P129

Intervention en commission de M. Olivier CADIC

mercredi 16 novembre 2022

Monsieur le Président, Chers Collègues,

Les crédits du programme 129 que nous allons vous présenter avec mon collègue Mickaël Vallet, dont je salue l'engagement, portent sur la coordination de la sécurité et de la défense, et plus précisément sur la cyberdéfense et les stratégies d'influence.

Nous avons procédé à 6 auditions au Sénat, 3 déplacements en France (Viginum, campus cyber et porte parole de l'État major des armées) et un déplacement à Atlanta avec 4 auditions, tout ça en moins de deux mois, depuis l'arrivée de Jean Pouch, que je salue pour son remarquable travail.

L'enjeu de la guerre informationnelle, que j'avais mentionné lors des débats sur la LPM en 2018, est enfin pleinement reconnu.

Le Président de la République vient de les élever au rang de nouvelle fonction stratégique dans son discours de Toulon du 9 novembre dernier.

Je m'en félicite. J'avais salué la création de Viginum l'an dernier.

Je suis circonspect, en observant le champ restreint de ses missions qui s'arrêtent à la caractérisation de situations d'ingérence et de désinformation.

Sans pouvoir intervenir dans la réponse – ou la contre-attaque – à apporter, nous sommes loin de Taiwan qui répond à une désinformation en 2 heures et 200 mots.
J'espère que l'impulsion donnée par la revue nationale stratégique sera de nature à rendre plus efficace nos actions de contre ingérence.

La passivité est une erreur qui nous a couté très cher.

Je parle de l'opération de désinformation dont l'armée française a été victime dans l'affaire de Bounti au Mali en janvier. Les leçons en ont été tirées. L'efficace riposte pour déjouer le stratagème de Wagner du charnier de Gossi l'a démontré. Il nous faut maintenant assumer une posture plus offensive y compris dans le domaine de la cybersécurité.

En effet, les menaces de cybersécurité croissent suivant un rythme exponentiel. L'augmentation des moyens humains (+61 ETP) et budgétaires (+9 M€) du SGDSN ne semble pouvoir en ralentir la course. (173 000 demandes d'assistance en 2021 sur le site cybermalveillance.gouv.fr et 1082 signalements d'incidents traités par l'ANSSI). Des attaques très graves ont perturbé les services publics, collectivités territoriales et établissements de santé. Avec une hausse de 95 % des attaques, les rançongiciels sont la première menace pour les professionnels (entreprises, associations et

collectivités). Les préjudices subis, financiers mais aussi humains, peuvent aller jusqu'à compromettre la sécurité nationale.

Nos capacités techniques, notamment l'expertise de l'ANSSI, sont reconnus par nos partenaires.

Mes chers collègues, allons-nous nous contenter de regarder chaque année le compteur s'affoler ?

Nos principaux partenaires, américains et britanniques, ont compris qu'aller entraver les cybercriminels sur leur terrain, c'est aussi prévenir les attaques avant qu'elles n'arrivent et pratiquer une forme de dissuasion numérique.

Je formule donc la proposition que nous nous dotions d'une stratégie offensive face aux cyber-attaques, que nous nous dotions d'un directeur national de la cybersécurité et que nous nous coordonnions avec nos principaux partenaires, car c'est un combat sans frontières.

Avant de céder la parole à mon collègue, je voudrais insister sur deux points :

1- La nécessité de former et responsabiliser tous les acteurs en cybersécurité, à commencer par les simples utilisateurs ;
2- Alerter sur la nocivité du paiement des rançons. Ceux qui sont contraints de payer pour sauver leur entreprise doivent savoir qu'ils alimentent les revenus de la cybercriminalité qui dépassent désormais ceux du narcotrafic. Ils contribuent également au financement du terrorisme.

Tous les pays occidentaux sont dépassés par l'échelle des attaques. On nous fait une guerre cyber. Les 14 affaires d'espionnage cyber en 2021 dont 9 sont d'origine chinoises en témoignent. Nos agresseurs sont à l'initiative. Nous avons un retard à rattraper.