

ASSEMBLÉE NATIONALE

4 mai 2023

PROGRAMMATION MILITAIRE 2024-2030 - (N° 1033)

Non soutenu

AMENDEMENT

N° CL8

présenté par

Mme Lingemann, M. Blanchet, M. Bru, M. Lainé, Mme Poueyto et M. Cubertafon

ARTICLE ADDITIONNEL**APRÈS L'ARTICLE 35, insérer l'article suivant:**

Le ministère de la défense met en place plusieurs niveaux de certification militaire répondant aux normes en matière de cybersécurité et de conformité à destination des organismes et entreprises.

À destination des organismes et entreprises, le ministère de la défense dresse une liste regroupant les normes, directives et bonnes pratiques pour gérer les risques liés à la cybersécurité.

EXPOSÉ SOMMAIRE

La cybersécurité est devenue un enjeu majeur pour les entreprises et les organisations, et l'identification des risques en amont est cruciale pour éviter les conséquences graves que peut entraîner une attaque informatique. Pour réduire les risques liés à la cybersécurité, il est important de mettre en place des certifications de sécurité qui s'inspirent des certifications de type DGA et BPI ainsi que du modèle américain du National Institute of Standards and Technology (NIST) et sa liste "Cybersecurity Framework".

De manière complémentaire, il convient d'ériger un ensemble de normes, de directives et de bonnes pratiques pour la gestion de ces risques afin d'instaurer des pratiques de sécurité standardisées au sein des organisations, ce qui facilite la gestion des risques et la mise en place de mesures de protection adéquates.

Ainsi, cet amendement a pour objectif de fixer un cadre volontaire qui peut être utilisé pour analyser, encadrer et réduire les risques cyber selon une échelle de priorités.