Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2021-03 DU 29 AVRIL 2021

PORTANT RECOMMANDATIONS

DANS LE DOMAINE DE LA SECURITE NUMERIQUE

Les attaques dans l'espace numérique se sont multipliées à un rythme quasi-exponentiel ces deux dernières années, partout dans le monde. Tous les experts auditionnés par notre Commission nous ont fait part de leurs inquiétudes. Ils ont confirmé que la situation sécuritaire dans l'espace numérique est désormais particulièrement préoccupante et qu'elle devrait continuer à se dégrader dans les années qui viennent. La capacité des cybercriminels à commettre leurs forfaits s'est professionnalisée, mondialisée et industrialisée, et croît plus rapidement que celle de leurs victimes à se protéger. Les principales puissances numériques elles-mêmes, à commencer par les Etats-Unis, la Chine et la Russie, sont au bord du cyber-affrontement. A ce rythme, si la France et l'Europe ne prennent pas rapidement la mesure du défi sécuritaire auquel nous sommes collectivement confrontés, et n'adoptent pas des mesures vigoureuses permettant de changer les paradigmes de la sécurité dans l'espace numérique, nos Etats, notre économie, nos concitoyens, le fonctionnement même de nos démocraties pourraient être confrontés au chaos numérique à l'horizon de la prochaine décennie. Cette sombre perspective n'est hélas pas qu'une simple hypothèse ou une vue de l'esprit, mais un scénario plausible qui prolonge le caractère exponentiel de la croissance des cybermenaces observée au cours de ces dernières années.

La stratégie nationale pour la cybersécurité, présentée par le Président de la République le 18 février dernier, et pilotée par le Secrétaire d'Etat chargé de la Transition numérique et des communications électroniques, est un plan ambitieux. Elle apporte un certain nombre de réponses à des besoins identifiés en mobilisant des financements importants - 1 milliard d'euros dont 720 millions de financements publics – qui devraient permettre de réduire les vulnérabilités des systèmes informatiques de nombreuses infrastructures publiques et privées.

Pour autant, une stratégie nationale pour la sécurité dans l'espace numérique ne peut se limiter à un tel plan, aussi nécessaire soit-il. La cybersécurité ne constitue qu'un volet des mesures qui permettront, à terme, de renforcer le niveau global de la sécurité dans l'espace numérique dont l'Etat français, les services publics nationaux, les collectivités territoriales, les entreprises et nos concitoyens ont désormais une absolue nécessité. C'est en articulant l'ensemble de ces volets que l'Etat sera en mesure d'assurer l'ordre public et la sécurité des biens et des personnes dans l'espace numérique au même titre que dans l'espace physique. A cet égard, les mesures de renforcement des capacités de lutte contre la cybercriminalité apparaissent comme prioritaires.

Enfin, il est essentiel que la sécurité numérique soit mieux comprise par nos concitoyens. Ils doivent être instruits des menaces auxquelles ils peuvent être confrontés dans leurs usages du numérique, que ce soit dans leurs usages numériques du quotidien, en utilisant des objets connectés ou dans le cadre du télétravail qu'ils sont de plus en plus nombreux à pratiquer, et qui peuvent mettre en cause la protection de leurs données personnelles.

Au terme de ses auditions, la CSNP a souhaité émettre dans les meilleurs délais, compte tenu de la gravité d'une situation sécuritaire qui ne cesse de se dégrader dans l'espace numérique, un certain nombre de recommandations concrètes portant sur les cinq champs de progrès suivants que notre commission a identifié :

- Le renforcement de la lutte contre la cybercriminalité ;
- Les points d'amélioration du plan cyber ;
- La stratégie de cyberdéfense de l'Etat français ;
- La sécurité des produits et services numériques, et le développement du *cloud* de confiance ;
- La conduite des politiques publiques en faveur de la sécurité dans l'espace numérique.

I. Sur les moyens judiciaires et policiers pour combattre la cybercriminalité

La CSNP a bien noté que la stratégie nationale pour la cybersécurité n'aborde pas le volet du traitement policier et judiciaire de la cybercriminalité. Notre commission estime que ce champ de progrès doit faire l'objet d'une priorité gouvernementale dans un contexte de croissance quasi exponentielle de cette criminalité nouvelle.

- **Sur le volet judiciaire**

Les membres de la CSNP observent une véritable carence de l'Etat dans les moyens dédiés à la lutte contre la cybercriminalité. Aujourd'hui, trois magistrats seulement traitent les dossiers de cybercriminalité en France alors que le nombre d'attaques augmente à un rythme exponentiel depuis deux ans. La qualité et l'engagement de ces magistrats doivent être salués mais cet effectif est clairement insuffisant. Le décalage croissant entre la réalité de la criminalité dans l'espace numérique et les moyens dont dispose l'institution judiciaire pour traiter cette cyber-délinquance mondialisée et industrialisée, est un sujet de préoccupation majeur pour les parlementaires membres de notre Commission.

Recommandation n°1 : La CSNP engage le Gouvernement à étudier la création d'un parquet national cyber, disposant des ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber-délinquance les plus complexes.

Recommandation n°2 : La CSNP recommande au Gouvernement de consolider le dispositif des référents cybercriminalité, auprès de chaque Cour d'appel, en renforçant notamment leur formation à ces enjeux.

Recommandation n°3 : La CSNP recommande une formation spécifique des magistrats sur les enjeux du numérique, la sécurité dans l'espace numérique, et le traitement judiciaire de la cybercriminalité, dès leur formation initiale et au cœur des dispositifs de leur formation continue.

Recommandation n°4 : La CSNP recommande de renforcer la coopération judiciaire européenne et internationale et encourage une initiative française en vue de la création d'un véritable parquet européen spécialisé dans la cybercriminalité, dans la perspective de la Présidence française de l'Union européenne.

- **Sur le volet organisationnel de la police et de la gendarmerie nationale**

L'arrêté du 25 février 2021 portant création du commandement de la gendarmerie dans le cyberespace est une disposition nécessaire pour structurer l'action des forces de gendarmerie dans la lutte contre la cybercriminalité. Cependant, les membres de la CSNP estiment que le Ministère de l'Intérieur ne dispose pas des moyens suffisants, en nombre et en qualité, pour assurer le maintien de l'ordre public dans l'espace numérique, et pour lutter contre et enquêter sur la grande délinquance numérique. L'Etat doit pouvoir assurer la sécurité des citoyens et le maintien de l'ordre public dans l'espace numérique, y compris dans ses dimensions les moins régulés comme le *darkweb*.

Recommandation n°5 : La CSNP recommande un renforcement significatif des moyens des services d'enquête pour lutter contre la grande cyberdélinquance, dans le cadre d'un plan ambitieux d'adaptation des ressources relevant du Ministère de l'Intérieur à ces nouvelles formes de délinquance.

- **Sur l'adaptation du corpus législatif**

La CSNP n'appelle pas à l'adoption d'une nouvelle loi sur la cybersécurité mais propose des aménagements aux textes actuels en étendant les pouvoirs de l'ANSSI dans le cadre de la loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 du 13 juillet 2018.

La cybercriminalité est devenue une nouvelle forme d'atteinte aux intérêts vitaux de la nation, au même titre que le terrorisme. Il convient de s'interroger sur l'adaptation des mesures permettant de lever le secret des enquêtes judiciaires pour renforcer le champ d'action de l'ANSSI à l'instar des mesures qui ont été prises pour renforcer l'action de nos services de renseignement en matière de lutte contre le terrorisme.

Recommandation n°6 : La CSNP suggère :

- De modifier l'article 34 de la loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 du 13 juillet 2018 afin de d'étendre les capacités d'investigation technique de l'ANSSI aux contenus des équipements informatiques ;
- De permettre à la Justice de transmettre à l'ANSSI des informations couvertes par le secret de l'instruction mais utiles à l'accomplissement de ses missions.

- **Sur le paiement des rançons par les entreprises**

Environ 20% des entreprises subissant une attaque par rançongiciel paieraient la rançon qui leur est réclamée par les attaquants, souvent incitées à le faire par les sociétés d'assurance auprès desquelles elles ont souscrit une police d'assurance contre les cyber-risques. Cette situation n'est pas acceptable car elle entretient et renforce l'activité des cybercriminels, dont il est absolument indispensable de tarir les ressources.

Recommandation n°7 : La CSNP recommande au Gouvernement de développer un dispositif de régulation du paiement des rançons par les entreprises françaises, soit pour l'interdire, soit pour rendre obligatoire, sous le couvert d'une protection du type « secret des affaires », la déclaration aux autorités françaises, d'une demande de rançon et de son traitement.

II. Recommandations visant à renforcer et compléter les mesures annoncées dans le cadre de la stratégie nationale pour la cybersécurité

La CSNP reconnait l'ambition et la pertinence des mesures annoncées dans le cadre du plan d'accélération de la cybersécurité aux besoins identifiés de l'écosystème français (renforcer la filière française de la cybersécurité, en doublant les emplois passant de 37 000 à 75 000), destiné prioritairement à stimuler la recherche française en cybersécurité et l'innovation industrielle.

- **Sur le dispositif national de cybersécurité**

Un effort particulier a été porté sur les moyens budgétaires de l'ANSSI qui va bénéficier d'un budget de 136 millions d'euros sur 2021/2022 pour financer des projets structurants. De l'avis unanime des parties prenantes, l'ANSSI effectue un travail remarquable et remplit sa mission avec efficacité. L'Etat a su dégager des moyens pour permettre le recrutement de 600 experts en cybersécurité (contre 200 experts à sa création en 2009). L'Agence connait cependant un turn-over relativement élevé, et ses experts sont très recherchés sur un marché des compétences en cybersécurité particulièrement en tension.

Recommandation n°8 : La CSNP recommande au Gouvernement de mobiliser les moyens qui permettront à l'ANSSI de fidéliser ses agents en leur offrant des conditions plus attractives.

Initié par le Président de la République en 2019, le Campus Cyber a vocation à être, dès cette année, un lieu emblématique qui rassemblera les principaux acteurs du domaine de la cybersécurité afin de développer des synergies entre grands groupes, PME, startups, services de l'État, organismes de formation, acteurs de la recherche et associations. Le Campus Cyber a également pour mission de développer des partenariats avec des pôles de cybersécurité en région.

Par ailleurs, le plan d'accélération cyber prévoit le déploiement dans chaque région d'un CSIRT (*Computer Security Incident Response Team* - équipe de réponse aux incidents informatiques) incubé avec le soutien de l'ANSSI. Ces CSIRT doivent permettre de réagir plus rapidement et efficacement aux incidents cybers qui peuvent frapper les collectivités territoriales, les structures du tissu sanitaire (hôpitaux, cliniques) et les structures du tissu économique local.

Recommandation n°9 : La CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale. Elle recommande notamment la création dans chaque région d'un campus régional de la sécurité numérique capable de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques. Ce campus hébergerait le CSIRT incubé par l'ANSSI et serait notamment un véritable relais de gouvernance régional pour l'ANSSI, au service de tous les départements d'une même région pour un maillage territorial efficace. La création de ces campus régionaux pourrait s'appuyer sur l'article L4251-13 du Code général des collectivités territoriales portant nouvelle organisation territoriale de la République, et être inscrite dans les schémas régionaux de développement économique, d'innovation et d'internationalisation.

- **Sur la sensibilisation et la formation à la sécurité numérique**

Recommandation n°10 : La CSNP recommande aux pouvoirs publics de développer une politique massive d'information et de sensibilisation de la population sur les risques encourus dans l'espace numérique, tant à titre privé que professionnel, et sur les mesures et dispositions permettant de s'en prémunir.

La formation est la condition sine qua non de la mise en œuvre opérationnelle du plan d'accélération cyber en raison de la pénurie de compétences : 500 000 emplois déficitaires en Europe dans le numérique en général, notamment la cybersécurité, la science des données et l'intelligence artificielle, sont annoncés d'ici 2025 par la Commission européenne.

Le plan d'accélération cyber propose de renforcer la formation initiale et continue aux métiers de la cybersécurité, afin de résorber les déficits de compétences dans ce domaine en établissant un diagnostic des formations et des métiers existants pour répondre à la demande et aux enjeux de la cybersécurité de manière transversale. La sécurité numérique doit être plus systématiquement intégrée dans l'ensemble des formations pour changer le paradigme de la sécurité dans l'espace numérique. La sensibilisation à ces sujets doit s'effectuer dès le collège, grâce aux stages de troisième.

Recommandation n°11 : La CSNP recommande que des enseignements portant sur la sécurité numérique et la cybersécurité soient intégrés systématiquement et rapidement dans tous les cursus de formation aux métiers du numérique. Les principes de « sécurité par conception », « d'architecture sécurisée » et de « sécurité d'exploitation » doivent s'imposer dans les formations de tous niveaux aux métiers du numérique. Cette recommandation est formulée tant pour la formation initiale que pour la formation continue.

Recommandation n°12 : La CSNP recommande qu'un effort tout particulier soit engagé en faveur de la sensibilisation et la formation aux enjeux de la sécurité numérique et de la cybersécurité au profit des agents publics, notamment ceux qui sont employés dans les plus petites structures, particulièrement vulnérables.

Nous faisons le constat de la faible féminisation de ces métiers (à peine 15%) et particulièrement des métiers de la cybersécurité, dans lesquels les femmes représentent à peine 11% des effectifs, selon la plupart des études.

Recommandation n°13 : La CSNP suggère de renforcer de manière très substantielle les actions en faveur de la féminisation des métiers du secteur numérique. Dans un contexte de déficit de compétences, nous demandons que soit mis un terme à ce phénomène d'éviction croissante des femmes de ces métiers. A ce titre, nous appelons les pouvoirs publics à renforcer leurs soutiens à la fondation Femmes@Numérique présidée par notre collègue Christine Hennion, députée des Hauts de Seine, et membre de la CSNP, fondation qui œuvre en faveur de la féminisation des métiers du numérique.

- **Sur la consolidation de la filière cybersécurité**

Aujourd'hui la filière française de l'industrie de la cybersécurité est morcelée entre de nombreuses PME et quelques grands industriels très spécialisés. Elle ne propose pas dans son offre, contrairement à ses concurrents américains, de dispositifs de sécurité intégrés (firewall, antivirus, EDR etc.). Un des axes de renforcement de la filière pourrait passer par des objectifs de consolidation de ces dispositifs afin que l'offre française en matière de cybersécurité puisse proposer des offres intégrées plus facilement commercialisables auprès des acteurs de taille modeste ou intermédiaire. Le plan propose de structurer la filière et de repositionner la France par rapport à la concurrence internationale en nombre d'entreprises.

Recommandation n°14 : La CSNP recommande au Gouvernement de développer une politique industrielle active de consolidation de la filière industrielle française des produits et services de cybersécurité afin de favoriser la création d'entreprises *leader*s de la cybersécurité, disposant d'une taille critique de classe mondiale et capables de développer des gammes de produits de sécurité répondant aux attentes du marché mondial. Le contrat de la filière des industries de sécurité 2020 /2022 peut permettre à l'écosystème numérique français d'être moins compartimenté grâce à ses projets structurants sur la cybersécurité et le numérique de confiance, tout en s'ouvrant à la dimension européenne.

Recommandation n°15 : La CSNP recommande que l'Etat prenne une part plus active à la consolidation de la filière cybersécurité en mobilisant d'avantage le levier de la commande publique au niveau national et européen. Il convient par ailleurs d'étudier si la directive 2014/25/UE du 26 février 2014 relative à la commande publique des opérateurs de réseaux doit être modifiée, notamment pour permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens. A minima, il conviendrait de définir que la cybersécurité entre dans le champ d'exclusion de l'application de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance.

- **Sur les mesures incitatives pour renforcer les budgets sécurité numérique du secteur privé**

Le plan d'accélération cyber incite les entreprises à porter leurs investissements dans les produits et services de sécurité numérique à hauteur de 5 à 10% du montant de leur budget informatique.

Recommandation n°16 : La CSNP suggère d'accompagner le plan d'accélération cyber par des mesures d'incitation fiscale afin que les entreprises puissent dédier plus facilement et rapidement des moyens supplémentaires à leur budget cybersécurité. Cela peut prendre la forme de suramortissement des investissements en sécurité numérique ou d'un crédit d'impôt sur les dépenses et investissements engagés dans ce secteur auprès de fournisseurs nationaux et européens.

- **Sur le pilotage de la mise en œuvre du plan d'accélération cyber**

Le plan d'accélération cyber est inédit par son ambition et l'ampleur des ressources financières qui lui sont consacrées. Ce sont désormais la qualité de sa mise en œuvre et la rapidité de son exécution qui seront déterminantes, notamment parce que la dégradation de la situation actuelle appelle des mesures urgentes.

Recommandation n°17 : La CSNP attire l'attention du Gouvernement sur la nécessité de garantir la disponibilité des moyens humains et financiers dédiés à la mise en œuvre du plan d'accélération cyber, sous la direction de son coordinateur. L'exécution de ce plan d'accélération cyber nécessite un effort de gouvernance très substantiel, inscrit dans la durée.

Recommandation n°18 : La CSNP demande au Gouvernement de déterminer les indicateurs pertinents de pilotage de ce plan et d'établir un tableau de bord qui sera présenté semestriellement à notre Commission.

- **Sur l'identité numérique régalienne**

Dans un contexte de dématérialisation croissante de tous types de démarches, tant administratives que privées, l'accès aux ressources numériques devient un enjeu de sécurité pour l'ensemble de nos concitoyens. Plus de 200 000 Français par an sont victimes d'usurpation de leur identité dans l'espace numérique. L'identité numérique est la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources numériques. Le projet d'identité numérique porté par le programme France Identité Numérique vise à répondre à ce besoin. Après la mise en place de FranceConnect, en 2016, fédérateur d'identité, et l'expérimentation d'Alicem en 2019, le déploiement de la carte nationale d'identité électronique (CNIe), prévu à partir de 2021, devrait permettre de proposer une solution d'identité numérique régalienne à l'ensemble des français.

Recommandation n°19 : La CSNP demande au Gouvernement d'accélérer le déploiement de l'identité numérique régalienne afin que nos concitoyens disposent dans les meilleurs délais de cet instrument essentiel pour la sécurité des accès aux ressources numériques. Cette accélération est également nécessaire pour que la France ne prenne pas de retard supplémentaire par rapport à ses voisins européens.

III. Sur la dimension géopolitique de la lutte contre les cybermenaces

- **Sur une mise en œuvre plus rapide de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace**

Le 12 novembre 2018, à l'occasion de la réunion à l'UNESCO du Forum sur la gouvernance de l'internet (FGI) et du premier Forum de Paris sur la paix, le Président de la République, Emmanuel Macron, a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, une déclaration de haut niveau articulée autour de neuf principes et de valeurs communes pour faire du cyberespace un espace libre, sûr et ouvert.

Aujourd'hui soutenu par 79 Etats, 35 organismes publics, 387 organisations et membres de la société civile ainsi que par 702 entreprises, l'Appel de Paris permet à l'ensemble de ces acteurs d'agir de

concert afin de faire respecter dans le cyberespace les mêmes droits fondamentaux et principes qui s'appliquent dans le monde physique. En novembre 2020, le ministre de l'Europe et des Affaires étrangères a annoncé la création de six groupes de travail issus de secteurs et pays différents qui rendront des travaux et résultats préliminaires en novembre 2021.

Pour les membres de la CSNP, la France doit se saisir de cet Appel pour amorcer un véritable changement de paradigme dans la gestion de la sécurité dans l'espace numérique. Il s'agit d'une opportunité à développer au profit du caractère opératoire et législatif de cet Appel afin qu'il soit en mesure de fournir des cadres concrets de lutte contre les nouvelles menaces : cybercriminalité, espionnage, vols de données personnelles ou d'informations confidentielles, attaques contre des individus ou des infrastructures…

Recommandation n°20 : La CSNP recommande que les ambitions de l'Appel de Paris, et leur traduction en mesures opératoires par les groupes de travail, soient portées par le gouvernement auprès de l'Union européenne dans le cadre de la Présidence française de l'UE de 2022.

Dans une perspective d'amélioration de la coopération européenne et internationale en matière de lutte contre la cybercriminalité, il apparaît essentiel de réguler les activités de dévoilement des failles de sécurité et de vulnérabilité. Certains chercheurs agissent de manière irresponsable en documentant publiquement des vulnérabilités, laissant ainsi le champ libre aux cybercriminels pour les exploiter avant qu'elles aient fait l'objet de la publication de correctifs.

Recommandation n° 21 : La CSNP recommande le développement d'une politique publique de régulation des démarches de divulgation des vulnérabilités afin que les propriétaires de vulnérabilités et les chercheurs coopèrent pour réduire les risques associés à une divulgation inappropriée dans l'espace public. La CSNP appelle le Gouvernement à se saisir des recommandations du rapport de l'OCDE "*Encouraging vulnerability treatment*" publié le 11 février 2021, et à les porter au niveau européen dans le cadre de la PFUE 2022, et à l'international à l'ONU, dans le cadre de l'Appel de Paris, du G7 et du G20.

- **Sur la stratégie de cyberdéfense française**

La cyberdéfense est un pilier essentiel de la stratégie de défense et de sécurité nationale. L'ANSSI déploie des compétences remarquables au profit de la cyberprotection des services de l'État, des opérateurs d'importance vitale et de services essentiels, ainsi que de l'ensemble des organismes publics et privés. Cependant, à la lumière des dernières attaques, l'on constate que ces capacités nationales interviennent essentiellement en "pompiers" pour accompagner les victimes des cyber-agressions. Confrontée à ce qui s'apparente à une guerre permanente, menée par des cybercriminels qui agissent bien souvent en proximité avec des agences étatiques ou des officines paraétatiques, la défense dans la profondeur de la collectivité nationale est désormais une priorité au service de la résilience de la société et de son économie. La capacité des services de l'Etat concernés (ANSSI, Ministère de l'Intérieur, Ministère des Armées) doit être développée de manière très substantielle afin qu'ils soient en mesure de détecter et d'identifier les attaquants partout sur la planète, et engager les instruments de la force légitimes pour neutraliser les cybercriminels, avant qu'ils ne commettent leurs méfaits.

Recommandation n°22 : La CSNP invite les commissions compétentes du Parlement à s'informer auprès du Gouvernement et des services chargés, à divers titres, des missions de cyberdéfense dans le détail, et à vérifier l'adéquation du dispositif national à la réalité évolutive et croissante de la cybermenace. La CSNP se tient à leur disposition pour compléter leur information sur le diagnostic porté par ses membres.

- **Sur les priorités de la présidence française de l'Union Européenne en 2022**

La France présidera le Conseil de l'Union européenne au cours du premier semestre 2022. Il paraît hautement souhaitable aux membres de la CSNP que les autorités françaises inscrivent à l'agenda de ses travaux, le sujet de la coopération européenne en matière de politique numérique et de sécurité dans l'espace numérique.

Il apparaît à notre Commission qu'un véritable changement de paradigme doit s'opérer en Europe pour envisager un niveau acceptable de cyber-risque dans l'espace numérique. Dans un secteur largement dominé par les Etats-Unis, et demain par la Chine, l'Europe doit trouver les voies et moyens de son autonomie afin de maîtriser ses dépendances à des technologies et des opérateurs extra-européens. La présidence française de l'Union Européenne en 2022 constitue une opportunité que la France doit saisir pour initier ce changement de paradigme et mobiliser dans cette démarche ses partenaires européens, ainsi que les acteurs clés du secteur du numérique.

Recommandation n°23 : La CSNP recommande que la PFUE 2022 soit mise à profit pour porter différents sujets auprès des Etats membres et des institutions, afin de renforcer la sécurité et la protection de l'espace numérique européen :

- Le parquet européen doit acquérir des compétences dans le traitement et l'application de peines en matière de cybersécurité sans toutefois empiéter sur les compétences qui relèvent du droit national. (Cf. recommandation n°4)
- Les recommandations des groupes de travail de l'Appel de Paris devront être endossées par les institutions européennes afin d'orienter les futures politiques publiques sur l'espace numérique et sa protection. (Cf. recommandation n°20)
- La France doit engager les institutions européennes dans la promotion d'une régulation internationale du dévoilement des vulnérabilités des produits et services numériques. (Cf. recommandation n°21)
- La France doit promouvoir l'échelle européenne pour imposer des normes minimales de sécurité par conception sur l'ensemble des produits et services numériques mis en service sur le marché européen. (Cf. recommandation n°24)

IV. <u>Sur les enjeux liés à la sécurité des produits numériques et connectés et un cloud de confiance</u>

- **Sur la sécurité des produits et des services numériques**

L'espace numérique recouvre un ensemble d'acteurs, de technologies et de chaînes de valeurs complexes et souvent mondialisés (hardware, middlewares, softwares, datas…). Bien souvent les produits et services numériques sont considérés à tort comme « suffisamment sûrs » or, ils reposent

sur un code informatique par nature vulnérable aux cyberattaques. Ces failles de sécurité n'apparaissent pas seulement lors de la phase d'exploitation d'un produit ou d'un service numérique mais bien tout au long de son cycle de vie, et notamment lors de sa conception.

En s'appuyant sur deux études comparatives sur le cycle de vie et la chaîne de valeur des produits et services numérique, l'OCDE a mis en évidence le rôle des facteurs économiques, des pouvoirs publics et des acteurs finaux dans les dynamiques de création et d'établissement des normes de sécurité de ces produits et services. L'Organisation met en évidence les nombreuses défaillances de marchés qui ne permettent pas aux acteurs industriels de fournir des normes de sécurité optimales sur le marché du numérique. Contrairement à la plupart des autres secteurs industriels, l'industrie du numérique n'est pas encore soumise à des normes minimales de sécurité. La sécurité numérique étant un domaine dynamique en constante évolution, les acteurs industriels doivent être encouragés à traiter ces vulnérabilités de façon plus efficace sur le temps long.

Recommandation n° 24 : Les membres de la CSNP appellent à l'adoption de normes minimales de sécurité sur tous les produits et services numériques avant leur mise sur le marché, en cohérence avec les préconisations formulées par l'OCDE dans son rapport « *Enhancing the digital security of products* » publié le 9 février 2021. Afin de favoriser l'adoption de principes de haut niveau de sécurité numérique par conception, les pouvoirs publics nationaux et européens pourraient décliner des mécanismes d'incitations pour le développement de normes communes et des instruments règlementaires contraignants. A cet égard, la France et l'Europe doivent renforcer leur présence dans les instances de normalisation internationales.

- **Sur le *cloud* de confiance**

Le *cloud* n'est plus un simple sous-domaine du secteur numérique. Il est désormais celui qui commande tous les autres. Comme la crise sanitaire l'a amplement montré, de façon extrêmement concrète, les données sont au cœur de la transformation numérique, et le *cloud* est à présent le socle incontournable du système d'information des entreprises et administrations publiques. De plus, quasiment tous les champs de l'innovation numérique (intelligence artificielle, objets connectés, *edge computing*, industrie 4.0, 5G et 6G, calcul intensif, *quantum computing*, pour ne citer que ces quelques exemples) se cultivent aujourd'hui dans les environnements mis à disposition par le *cloud*.

Le concept de cloud de confiance repose sur trois piliers : la garantie de sécurité, à laquelle le label SecNumCloud serait susceptible de répondre, l'immunité aux législations extra-européennes, la maîtrise de leurs dépendances par les utilisateurs, notamment en termes de portabilité des données et des traitements associés, de réversibilité des offres, d'interopérabilité des solutions, de transparence des contrats. Le cloud de confiance va progressivement devenir une condition indispensable de la sécurité dans l'espace numérique des entreprises et administrations publiques de toutes tailles et de toutes natures.

Recommandation n°25 : La CSNP incite le Gouvernement à développer et renforcer les liens entre les acteurs politiques et industriels du numérique afin de faire émerger des solutions de cloud de confiance, notamment au profit des applications les plus sensibles pour nos concitoyens comme celles traitant des données de santé. La CSNP appuie par ailleurs la mise en cohérence du projet GAIA-X avec les enjeux nationaux du cloud de confiance. Enfin, la CSNP demande au Gouvernement de l'informer régulièrement de la mise en œuvre de sa feuille de route d'accélération du cloud de confiance.

V. L'élaboration et la conduite des politiques publiques en faveur de la sécurité dans l'espace numérique.

Depuis plusieurs années, les sujets numériques sont désormais présents à tous les niveaux, et dans tous les départements ministériels. Ils nécessitent un pilotage à la fois transversal et centralisé permettant de renforcer la cohérence des actions engagées. La plupart des recommandations émises plus haut dans cet avis relèvent du champ de compétence des Ministères de l'Economie, des Finances et de la Relance, des Armées, de la Justice, de l'Intérieur, de l'Europe et des Affaires étrangères, de l'Enseignement supérieur de le Recherche et de l'Innovation, de la Cohésion des territoires et des Relations avec les collectivités territoriales, voire directement de l'action du Premier ministre.

Recommandation n°26 : Suivant en cela une appréciation constante de notre commission, la CSNP recommande au Gouvernement d'incarner au meilleur niveau, auprès du Premier ministre, une autorité politique interministérielle chargée d'élaborer, de fédérer et de conduire les politiques publiques en matière de numérique, et dont la sécurité serait une priorité.

La France, son économie, et l'ensemble de nos concitoyens doivent pouvoir compter, pour adapter le pays aux enjeux du vingt-et-unième siècle, dans la durée et le temps long, sur une puissante organisation en mesure d'éclairer l'avenir numérique par la recherche, et de le préparer par l'investissement. C'est à cette condition que la France, et avec elle le continent européen, retrouveront leur autonomie et leur capacité à développer un numérique sûr, éthique, durable et de confiance.

L'histoire du Commissariat à l'énergie atomique et aux énergies alternatives peut nous inspirer en la matière. Il a été l'instrument de l'autonomie de la France dans le domaine de l'énergie atomique civile et militaire, laquelle permet à notre pays de disposer d'un siège permanent au Conseil de sécurité de l'ONU et d'être un Etat parmi les plus vertueux en matière de rejet de CO2 pour sa production électrique.

Recommandation n°27 : La CSNP suggère au Gouvernement d'étudier une articulation plus efficiente des capacités nationales de recherche et technologie dans le domaine du numérique, fédérant notamment les ressources de l'INRIA, du CEA et du CNRS, dans une gouvernance commune. Cette gouvernance pourrait reposer sur une direction des applications civiles et une direction des applications de sécurité nationale. Son objectif, assorti des moyens nécessaires, consisterait à éclairer l'avenir par la recherche et à le préparer par l'investissement.

Auditions de la Commission supérieure du numérique et des postes

M. Guillaume POUPARD, Directeur général de l'ANSSI

M. Mathieu HEURTEL, conseiller en charge des Entreprises et des Technologies auprès du cabinet du Secrétaire d'État chargé de la Transition numérique et des Communications électroniques

Mme Myriam QUEMENEUR, Magistrate

M. Bruno CHARRAT, Directeur du département cybersécurité au Commissariat à l'Energie Atomique

M. Bernard DUVERNEUIL, Président du Cigref

MM Laurent BERNAT et **Gislain de SALINS**, Département Digital Security Policy de l'OCDE et auteurs du rapport « Des politiques intelligentes pour les produits intelligents »

M. Gérôme BILLOIS, Partenaire cybersécurité et confiance numérique en charge de la gestion des risques numériques de Wavestone

Bibliographie

"Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris,

« Des politiques intelligentes pour les produits intelligents », Note sur les politiques de la Direction de la science, de la technologie et de l'innovation, OCDE, Paris.

"Encouraging vulnerability treatment: Overview for policy makers", OECD Digital Economy Papers, No. 307, OECD Publishing, Paris

Dossier de presse du 18 février 2021, "Cybersécurité faire face à la menace : la stratégie française", Gouvernement.

Dossier de presse du 22 mars 2021, « Cybersécurité : protéger les services publics et les collectivités territoriales avec France Relance », Gouvernement.

Sitographie

Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace