…le rapport d'information sur le programme 129 « Coordination du travail gouvernemental »

POUR UNE COORDINATION DE LA CYBERDÉFENSE PLUS OFFENSIVE DANS LA LOI DE PROGRAMMATION MILITAIRE 2024-2030

Rapport d'information n° 638 (2022-2023) du groupe de travail de préparation de la loi de programmation militaire 2024-2030 (LPM 2024-2030) sur la coordination de la cybersécurité (programme 129), composé de MM. Oliver CADIC, Mickaël VALLET, rapporteurs, et André GATTOLIN, sénateur.

Avec **831 intrusions répertoriées en 2022 par l'ANSSI** dans sa publication annuelle du panorama de la cybermenace, plus de **170 000 demandes d'assistance reçues par Cybermalveillance**, dont 90 % émanent de collectivités territoriales, et **150 événements de sécurité numérique touchant au périmètre du ministère des armées** (hors services de renseignement), l'**évolution du niveau de la menace** se caractérise par un passage à l'**échelle « industrielle »** des organisations criminelles (étatique et non-étatique), une concentration des attaques sur les **vulnérabilités des systèmes** (établissements de santé, collectivités territoriales et PME), une **agilité technologique** accrue des cybercriminels et une **finalité lucrative** (rançongiciels).

Aussi, parmi les 10 objectifs stratégiques fixés par la **revue nationale stratégique** de 2022 (RNS 2022), **l'objectif n°4 vise à atteindre « une résilience cyber de premier rang »** afin de prévenir et réduire l'impact et la durée des cyberattaques à l'encontre des fonctions les plus critiques ; cela en s'appuyant sur l'écosystème cyber public et privé, la gouvernance de la sécurité numérique de l'État et en élevant le niveau global de cybersécurité de l'ensemble des acteurs.

La LPM 2024-2030 prévoit 3 axes de renforcement de la cyberdéfense :

- **4 milliards d'euros de besoins programmés** (effectifs et technologies) ;
- **appui à l'Agence nationale de sécurité des systèmes d'information** (ANSSI) ;
- **renforcement des capacités de l'ANSSI pour l'analyse et la détection des cyber menaces**.

4 milliards d'euros de besoins programmés pour le Cyber, contre 1,6 milliard d'euros pour la LPM 2019-2025

Périmètre des emplois cyber en 2023 (3 502 postes armés) pour un objectif initial de 5 000 cyber-combattants en 2025[1]

Augmentation des effectifs sur la période 2024-2030 au profit principalement de l'État-major, de la DGA et de la DGSE

[1] 770 cyber-combattants en plus des 1 100 initialement prévus par la LPM 2019-2025 pour porter à 5 000 le nombre de cyber-combattants en 2025.

1. BUDGET CYBER DE LA LPM 2024-2030 : 4 MILLIARDS D'EUROS

A. TROIS AXES D'EFFORT EN FAVEUR DE LA CYBER PROTECTION, DE LA LUTTE INFORMATIQUE DÉFENSIVE ET LA DIVERSIFICATION DES MOYENS D'ACTION

Avec **4 milliards d'euros de besoins programmés pour le cyber, contre 1,6 milliard d'euros pour la LPM 2019-2025**, l'enveloppe de la LPM 2024-2030 concerne principalement la **cyber protection**, notamment la cryptographie, dans le cadre du programme 146 « Équipement des forces ». Verront leurs dotations augmentées les dépenses de fonctionnement du commandement de la cyberdéfense (ComCyber), le maintien en condition opérationnelle des programmes d'armement, et le développement de capacité cyber de la DGSE. La **lutte informatique défensive** (LID) et les nouveaux domaines d'actions sont les deux autres axes d'effort de cette LPM.

On estime à **près d'un milliard d'euros** la **« dette technique »** à rattraper pour adapter nos forces aux évolutions technologiques.

De plus, le besoin de diversification des moyens d'actions vise à prendre en compte le développement de **l'intelligence artificielle** (IA) pour acquérir une supériorité dans le cyberespace, aussi bien dans les domaines de la LID, la **lutte informatique offensive** (LIO) que dans la **lutte informationnelle et d'influence** (L2I). Il s'agit ici de domaines d'effort dont la ventilation n'est volontairement pas chiffrée afin de ne pas fournir d'éléments pouvant porter atteinte à la défense nationale.

Au retour de leur **visite à Rennes** de la DGA-Maîtrise de l'information, du ComCyber (photo ci-après) et du pôle d'excellence cyber, vos rapporteurs tiennent à saluer l'expertise et le très haut niveau technologique et scientifique des moyens militaires de cyberdéfense.

Ils ont pu constater sur place les synergies développées entre les différents acteurs publics et privés de cet écosystème régalien, inséré dans un bassin régional de formation et d'emploi.

Le pôle d'excellence cyber de Rennes

Le Pôle d'Excellence Cyber a été cofondé par le Minarm et la région Bretagne en 2014 afin de créer un écosystème « régalien » mettant en présence les armées, la Région Bretagne au titre de ses compétences en matière de formation et de développement économique, d'entreprises de cybersécurité (Orange cyber défense, Thalès, Cap Gemini, etc.) et les services de l'ANSSI.

Selon les données de la Région Bretagne, cet écosystème représente :

- 3 280 emplois directs
- 1 000 étudiants formés par an
- 880 cyber-combattants du ministère des armées

À noter que les effectifs de la DGA-MI de l'ordre de 1 400 collaborateurs augmenteront de 500 collaborateurs d'ici 2027 et que le ComCyber et l'ANSSI bénéficieront de nouvelles implantations immobilières.

Visite du groupement de Cyberdéfense des Armées à Saint-Jacques-de-la-Lande (35)

L'effort cyber de la LPM 2024-2030 est donc sans précédent en France. Toutefois, à titre de comparaison, l'audition de **M. Philip M. Stupak, directeur fédéral de la cybersécurité** des États-Unis, a permis de mettre en perspective ce chiffre de 4 milliards d'euros répartis sur 7 ans avec le montant de 5 milliards de dollars qui est l'augmentation en une seule année des moyens fédéraux de la cybersécurité américaine dans les domaines civil et militaire, soit un ordre de grandeur estimatif de **45 milliards de dollars annuels**.

Deux autres ordres de grandeur sont éclairants :

- lorsque Google Cloud investit 10 milliards de dollars, 10 %, soit 1 milliard de dollars, sont consacrés à la cybersécurité ;
- lorsque le Pentagone décide d'engager un programme de cloud de confiance dit « zero trust » avec un consortium d'acteurs majeurs du numérique au profit des forces armées américaines, le projet se chiffre à 9 milliards de dollars.

À cet égard, le sujet du cloud de confiance n'apparaît pas comme faisant partie des priorités de cette LPM, les projets par ailleurs étant conduits par des acteurs français en association avec des sociétés américaines (Thalès et Google cloud, Microsoft avec Cap Gemini et Orange) à l'exception de Dassault.

Constats :
- La LPM 2024-2030 constitue un effort sans précédent au profit de la cyberdéfense des armées ;
- Toutefois le cloud de confiance reste un angle mort de la LPM.

Recommandations :
- Accompagner le développement de la cyberdéfense régalienne autour de l'écosystème de Rennes en renforçant l'offre de formation ;
- Encourager les acteurs français du cloud et de la cybersécurité.

B. DES MOYENS HUMAINS EN HAUSSE EN DÉPIT DE DIFFICULTÉS RÉCURRENTES DE RECRUTEMENT EN RESSOURCES CYBER

Conformément à la trajectoire visée de 5 000 cyber-combattants en 2025, le nombre de postes effectivement ouverts en 2023 s'établissait à 4 600. La LPM 2024-2030 prolonge cette hausse de 953 emplois supplémentaires, soit **un total de plus de 5 553 postes à l'horizon 2030**.

Ventilation de l'augmentation d'effectifs sur la période 2024-2030

	ETPTE
État-major des armées	351
DGA	192
DGSE	386
Autres	24
TOTAL	**953**

Source : réponses du ministère des armées au questionnaire de la commission

Mais sur ce total de 4 600 en 2023, **seuls 3 502 postes sont comptabilisés comme « armés », ce qui représente un déficit de près de 1 100 emplois non pourvus**.

L'ensemble des acteurs publics comme privés font part de difficultés de recrutement pour deux raisons essentielles : l'insuffisance de l'offre de formation et l'inadéquation des salaires proposés par les armées par rapport à l'offre du marché contractuel.

Constats :
- Un déficit de ressources humaines sur le marché de l'emploi cyber ;
- 1 100 postes de cyber-combattants sont encore non pourvus.

Recommandations :
- Prioriser les recrutements sur les postes non encore « armés » ;
- Harmoniser les pratiques de recrutement sur la base du référentiel de rémunération des 56 métiers de la filière numérique et des systèmes d'information et de communication pour fidéliser les agents en poste et recruter des profils expérimentés (direction interministérielle du numérique).

C. CRÉATION D'UN PÔLE D'EXCELLENCE DE FORMATION AUTOUR DE L'ÉCOLE POLYTECHNIQUE

Le troisième axe d'effort de la LPM porte sur la structuration d'une offre de formation (contenus, méthodes et équipes académiques) autour de l'École Polytechnique.

Constat : attention au saupoudrage des moyens dédiés aux pôles d'excellence.
Recommandation : veiller à la complémentarité de l'ensemble des pôles cyber existants en rapprochant le futur pôle d'excellence de formation cyber de Polytechnique avec l'écosystème et l'académie de la cyberdéfense de Rennes.

Si les 4 milliards d'euros de crédits prévus par la LPM sont exclusivement destinés aux armées, elle prévoit deux mesures de soutien à la cyber sécurité civile :

- un appui militaire à l'ANSSI en cas de crise cyber majeure ;

- un renforcement des capacités d'analyse de la menace et de détection des attaques cyber.

2. L'APPUI DES ARMÉES À L'ANSSI EN CAS DE CRISE CYBER MAJEURE

A. RAPPEL DES MOYENS DE LA CYBERDÉFENSE RATTACHÉE AUX SERVICES DU PREMIER MINISTRE (PROGRAMME 129)

Avec **quelque 120 millions d'euros**, les moyens de la cybersécurité « civile » restent sans commune mesure inférieurs à ceux consacrés aux armées.

Agence nationale de la sécurité des systèmes d'information (ANSSI)
création en 2009
660 postes (527 ETPT)
75 millions €

Opérateur des systèmes d'information interministériels classifiés (OSIIC)
création en 2020
300 personnels (135 ETPT)
40 millions €

Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)
création en 2021
42 personnels (47 ETPT)
7 millions €

Or, l'ANSSI doit déjà faire face à la multiplication et à la complexification des cyber menaces. De plus, la directive NIS 2 conduira l'ANSSI à devoir protéger, au-delà des quelques centaines d'OIV et d'OSE (environ 700), plusieurs milliers d'entreprises supplémentaires (7 000 à 14 000).

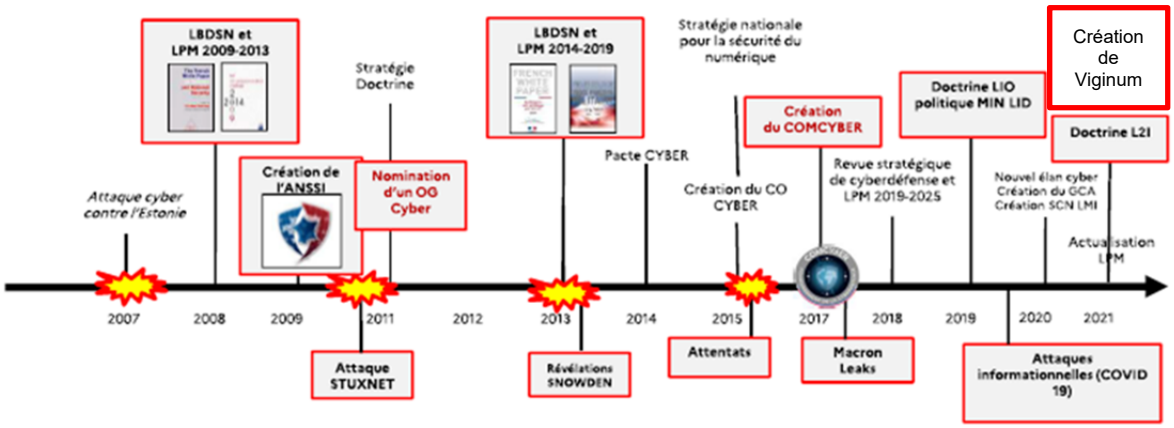
Constats :
- Les moyens de l'ANSSI devraient progresser de 660 personnels en 2023 à 800 en 2027 ;
- Il n'existe pas de trajectoire de programmation des moyens de cyberdéfense du SGDSN comparable dans le montant et la durée avec la LPM.

Recommandations :
- Clarifier le périmètre de la transposition en France de la directive NIS 2 ;
- Établir un plan de progression des moyens de l'ANSSI, de l'OSIIC et de Viginum en rapport avec l'augmentation du périmètre de protection de la directive NIS 2.

B. UNE COORDINATION CIVILO-MILITAIRE QUI S'EST PROGRESSIVEMENT STRUCTURÉE ET DIVERSIFIÉE DEPUIS LES ANNÉES 2010

Bref rappel chronologique des doctrines de LID, LIO et L2I : à la suite d'attaques informatiques étatiques dans les années 2000, l'ANSSI a été créée en 2009, puis le ComCyber en 2017 en matière de LID. La doctrine LIO s'est structurée à partir de 2019, puis la doctrine d'influence (L2I) à partir de 2021 avec la création de Viginum (cf. chronologie ci-dessous).

Chronologie des établissements en charge de la cyberdéfense et de la cybersécurité



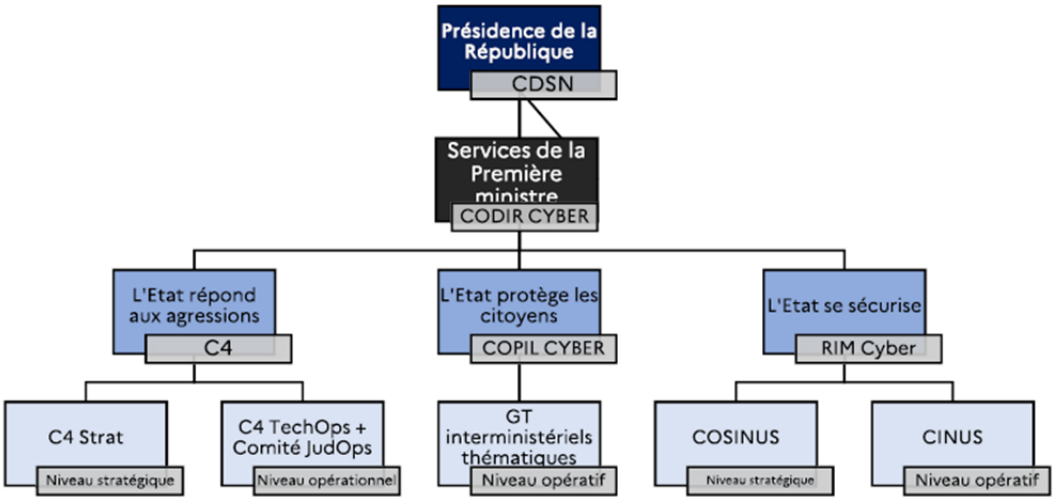
Source : ministère des armées, ComCyber

Le déplacement à Rennes du groupe de travail a permis de constater que la coopération opérationnelle et capacitaire des armées prenait la forme d'échanges réguliers entre la DGA-MI, le ComCyber et l'ANSSI.

C. LE CENTRE DE COORDINATION DES CRISES CYBER (C4) EST LE POINT CENTRAL DES COORDINATIONS STRATÉGIQUE ET OPÉRATIONNELLE

La juxtaposition des doctrines et de moyens civils et militaires s'est accompagnée de la mise en place d'une **coordination interministérielle placée sous l'égide du secrétariat général de la défense et de la sécurité nationale** (SGDSN) qui, en matière de traitement des cyber attaques, est réalisée au sein du centre de coordination des crises cyber (C4).

Schéma représentant les instances de la gouvernance cyber en France



Source : ANSSI

L'ANSSI est l'Autorité nationale de défense et de sécurité des systèmes d'information rattachée au SGDSN qui est un service du Premier ministre. Elle est chargée d'accompagner et de sécuriser le développement du numérique et d'apporter son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE). Elle assure également un service de veille, de détection, d'alerte et de réaction aux attaques informatiques. Son **domaine d'action est défensif**.

La particularité du ComCyber est d'intégrer l'ensemble des missions LID, LIO et L2I dans une même structure de commandement – l'état-major des armées – afin d'assurer la protection des systèmes d'information du ministère y compris sur les théâtres d'opération, ce qui implique une posture permanente.

La coordination technique civilo-militaire se matérialise par une **co-localisation du centre d'analyse en lutte informatique défensive (CALID) du ComCyber avec le centre opérationnel de la sécurité des systèmes d'information de l'ANSSI**.

Au-dessus de ce volet opérationnel (C4 TechOps), le C4 Strat réunit une fois par mois un échelon interministériel de coordination réunissant au SGDSN les ministères et services concernés par la crise. **C'est donc au niveau ministériel et *in fine* présidentiel, pour le volet offensif, que la réponse de l'État aux cyber attaques est traitée**.

La protection des citoyens (Copil Cyber) et la sécurité numérique de l'État (RIM Cyber) relèvent d'une autre comitologie dont le SGDSN est également en charge.

De nouvelles synergies opérationnelles entre la cyberdéfense et la cyber sécurité civile sont à attendre de la localisation de l'ANSSI à Rennes à proximité immédiate du Com Cyber et de la DGA-MI. Toutefois, les rapporteurs citent en exemple de **réactivité la chaîne de commandement militaire, laquelle intègre les 3 fonctions défensive, offensive et d'influence** du cyber, sans équivalant en matière de réponse aux cyber attaques sur des objectifs civils.

À cet égard, **les rapporteurs saluent la prise de position du ministère de l'Europe et des affaires étrangères contre les manipulations russes à l'égard de l'action de la France en Ukraine**. Cette « diplomatie de combat » est rendue possible grâce au travail de détection des campagnes étrangères de désinformation réalisé par Viginum[1]. Cet exemple doit inciter le gouvernement à **adopter une stratégie plus offensive – une « cyber dissuasion » – s'appuyant sur les capacités de cyber sécurité de l'ANSSI et de caractérisation des attaques informationnelles relevant de Viginum**.

> **Constats :**
> - La coordination opérationnelle et technique des moyens militaires et civils en matière de cybersécurité est permanente ;
> - La chaîne de commandement militaire, laquelle intègre les 3 fonctions défensive, offensive et d'influence du cyber, est sans véritable équivalant en matière civile ;
> - Par nature les actions de lutte informatiques et informationnelles offensives d'un certain niveau relèvent de l'autorité présidentielle et du secret de la défense nationale.
>
> **Recommandations :**
> - Lancer une réflexion sur l'opportunité de mieux intégrer les 3 fonctions de LID, LIO et L2I dans le domaine civil ;
> - Affirmer une stratégie de cyber dissuasion s'appuyant sur les capacités de cybersécurité de l'ANSSI et de caractérisation des attaques informationnelles relevant de Viginum ;
> - Envisager la nomination d'un responsable qualité des activités de cyberdéfense.

D. LA NÉCESSITÉ DE CLARIFIER LE VOLET RÉGIONAL DE LA CYBERSÉCURITÉ ENTRE LES CSIRT RÉGIONAUX ET LE GIP ACYMA « CYBERMALVEILLANCE »

Le Plan de relance a prévu une enveloppe de 12 millions d'euros répartis entre 12 CSIRT régionaux (Computer security incident response team[2]), à l'exception de la région Auvergne-Rhône-Alpes. Ces dispositifs, contractualisés en 2021 dans le cadre du Plan de relance, entrent progressivement en œuvre après 2 années consacrées à la création des structures par les régions, l'embauche d'experts et la recherche de locaux sécurisés.

Plusieurs observations peuvent être faites à la lumière d'une visite effectuée au Campus cyber de Nouvelle Aquitaine dont le CSIRT venait d'entrer en service en avril 2023 :

- la création de ces centres, qui remplissent localement les missions régaliennes qui lui sont confiées par l'ANSSI, nécessite **un portage politique important** (au titre de la compétence des régions en matière de développement économique) a**lors même que la pérennité de leur financement n'est pas assurée**. Ceci a pu expliquer le choix légitime d'une région de ne pas rejoindre le dispositif ;

[1] Source : https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et

[2] Centre de réponse aux incidents cyber (CRIC)

- **après la consommation des crédits du Plan de Relance** (1 million d'euros de démarrage par région), l**e risque est grand de voir toute la charge reposer sur les conseils régionaux**. Cela pose la question d'un transfert de compétences régaliennes à des collectivités territoriales.

Les élus régionaux rencontrés en Bretagne et Nouvelle Aquitaine se sont montré allant sur la création de leurs CSIRT respectifs mais appellent d'**urgence à penser dès maintenant l'après Plan de relance** notamment par le biais d'un plan État-Région.

Cette question ne s'éloigne pas du sujet de la LPM dans la mesure où l'objectif stratégique de la revue nationale stratégique est de constituer des synergies entre public et privé pour constituer un environnement sécurisé et faire face aux menaces. Dans une optique d'économie de guerre, **le caractère régalien de la cyber sécurité nécessiterait une harmonisation de l'offre de services** et des modalités d'appel en cas d'incident. L'ANSSI assume le caractère expérimental de la démarche dans sa phase de lancement, mais indique que l'**association « Inter-CERT »** pourrait constituer la tête de réseau des CSIRT régionaux et ultérieurement harmoniser les procédures (certains CSIRT communiquent largement leurs coordonnées tandis que d'autres confient le soin de la diffusion d'informations aux réseaux consulaires et organisations professionnelles).

Pour les rapporteurs, le principe du numéro d'appel universel tel que le « 17 cyber » serait à privilégier en cas d'attaque cyber. Le développement d'une organisation régionale, sans compter les organisations sectorielles, prôné par l'ANSSI pour répondre aux attaques cyber ne fait pas consensus. Ce dispositif n'apporte pas une réponse uniforme sur le territoire national en cas de conflit et fait apparaître de nombreuses faiblesses à commencer par de nombreuses interrogations sur sa pérennité. Une option serait de concentrer les efforts budgétaires publics sur un seul acteur comme le GIP ACYMA (Groupement d'Intérêt Public Action contre la Cybermalveillance), qui a fait ses preuves et dont l'action est plébiscitée. Sa mission est déjà d'organiser les réponses aux victimes, hors du périmètre d'intervention de l'ANSSI (opérateurs d'importance vitale, opérateurs de services essentiels). Ainsi conforté, ACYMA pourrait coordonner les acteurs en région et adresser l'ensemble du territoire national. Il apparaît urgent de revoir la stratégie en cours sur les CSIRT afin de mieux employer les deniers publics et d'opter pour une organisation rationnelle et pérenne, susceptible de répondre à tous les acteurs qui ne relèvent pas de l'ANSSI, à l'image de l'organisation du Centre de crise et de soutien (CDCS) du ministère de l'Europe et des affaires étrangères.

Le Centre de réponse aux incidents cyber de Nouvelle Aquitaine

Locaux du CRIC de Nouvelle Aquitaine

Coordination régionale et interministérielle de cybersécurité

Constats :
- La mise en place des CSIRT régionaux s'est faite sur la base d'un volontariat des régions et selon un modèle assumé comme « expérimental » par l'ANSSI ;
- La pérennité du financement des CSIRT n'est pas assurée au-delà de l'amorçage du Plan de relance ;
- Les régions alertent sur le risque de devoir seule assumer la charge du dispositif alors qu'il s'agit d'une mission régalienne.

Recommandations :
- Rationnaliser l'organisation cyber vers un guichet unique pour orienter les victimes en cas d'attaque ou de conflit majeur ;

- Évaluer une organisation alternative aux CSIRT en concentrant les moyens publics sur le GIP ACYMA, tout en prévoyant une contractualisation État-Région pour les régions qui souhaitent pérenniser leurs centres de réponse ;
- Harmoniser, en collaboration avec le GIP ACYMA, les modalités d'appel des CSIRT régionaux et les services de cybersécurité rendus.

3. RENFORCEMENT DES CAPACITÉS DE DÉTECTION DE L'ANSSI

Le troisième point de contact entre ANSSI et LPM se matérialise par 4 articles normatifs au sein de la LPM :

- l'article 32 visent à demander aux opérateurs un filtrage des noms de domaine afin d'entraver une menace susceptible de porter atteinte à la sécurité nationale ;

- l'article 33 prévoit la transmission à l'ANSSI de données lui permettant d'identifier les serveurs et infrastructures des pirates informatiques ;

- l'article 34 vise à obliger les éditeurs de logiciels informatiques à informer l'ANSSI et les utilisateurs de tous incidents ou vulnérabilité de leur produit ;

- enfin, l'article 35 vise à renforcer les capacités de détection des cyberattaques en permettant à l'ANSSI l'accès au contenu des communications et à l'identité des victimes présumées de cyberattaques.

Cet accroissement très important des capacités de filtrage et de collecte de données par l'agence doit appeler à réaffirmer que les nouvelles méthodes de détections et de caractérisation des cyber attaques doivent impérativement être dissociées des méthodes de collecte et de traitement effectuées par les services de renseignement, ce que l'ANSSI n'est pas.
Les rapporteurs prennent acte de la garantie qui serait apportée par un contrôle a priori et a posteriori de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Cette garantie rendue par une autorité administrative indépendante doit être complétée par un contrôle du Parlement au moyen de la remise d'un rapport pour rendre compte de l'application de la mesure de filtrage des noms de domaine.

POUR EN SAVOIR +

• Examen du rapport d'information du groupe de travail (compte-rendu du 24 mai 2023)

Christian Cambon
Président de la commission
Sénateur du Val-de-Marne (LR)

Olivier Cadic
Rapporteur
Sénateur représentant les Français établis hors de France (UC)

Commission des affaires étrangères, de la défense et des forces armées
http://www.senat.fr/commission/etr/index.html

Lien vers le rapport :

Mickaël Vallet
Rapporteur
Sénateur de la Charente-Maritime (SER)