

France : la surveillance massive actée en juillet 2018 dans la LPM

Loi de programmation militaire « 2019-2025 »

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037192797&categorieLien=id>

[LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense \(1\)](#)

- [Titre II : DISPOSITIONS NORMATIVES INTÉRESSANT LA DÉFENSE NATIONALE](#)
 - [Chapitre XI : Dispositions diverses et finales](#)

Article 65

ELI: https://www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/article_65

Alias: https://www.legifrance.gouv.fr/eli/loi/2018/7/13/2018-607/jo/article_65

Article 65

3.-UNE LPM STRUCTURÉE AUTOUR DES AXES PRIORITAIRES DE L'AMBITION 2030

3.3.3.1. Une structuration volontariste de l'action du ministère dans l'espace numérique

Le développement du cyberspace à l'échelle planétaire, la rapidité d'accroissement de la dépendance au numérique de nos moyens militaires ainsi que l'extension des risques d'attaque sur nos systèmes électroniques, nécessitent le développement de capacités de cyberdéfense dans toutes leurs dimensions. Transverse aux fonctions stratégiques qu'elle soutient, la cyberdéfense porte en son sein un enjeu de souveraineté nationale.

S'inscrivant dans la cadre des conclusions de la revue stratégique Cyber, la loi de programmation militaire 2019-2025 renforce les capacités des armées en matière de prévention, de détection et d'attribution des cyberattaques. Elle les dote également de moyens de réaction rapides, efficaces et coordonnés à l'horizon 2025 afin de garantir une protection et une défense de nos systèmes et réseaux, cohérente dans tous les secteurs (cyberprotection, lutte informatique défensive, influence numérique, lutte informatique offensive et moyens de commandement et d'entraînement). Elle prévoit en outre des effectifs supplémentaires à hauteur de 1 500 sur la période.

L'effort au profit de la cyberdéfense concernera également la protection des systèmes d'armes et des systèmes d'information, dès leur phase de conception et pendant leur utilisation. **En outre, la posture permanente cyber (PPC) garantira la surveillance de nos réseaux ainsi que le caractère opérationnel des capacités actives ou passives de lutte informatique défensive.** Pour ce faire, les capacités d'intervention et de détection du centre d'analyse et de lutte informatique défensive (CALID), des centres opérationnels de sécurité (SOC) des armées, de la 807e compagnie de transmissions et du centre interarmées des actions sur l'environnement (CIAE) seront renforcées. En outre, un grand nombre d'unités spécialisées seront regroupées sur le pôle de Rennes.

En matière de lutte informatique offensive, de nouvelles capacités d'action, intégrées à la chaîne de planification et de conduite des opérations, seront systématiquement déployées en appui de la manœuvre des armées. En effet, s'appuyant sur la numérisation croissante de nos adversaires, elles offrent des options alternatives ou complémentaires aux effets des systèmes d'armes conventionnels. Cette période sera aussi mise à profit pour étudier l'élargissement des contextes opérationnels d'emploi de l'arme cybernétique.

Source :

<http://www.santepublique-editions.fr/objects/France-surveillance-massive-actee-dans-LPM-juillet-2018.pdf>