ASSEMBLÉE NATIONALE

17ème législature

Actualisation de la revue stratégique de cyberdéfense

Question écrite n° 3652

Texte de la question

Mme Anne Le Hénanff appelle l'attention de M. le ministre des armées sur l'actualisation de la revue stratégique de cyberdéfense. Conscient que l'augmentation des cyberattaques et de leur intensité était susceptibles de porter atteinte, à tout moment, aux intérêts et à la souveraineté de la Nation, Edouard Philippe, alors Premier ministre, avait confié au Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) le soin de rédiger en 2018 une revue stratégique de cyberdéfense. Véritable livre blanc, cette revue est le premier grand exercice de synthèse stratégique dans ce domaine et dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la Nation et ouvre des perspectives visant à améliorer la cybersécurité de la société française. Si cette première édition marque le début d'une véritable prise de conscience de la menace et d'une stratégie pour le pays, 6 ans plus tard, force est de constater que les menaces cyber auxquelles il faut faire face ont évolué, augmenté et se sont intensifiées. Les crédits inédits (4 milliards) alloués à la cyberdéfense dans le cadre de la LMP 2024-2030 ou encore la future transposition de la directive NIS 2 témoignent de la nécessité d'investir et de renforcer l'arsenal aussi bien matériel que législatif dans le domaine cyber. Comme le recommande le rapport sur les défis de la cyberdéfense (2024) dont Mme la députée est co-auteure, il est nécessaire de mettre à jour cette revue stratégique afin de prendre en compte de nouveaux enjeux et de nouveaux acteurs telles que les collectivités locales. Enfin, alors que le Président de la République, lors de ses vœux aux armées le lundi 20 janvier 2025 a demandé l'actualisation de la revue nationale stratégique (RNS) d'ici le mois de mai prochain, notamment au regard du contexte géopolitique, la mise à jour de la revue stratégique de cyberdéfense apparaît très opportune. Aussi, elle souhaite savoir quand paraîtra l'actualisation de la revue stratégique de cyberdéfense.

Texte de la réponse

La revue stratégique de cyberdéfense du 12 février 2018, faisant suite à un premier exercice de stratégie nationale du numérique datant de 2015, a constitué une incontestable avancée conceptuelle et organisationnelle pour le dispositif nationale de cybersécurité. Ainsi, c'est la revue stratégique de cyberdéfense qui a fixé l'actuelle organisation nationale en quatre chaînes de responsabilité, couvrant l'intégralité des besoins de cybersécurité du pays. C'est aussi la revue de 2018 qui a renforcé les structures de gouvernance du domaine de la cybersécurité et leur a donné leur forme actuelle. Depuis lors, et tout particulièrement depuis deux ans au moins, le contexte cybersécuritaire s'est considérablement dégradé. Comme les rapports de l'agence nationale de sécurité des systèmes d'information consacrés à l'état de la menace le décrivent, les actes de malveillance à l'encontre des systèmes d'information ne cessent de croître. La cybermenace est donc désormais considérée comme une menace systémique. Sommairement, cette menace se décompose en trois : le cyberespionnage et l'ensemble des manœuvres menées ou commanditées par des États ; la cybercriminalité ; le militantisme hacktiviste. Indéniablement, les deux premières catégories sont les plus dangereuses. La menace de type étatique a muté et s'est aggravée : longtemps centrées sur l'espionnage, les opérations des services spéciaux comprennent désormais beaucoup de prépositionnements à des fins destructives, pouvant affecter des infrastructures vitales et donc les populations. Pour sa part, la cybercriminalité a industrialisé les attaques à des

fins crapuleuses - notamment le blocage des systèmes d'information par rançongiciel - et cause des dégâts considérables au sein de certaines infrastructures d'intérêt public comme les hôpitaux, mais aussi parmi les acteurs économiques. Ce caractère systémique de la cybermenace allié à une dégradation de l'environnement géostratégique et un affaiblissement des cadres internationaux de régulation des tensions a amené le Président de la République à confier au secrétariat général de la défense et de la sécurité nationale la mission d'animer des travaux interministériels d'actualisation de la stratégie nationale de cybersécurité. Ce travail a été mené par l'ingénieur général de l'armement Bruno Marescaux qui a présenté les principes dégagés par ses travaux au cours du mois de décembre 2024. Le Président de la République a souhaité que divers aspects complémentaires soient étudiés en détail. Le rapporteur présentera le résultat de ces travaux complémentaires au Président de la République et au Premier ministre au mois de mai 2025. Par ailleurs, ces travaux alimenteront l'actualisation de la revue nationale de stratégie qui devrait être publiée à l'été 2025.

Données clés

Auteur : Mme Anne Le Hénanff
Circonscription : Morbihan (1re circonscription) - Horizons & Indépendants
Type de question : Question écrite
Numéro de la question : 3652
Rubrique : Défense
Ministère interrogé : Armées
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 4 février 2025, page 440
Réponse publiée au JO le : 29 avril 2025, page 3073