

Recommandations dans le domaine de la sécurité numérique

Description

Pour éviter que nos démocraties soient confrontées au chaos numérique à l'horizon de la prochaine décennie

Face à la très forte recrudescence d'attaques informatiques depuis deux ans, la Commission supérieure du numérique et des postes (CSNP), constituée de parlementaires des deux chambres, a remis au gouvernement, dans un avis du 29 avril 2021, vingt-sept recommandations pour éviter que nos démocraties soient « *confrontées au chaos numérique à l'horizon de la prochaine décennie* ». Tout en saluant le plan « cyber », stratégie nationale pour la cybersécurité présentée par Emmanuel Macron le 18 février 2021, et notamment l'investissement de 1 milliard d'euros « *qui devraient permettre de réduire les vulnérabilités des systèmes informatiques de nombreuses infrastructures publiques et privées* », la CSNP exhorte l'exécutif à déployer et renforcer sans commune mesure les capacités de lutte contre la cybercriminalité.

L'avis détaille les points d'amélioration du plan cyber mais aussi « *la stratégie de cyberdéfense de l'État 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* ».

La Commission recommande notamment la création d'un « *parquet national cyber* », afin de remédier à la situation actuelle avec, pour tout le pays, seulement trois magistrats pour traiter les dossiers de cybercriminalité et elle plaide également pour la création, lorsque la France présidera l'Union européenne de janvier 2022 à juin 2022, d'un parquet européen spécialisé dans la cybercriminalité. La Commission suggère en outre l'adoption de mesures visant à lever le secret des enquêtes judiciaires en renforçant le champ d'action de l'Agence nationale de la sécurité des systèmes d'information (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* » ; elle encourage également à mobiliser des moyens pour que l'ANSSI parvienne à fidéliser ses agents dont le profil est fortement recherché sur le marché du recrutement.

Pour développer une cybersécurité à l'échelle territoriale, la CSNP préconise de renforcer le rôle des CSIRT (Computer Security Incident Response Team – équipe de réponse aux incidents informatiques) prévues par le plan cyber pour être déployées dans chaque région. Elles pourraient ainsi devenir, coordonnées par l'ANSSI, des « *campus régionaux de la sécurité numérique capables de fédérer localement les acteurs de la sécurité numérique et de les faire travailler en réseau* ».

Les parlementaires suggèrent en outre au gouvernement de réguler le paiement des attaques par rançongiciels ([voir La rem n°56, p.24](#)) afin d'éviter que 20 % des entreprises victimes, incitées par des

sociétés d'assurances, optent pour le paiement de la rançon, *« car elle entretient et renforce l'activité des cybercriminels, dont il est absolument indispensable de tarir les ressources »*. Cette année 2021, l'ANSSI recense *« une attaque par semaine sur des établissements de la chaîne hospitalière »* et en 2020, *« 20 % des victimes de rançongiciels étaient des collectivités locales et 11 % des établissements de santé publics ou privés »*.

Quatre recommandations portent sur la sensibilisation et la formation à la sécurité numérique, ainsi qu'à la féminisation de ces métiers, et notamment ceux liés à la cybersécurité, *« dans lesquels les femmes représentent à peine 11 % des effectifs, selon la plupart des études »*.

Les parlementaires encouragent fortement à accélérer le déploiement de l'identité numérique régaliennne, alors que *« plus de 200 000 Français par an sont victimes d'usurpation de leur identité dans l'espace numérique »*. C'est l'objet du programme France Identité Numérique, créé en 2018, qui prolonge la mise en place de FranceConnect, depuis 2016, un dispositif d'identification utilisé par quelque 24 millions de Français en 2021, qui facilite l'accès aux services publics numériques et garantit la sécurisation des informations transmises. C'est également le but de la nouvelle génération de carte nationale d'identité électronique (CNIe), au format carte bancaire et dotée d'une puce sans contact, dont le lancement a été confirmé le 16 mars 2021. La Commission recommande d'accélérer le déploiement de ce système d'identité régaliennne, afin notamment que *« la France ne prenne pas de retard supplémentaire par rapport à ses voisins européens »*.

Tout en saluant les *« compétences remarquables »* de l'ANSSI, la Commission recommande cependant de considérablement développer et coordonner les capacités de l'État avec le ministère de l'Intérieur et le ministère des Armées, afin d'être en mesure de *« détecter et d'identifier les attaquants partout sur la planète, et engager les instruments de la force légitime pour neutraliser les cybercriminels avant qu'ils ne commettent leurs méfaits »*. En effet, l'avis révèle que l'ANSSI intervient très souvent en *« pompier »*, lorsqu'une attaque informatique a déjà eu lieu, et qu'une stratégie de cyberdéfense française ambitieuse doit s'adapter à ce qui s'apparente dorénavant *« à une guerre permanente, menée par des cybercriminels qui agissent bien souvent en proximité avec des agences étatiques ou des officines paraétatiques »*. Parce que la situation sécuritaire dans l'espace numérique, aujourd'hui particulièrement préoccupante, devrait continuer à se dégrader dans les années à venir, *« 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 »*.

Recommandations dans le domaine de la sécurité numérique, Commission supérieure du numérique et des postes (CSNP), avis n° 2021-03, 29 avril 2021.

Categorie

1. A lire en ligne

date créée

22 juillet 2021

Auteur

jacquesandrefines