François Parigi, Mme Josy Poueyto, Mme Natalia Pouzyreff, M. Joaquim Pueyo, M. Gwendal Rouillard, M. Jean-Louis Thiériot, Mme Sabine Thillaye, M. Pierre Venteau, M. Patrice Verchère, M. Charles de la Verpillière

*Excusés.* - M. Sylvain Brial, M. Olivier Faure, M. Yannick Favennec Becot, M. Richard Ferrand, M. Stanislas Guerini, M. Christian Jacob, Mme Manuéla Kéclard-Mondésir, M. Gilles Le Gendre, Mme Laurence Trastour-Isnart