N° 638

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 24 mai 2023

RAPPORT D'INFORMATION

FAIT

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) pour une **coordination** *de la* **cyberdéfense** *plus* **offensive** *dans la loi de* **programmation militaire 2024-2030***,*

Par MM. Olivier CADIC et Mickaël VALLET,

Sénateurs

(1) Cette commission est composée de : M. Christian Cambon*, président ;* MM. Pascal Allizard, Olivier Cadic, Mme Marie-Arlette Carlotti, MM. Olivier Cigolotti, André Gattolin, Guillaume Gontard, Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Philippe Paul, Cédric Perrin, Rachid Temal*, vice-présidents ;* Mmes Hélène Conway-Mouret, Joëlle Garriaud-Maylam, Isabelle Raimond-Pavero, M. Hugues Saury*, secrétaires ;* MM. François Bonneau, Gilbert Bouchet, Alain Cazabonne, Pierre Charon, Édouard Courtial, Yves Détraigne, Mmes Catherine Dumas, Nicole Duranton, MM. Philippe Folliot, Bernard Fournier, Mme Sylvie Goy-Chavent, M. Jean-Pierre Grand, Mme Michelle Gréaume, MM. André Guiol, Ludovic Haye, Alain Houpert, Mme Gisèle Jourda, MM. Alain Joyandet, Jean-Louis Lagourgue, Ronan Le Gleut, Jacques Le Nay, Mme Vivette Lopez, MM. Jean-Jacques Panunzi, François Patriat, Gérard Poadja, Stéphane Ravier, Gilbert Roger, Bruno Sido, Jean-Marc Todeschini, Mickaël Vallet, André Vallini, Yannick Vaugrenard.

SOMMAIRE

Pages

L'ESSENTIEL

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

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

I. 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.

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 (GCA) à Saint-Jacques-de-la-Lande (35)

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.

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* » ou « *Joint WARfighting Cloud Contract*[1] » avec un consortium d'acteurs majeurs du numérique (Amazon, Google, Microsoft et Oracle) 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 (ou dans une proportion bien moindre et non exprimée dans le rapport annexé au projet de loi), 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.

[1] *Traduction : « confiance zéro » et « capacité de cloud de combat interarmées ».*

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[1] 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.

La DGA-MI a dressé un état de ses difficultés de recrutement eu égard aux profils recherchés, au « prix du marché » et à la concurrence sur les salaires que se livrent les services de l'État entre eux :

- *« Les activités métiers Cyber exercées à la DGA requièrent un haut niveau de technicité qui ne peut s'acquérir que dans la durée avec, pour certaines activités, le suivi d'une formation interne longue, prérequis pour pouvoir réaliser certaines tâches. Il faut compter environ deux ans pour que ces profils commencent à devenir autonomes, d'où un fort besoin de fidélisation des agents formés en poste.*
- *« Fort d'un même constat pour attirer les talents dans le domaine Cyber, d'autres services de l'état ont fait évoluer sensiblement leur grille de salaire pour continuer à être attractif par rapport au secteur privé. La DGA est de ce fait moins attractive que le privé mais également moins attractive que les autres services de l'état implantés dans les mêmes bassins d'emploi que la DGA. »*

[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 (ministère des armées - https://archives.defense.gouv.fr/portail/actualites2/fic-2021-florence-parly-annonce-le-recrutement-de-770-cyber-combattants-supplementaires-d-ici-a-2025.html)*

Pour la DGA, la fidélisation des agents en poste nécessiterait une évolution des rémunérations afin d'une part de minimiser les démissions pour des questions de salaire, d'autre part d'améliorer le recrutement de profils expérimentés. À cet effet, la direction interministérielle du numérique a élaboré un référentiel de rémunération des 56 métiers de la filière numérique et des systèmes d'information et de communication[1].

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.

Les rapporteurs ont vu l'intérêt de rapprocher un véritable écosystème autour du domaine de la cybersécurité au sein de la ville de Rennes. À l'image de ce qui a été observé à la Telekom Innovation Lab de la Ben-Gurion University de Beer-Sheva en Israël, il semble important de rapprocher le projet de pôle d'excellence autour de l'école Polytechnique de l'éco-système de Rennes, notamment en coordination avec l'installation, en 2025, de l'académie de la cyberdéfense dans de nouveaux bâtiments en construction pour le groupement de la cyberdéfense des armées (GCA). Celle-ci aura pour vocation de fédérer et de coordonner la formation des trois armes (terre, air et mer) et de la faire monter en gamme[2].

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.

[1] https://www.numerique.gouv.fr/uploads/note-referentiel-remuneration-filiere-numerique.pdf
[2] *Source : Ouest-France, 18 juillet 2023.*

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.

II. 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 €[1]	**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 (de 7 000 à 14 000 selon l'évaluation très large de l'ANSSI).

Outre les crédits annuels décrits ci-dessus, il faut signaler que, dans le cadre de la stratégie nationale cyber[2] lancée en 2021, **le plan « France**

[1] *Dont 4,9 millions d'euros pour la préparation des JO de Paris 2024.*

[2] *Cette stratégie s'inscrit dans le plan d'investissement France 2030 visant à tripler le chiffre d'affaires du secteur cyber et créer 37 000 emplois d'ici 2025. Le financement total de la stratégie*

Relance » a dédié une enveloppe spécifique de 136 millions d'euros à l'ANSSI pour renforcer la cybersécurité de l'État et des territoires sur la période 2021-2022. Ces crédits sont destinés à cofinancer des projets de sécurisation de systèmes d'information existants, à accompagner, sur le plan financier et méthodologique, la création de centres régionaux de réponse à des incidents cyber (CSIRT[1]) et, plus largement, à élever le niveau de cybersécurité des services de l'État, des collectivités territoriales et des établissements de santé.

Répartition du volet ANSSI du plan France Relance

- 60 M€ au profit des collectivités territoriales, via des parcours de cybersécurité, le co-financement de projets et le soutien à la création des CSIRT régionaux ;

- 25 M€ au profit du secteur de la santé pour la sécurisation des établissements de santé, du ministère et des organismes qui en dépendent ;

- 30 M€ au profit des ministères et organismes qui en dépendent, hors secteur de la santé, notamment via le co-financement de projets de sécurisation des réseaux de l'État ;

- 21M€ pour le développement et le déploiement mutualisé des capacités nationales de cybersécurité.

Source : ANSSI

Plusieurs réflexions sur la cybersécurité civile peuvent être formulées :

- Contrairement à la programmation militaire qui se projette sur les 7 prochaines années, il est difficile d'obtenir une visibilité des moyens du SGDSN au-delà d'une trajectoire triennale. De ce point de vue, le Plan France Relance contribue à donner de la visibilité à des investissements sur le temps long. Mais un suivi régulier s'impose concernant la pérennité financière des projets au-delà de la période d'amorçage du plan de relance (cf. infra concernant la pérennité des CSIRT régionaux) ;

- L'appui à l'ANSSI des moyens technologiques des armées représente un puissant atout pour la cybersécurité française en ce qu'elle bénéficie de l'expertise des laboratoires spécialisés de la DGA-MI. Ces synergies évitent ainsi les doublons. En revanche, si l'appui en ressources humaines militaires peut être déterminant lors d'une crise, celui-ci se limite à certaines opérations et à quelques dizaines de personnels. Ce constat ne peut donc exonérer le gouvernement d'une réflexion sur l'évolution des moyens propres de l'ANSSI pour véritablement répondre à une crise cyber majeure et un doublement, voire plus, des attaques ;

---

d'accélération cybersécurité serait composé de 1 milliard d'euros dont 720 millions d'euros de crédits publics (source : https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite#).

[1] Computer security incident response team

- Sur le plan national et territorial, le rôle et les moyens de l'ANSSI devront évoluer à la mesure des obligations que créera la transposition de la directive NIS 2 que la France doit mettre en œuvre avant la fin 2024. Dans le même temps, devront être clarifiées les missions respectives des régions (dispositif CSIRT) et du GIP ACYMA en charge du site « Cybermalveillance ».

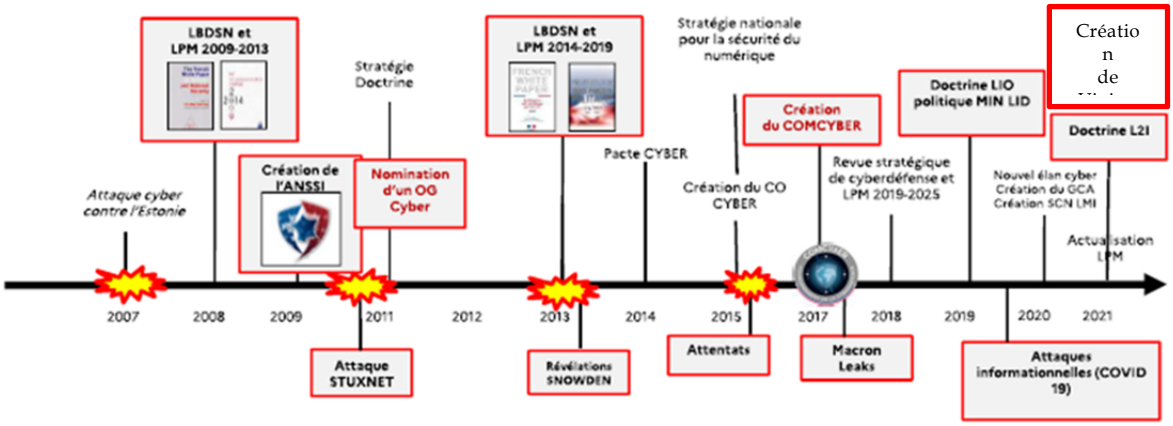
Constats :
- Les moyens de l'ANSSI devraient progresser de 660 personnels en 2023 à 800 en 2027 ;
- Il n'existe pas de trajectoire de programmation des moyens de cyberdéfense du SGDSN comparable dans le montant et la durée avec la LPM.

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



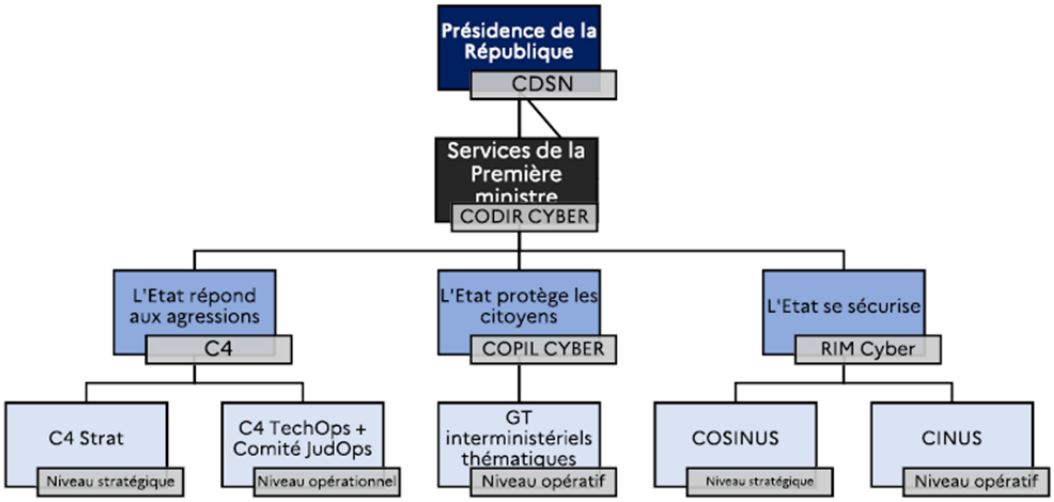
Source : ministère des armées, ComCyber

Le déplacement à Bruz, près de 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 équivalent 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** (cf. encadré ci-dessous). Cette « diplomatie de combat » est rendue possible grâce au travail de détection des campagnes étrangères de désinformation réalisé par Viginum. 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**.

Déclaration de Catherine Colonna - Ingérences numériques étrangères – Détection par la France d'une campagne de manipulation de l'information (13 juin 2023)

Les autorités françaises ont mis en évidence l'existence d'une campagne numérique de manipulation de l'information contre la France impliquant des acteurs russes et à laquelle des entités étatiques ou affiliées à l'État russe ont participé en amplifiant de fausses informations.

Cette campagne s'appuie notamment sur la création de fausses pages internet usurpant l'identité de médias nationaux et de sites gouvernementaux ainsi que sur la création de faux comptes sur les réseaux sociaux.

VIGINUM a été en mesure de détecter cette campagne en amont, ce qui a permis aux autorités françaises compétentes de prendre des mesures de protection et de prévention. Les autres démarches techniques pertinentes sont en cours. Le ministère de l'Europe et des Affaires étrangères a notamment déjoué une tentative d'usurpation d'identité sur son site internet (www.diplomatie.gouv.fr/).

Les investigations conduites par VIGINUM ont permis de mettre en évidence de nombreux éléments révélant l'implication d'individus russes ou russophones et de plusieurs sociétés russe dans la réalisation et la conduite de la campagne. VIGINUM a également observé que plusieurs entités étatiques ou affiliées à l'État russe avaient participé à la diffusion de certains contenus produits dans le cadre de la campagne.

Une synthèse des investigations réalisées par VIGINUM est disponible sur les sites de France Diplomatie et du Secrétariat Général à la Défense et la Sécurité Nationale (SGDSN)[1].

L'implication d'ambassades et de centres culturels russes qui ont activement participé à l'amplification de cette campagne, y compris via leurs comptes institutionnels sur les réseaux sociaux, est une nouvelle illustration de la stratégie hybride que la Russie met en œuvre pour saper les conditions d'un débat démocratique apaisé et donc porter atteinte à nos institutions démocratiques.

La France condamne ces agissements indignes d'un membre permanent du Conseil de sécurité des Nations Unies. Aucune tentative de manipulation ne détournera la France du soutien qu'elle apporte à l'Ukraine face à la guerre d'agression russe.

Les autorités françaises travaillent en lien étroit avec leurs partenaires afin de mettre en échec la guerre hybride menée par la Russie.

Source : ministère de l'Europe et des affaires européennes

Lors des différentes auditions, les rapporteurs ont eu du mal à apprécier la méthode retenue pour **évaluer la qualité des actions engagées** et si un processus d'amélioration continue était activé pour que l'ensemble des structures fonctionnent harmonieusement et efficacement.

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.

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

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[1]), 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 ;

- **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.

Visite du centre de réponse aux incidents cyber (CRIC) de Nouvelle Aquitaine

Locaux du CRIC de Nouvelle Aquitaine

Coordination régionale et interministérielle de cybersécurité

[1] *Traduction privilégiée par vos rapporteurs : centre de réponse aux incidents cyber (CRIC)*

Fonctionnement du CRIC de Nouvelle-Aquitaine

Créé en mai 2023, le centre de réponse aux incidents cyber (CRIC)[1] de Nouvelle-Aquitaine s'articule entre l'ANSSI et le GIP ACYMA :

- ANSSI : rôle de pilotage national (autorité de cybersécurité), en charge de la réponse à incident sur le périmètre des OIV et Entités essentielles (NIS 2) ;

- CSIRT : en charge de la réponse à incident sur le périmètre des entités importantes, PME et collectivités de plus de 20 000 habitants, de l'accompagnement à la montée en compétence des prestataires, de l'animation territoriale sur le sujet cyber (développer la résilience des entreprises et collectivités) ;

- ACYMA : en charge du 17 cyber, de la réponse à incident sur le périmètre des particuliers, TPE et collectivités de moins de 20 000 habitants, de la labellisation des prestataires et de l'orientation des victimes (vers ANSSI / CSIRT / eux-même).

Depuis sa création, le CRIC a répondu à 28 attaques : 1/3 de rançongiciels, fraudes, violation de données et piratage de compte. Malgré la concentration des acteurs économiques en Gironde, les incidents sont à peu près répartis sur toute la région (tous secteurs et toutes tailles d'entreprises). Le centre lui-même a fait l'objet de 2 000 attaques contre lesquelles il dispose de protection.

Source : Campus Cyber Nouvelle-Aquitaine

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).

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 (cf. le cas de la région Auvergne-Rhône-Alpe qui ne participe pas au dispositif des CSIRT régionaux) et fait apparaître de nombreuses faiblesses à commencer par les interrogations sur sa pérennité.

[1] *Appellation du CSIRT de Nouvelle-Aquitaine.*

Pour les rapporteurs, **le principe du numéro d'appel universel tel que le « 17 cyber » serait à privilégier** en cas d'attaque cyber.

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.

Une clarification des rôles s'impose, entre ANSSI, CSIRT régionaux ou sectoriels et GIP ACYMA, notamment dans la perspective de l'application de la directive NIS 2 et ne serait-ce que pour désigner un interlocuteur dans la région qui n'a pas souhaité rejoindre le dispositif du plan France Relance. **Un équilibre doit être trouvé afin d'une part de ne pas freiner, ne serait-ce que partiellement, le déploiement des CSIRT décidé par la plupart des régions, d'autre part de conforter le rôle du GIP ACYMA.** Aussi bien en Bretagne qu'en Nouvelle-Aquitaine, la territorialisation des CSIRT est un outil de montée en compétence les prestataires locaux mais aussi de protection du tissu économique et de formation dans le domaine cyber.

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 « 17 cyber » 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 coordination avec le GIP ACYMA, les modalités d'appel des CSIRT régionaux et les services de cybersécurité rendus.

III. UN RENFORCEMENT DES CAPACITÉS DE DÉTECTION DE L'ANSSI QUI APPELLE UN CONTRÔLE ACCRU DU PARLEMENT

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

- l'article 32 vise 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.

EXAMEN EN COMMISSION

Réunie le mercredi 24 mai 2023, sous la présidence de M. Christian Cambon, président, la commission des affaires étrangères, de la défense et des forces armées a procédé à l'examen du rapport d'information du groupe de travail sur le programme 129 « Coordination du travail gouvernemental » (action 2 : Coordination de la sécurité et de la défense, SGDSN, Cyberdéfense), dans la perspective de la loi de programmation militaire (MM. Olivier Cadic et Mickaël Vallet, rapporteurs).

M. Christian Cambon, président. - Nous examinons ce matin les conclusions de nos rapporteurs du groupe de travail sur le programme 129 « Coordination du travail gouvernemental », dans la perspective de la loi de programmation militaire (LPM).

M. Olivier Cadic. - Mes chers collègues, le programme 129 que je rapporte avec mon collègue Mickaël Vallet sur la coordination de la sécurité et de la défense relève de la mission « Direction de l'action du Gouvernement », c'est-à-dire les services de la Première ministre, et non de la mission « Défense ».

Nous y examinons chaque année en loi de finances le budget du Secrétariat général de la défense et de la sécurité nationale (SGDSN) dont relèvent notamment l'agence nationale de sécurité des systèmes d'information (ANSSI).

Ce programme comporte toutefois plusieurs liens avec la LPM en cours d'examen et je remercie le Président de la commission d'avoir bien voulu renouveler la mise en place d'un groupe de travail sur le thème de la coordination de la cyberdéfense, comme pour la LPM précédente.

Je remercie André Gattolin d'avoir rejoint et contribué aux travaux du groupe.

« *Il va falloir être plus connectés et moins vulnérables* », a dit Eric Trappier, Président de Dassault aviation, ce matin. Cet objectif guide nos réflexions.

Quels sont ces points de contact entre l'ANSSI et la LPM ?

En premier lieu, la résilience cyber a été érigée en objectif stratégique par la Revue nationale stratégique et le Président de la République a annoncé dans son discours sur la LPM son souhait de voir doubler notre capacité de traitement des attaques cyber majeures.

À notre sens, cet objectif ne peut s'inscrire que dans une coordination entre les milieux civils et militaires, le public et le privé, le national et le local.

S'y ajoute un enjeu de coordination entre le bouclier (la lutte informatique défensive) et le glaive (la lutte informatique offensive) qui caractérise la dichotomie du dispositif français :

- avec d'une part la compétence de l'ANSSI sur le volet défensif des réseaux interministériels, des opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE) au nombre desquels figurent par exemple 142 centre hospitaliers ;

- et d'autre part la compétence de lutte informatique offensive dont l'existence est reconnue mais dont les acteurs et les moyens relèvent du ministère des armées et donc *in fine* du Président de la République si une action devait être déclenchée.

On se demande d'ailleurs si le seul objectif de doublement de capacité est suffisant quand on sait la progression exponentielle des menaces répertoriées par l'ANSSI (831 intrusions avérées) et Cybermalveillance (plus de 170 000 demandes d'assistance dont plus de 90 % émanent de collectivités territoriales).

Sur le volet militaire de la lutte informatique défensive (LID), le commandement de la cyberdéfense (COMCYBER) a traité en une année 150 événements de sécurité numérique touchant au périmètre du ministère des armées (hors services de renseignements).

Le second point de contact a trait à la coordination civilo-militaire entre ANSSI d'une part et le COMCYBER, la DGA-MI, (Délégation générale à l'armement « maîtrise de l'information ») et la DGSE d'autre part.

Le groupe de travail s'est rendu à Rennes à la rencontre du Pôle d'excellence cyber et dans les locaux du ComCyber et de la DGA-MI. Il nous y a été relaté la relation très directe et quasi quotidienne entre l'ANSSI et la DGA-MI cette dernière apportant son expertise technique dans le traitement des données et la conception de programmes dédiés.

Comment véritablement inscrire dans la prochaine LPM la nécessité de rapprocher les fonctions défensives et offensives (qui sont traditionnellement et structurellement séparées dans notre organisation actuelle) pour que la défense de nos intérêts soit mieux intégrée, notamment entre l'ANSSI pour le volet civil (en métropole et dans les outre-mer) et le ComCyber pour le volet militaire?

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

- l'article 32 vise 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 infrastructure 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.

J'attire votre vigilance sur ces articles qui soulèveront certainement un débat sur la question de l'accès aux contenus des communications, alors que jusqu'à présent le leitmotiv de l'ANSSI était de n'accéder qu'aux réseaux, c'est-à-dire les contenants, voire aux métadonnées, mais pas aux contenus proprement-dit.

On pourra s'interroger sur la compétence de l'Autorité des communications électroniques, des postes et de la distribution de la presse (ARCEP) en tant qu'autorité de contrôle *a priori* sur les avis autorisant l'accès aux données de contenu.

Alors même que le projet de loi propose la suppression de l'assermentation judiciaire des agents de l'ANSSI, celle-ci emploierait des techniques d'accès au contenu jusqu'alors réservées aux services de renseignement, ce que l'agence n'est pas.

S'agissant du financement, le rapport annexé à la LPM prévoit 4 milliards d'euros de besoins programmés pour la cyberdéfense afin d'augmenter les effectifs, de s'adapter aux évolutions technologiques, d'accompagner les entreprises du secteur de la défense et d'appuyer l'ANSSI en cas de crise cyber nationale.

Il faut rappeler que le ComCyber est susceptible de mettre à disposition quelques cybercombattants pour soutenir directement l'ANSSI, mais pas dans des proportions annoncées pour faire face à un doublement des cyberattaques.

Cela pose la question de la cible d'augmentation des effectifs pour la période 2024-2030 : le ministre des armées a annoncé une hausse de 953 ETP pour le seul ministère des armées répartis entre la DGSE, la DGA et les armées. C'est moins que les 1 500 postes prévus dans le domaine cyber pour la LPM 2019-2025.

J'en viens maintenant à quelques observations assorties de propositions :

Ainsi que le ministre des armées l'a précisé lors de son audition, aucun des 4 milliards de crédit de la LPM n'est destiné à l'ANSSI. La LPM ne vise aucunement à financer le passage de l'ANSSI de 660 agents en 2023 à 800 agents en 2027. Cette augmentation sera financée par le budget du SGDSN.

Une question se pose de savoir si ces 4 milliards d'euros seront principalement fléchés vers la DGSE, la DGA-MI et le COMCYBER, en partie dans le but de pouvoir davantage contribuer à l'action défensive. La raison serait d'organiser l'emploi des ressources publiques et privées en cas de dépassement des capacités de l'État à faire face à une crise cyber d'ampleur. Mais alors pourquoi ne serait-ce pas à l'ANSSI, au lieu de l'armée, de monter davantage en puissance afin de coordonner directement les capacités cyberdéfensives publiques et privées du pays pour faire face à la massification des attaques ?

Enfin, je souhaite formuler deux observations plus générales sur les stratégies de réponse. S'il existe bien une comitologie de niveau stratégique (le C4 strat est mensuel) et opérationnel (le C4 TechOps est quasi quotidien), on peut s'interroger sur les conditions de contrôle de l'efficience globale du dispositif.

Ensuite, je ne partage pas, et d'autres pays alliés non plus, la stratégie de la revue nationale stratégique selon laquelle, je cite, « *l'application d'une logique dissuasive dans le cyberespace qui forcerait tout attaquant à la retenue contre la France est illusoire* ».

Comme l'a dit le Président de la République, le 9 novembre 2023, je cite, « *une attitude qui serait seulement réactive, voire défensive, pourrait passer pour une forme de passivité* ».

Voilà pourquoi je pense qu'il faut absolument faire évoluer l'action de l'ANSSI vers un rôle plus offensif, *a minima* plus proactif, ainsi que le prévoient certains des articles de la LPM.

M. Mickaël Vallet. - Mes chers collègues, je partage le constat sur la massification des attaques qui conduit l'ANSSI à devoir protéger les collectivités et les entreprises qui auparavant ne se trouvaient pas dans son périmètre de compétence. La part des incidents affectant le secteur de la santé n'a cessé d'augmenter en métropole comme en Outre-mer avec plus de 400 incidents depuis 2020. Au début de l'année 2023, c'était au tour de l'hôpital de la Réunion de détecter des « compromissions d'importance », traitées par les CERT Santé et CERT-FR national qui est l'équipe de réaction aux incidents cyber de niveau gouvernemental. Je précise que le CERT signifie « Computer Emergency Response Team », que la dénomination officielle française est centre gouvernemental de veille et de réponses aux attaques informatiques. C'est cette définition française que nous privilégierons dans nos rapports. Le sigle est formulé en anglais du fait des directives européennes.

Comme j'ai pu le constater avec Olivier Cadic, lors de la venue d'une délégation du Monténégro au Sénat, celle-ci nous avait décrit la paralysie dans laquelle s'étaient trouvés tous les ministères du pays suite à une cyberattaque. L'Albanie a fait l'objet elle aussi d'une attaque étatique, attribuée à l'Iran, en juillet 2022. Il faut conserver à l'esprit que personne

n'est à l'abri pas même l'Assemblée nationale et le Sénat qui peuvent être pris pour cible par des attaques.

L'enjeu de la coordination de la cyberdéfense n'est pas que celui des attaques, il est aussi celui de la définition et de la typologie des entreprises à protéger. La directive dite « NIS 2 » aura pour effet au niveau européen de considérablement ouvrir le champ des entreprises assujetties à des obligations de cybersécurité. Comme pour la sécurité incendie, il y a des tailles d'entreprises et des niveaux d'obligations différents selon d'un immeuble reçoit du public ou non. De quelques centaines d'acteurs à réguler, l'ANSSI prévoit une multiplication par 20, soit près de 15 000 entreprises.

C'est une des raisons ayant conduit l'agence à susciter la création dans chaque région d'un CSIRT (Computer security incident response team) - que nous pourrons appeler « centre de réponse aux incidents de cybersécurité » (CRIC) - afin de prendre en charge les entreprises qui entreront dans les critères de seuil les assujettissant aux obligations de cette directive NIS 2. Le plan de relance a prévu une enveloppe de 12 millions d'euros répartis entre 12 CSIRT régionaux, à l'exception de la région Auvergne-Rhône-Alpe. Nous y reviendrons plus loin.

Ces dispositifs, contractualisés en 2021 dans le cadre du plan de Relance, sont entrés progressivement en oeuvre après 2 années consacrées à la création des structures par les régions, l'embauche d'experts - ou la débauche 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 « CRIC » venait d'entrer en service en avril 2023 avec d'abord 2 ingénieurs puis un troisième par ailleurs ancien agent de l'ANSSI. Plusieurs remarques :

- la création de ces centres, qui remplissent localement des missions régaliennes qui leur sont confiées par l'ANSSI, nécessite un portage politique important (au titre de la compétence développement économique des régions) alors même que la pérennité de la ressource n'est pas assurée ;

- après la consommation des crédits du Plan de relance (1 million d'euros de démarrage par région), le risque est grand de voir toute la charge reposer sur des conseils régionaux qui n'ont pas vraiment l'obligation de poursuivre dans cette démarche. C'est ce qui se passe en Nouvelle Aquitaine pour un budget de 650 000 euros, le reste étant constitué d'apport des entreprises partenaires de ce Campus. Ce point nous a éclairé sur les raisons du refus de la région Auvergne-Rhône-Alpe de se lancer dans cette démarche car nous pouvons comprendre qu'une collectivité, ne voyant pas assuré sur le très long terme une mission qui n'entre pas forcément dans ses compétences, ne souhaite s'engager en toute confiance ;

- en tout état de cause les élus régionaux que nous avons rencontrés se sont malgré tout montré allants sur la création de leurs CSIRT respectifs (Bretagne et Nouvelle Aquitaine) mais ils appellent d'urgence à penser dès

maintenant l'après Plan de Relance, soit par le biais d'un plan État-Région, soit, et c'est plus original, au moyen d'un modèle de type SPL (société publique locale) qui générerait des ressources financières, comme une SPL de télécommunication, pour assurer le financement d'un CSIRT. La piste de la constitution de groupement d'intérêt public (GIP) a également été évoquée. Cela pose toutefois la question d'un transfert de compétences régaliennes à des collectivités territoriales ;

- cette question ne s'éloigne pas du sujet de la LPM dans la mesure où l'objectif 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 cybersécurité 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 qu'une association « Inter-CERT » serait créée pour constituer une 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'information aux réseaux consulaires et organisations professionnelles. On est encore loin du principe du numéro d'appel universel tel que le 18 ou le 112 sur les questions cyber.

Enfin, pour conclure ces observations sur la question des campus cyber en région, de la création récente du Campus Cyber national à Puteaux, ou d'autres initiatives qui se font jour, le rapport annexé de la LPM prévoit la création d'un nouveau pôle d'excellence structuré autour de l'Ecole polytechnique au bénéfice des armées. Ce sur quoi nous alertons, c'est qu'il ne faudrait pas que la multiplication des pôles d'excellence ou des campus cyber conduise à l'effet inverse de celui recherché qui était de mettre dans un même lieu des acteurs du cyber de tous horizons et non de multiplier les locaux, disperser les acteurs et saupoudrer les moyens.

J'ajoute un point sur ce qu'a évoqué Olivier Cadic et soulevé Yannick Vaugrenard, c'est la question des recrutements. Nous sommes dans un domaine ou des États étrangers recrutent des ingénieurs comme on recrute des joueurs de football en allant prospecter dans les écoles, et même en ciblant dès le collège pour identifier des talents. Cette rareté de la ressource est aggravée par le fait que les structures publiques se trouvent en situation de concurrence entre-elles, avec des grilles de rémunérations très diverses. Les débauchages mutuels conduisent à des effets contreproductifs sur lesquels il convient de s'interroger.

M. André Gattolin. - Je salue le travail des deux rapporteurs que j'ai eu l'occasion d'accompagner lors de la visite de la DGA-MI et du Comcyber à Rennes. Nous avons été impressionnés par les moyens mis en oeuvre et les capacités techniques de ces unités.

Je voudrais formuler une remarque valable pour les deux programmes, 129 et 144. Notre doctrine évolue sur la séparation dans le domaine cyber entre le défensif et l'offensif, cette distinction étant illusoire dans le contexte actuel. Le problème fondamental lorsque l'on passe du défensif à l'offensif est celui d'avoir une doctrine. Il faut savoir ce que l'on veut faire. Il faut le penser et le faire dans le cadre de l'État de droit. Et ce cadre, nous ne l'avons pas.

Nous sommes très bons pour nous occuper des tuyaux et des technologies. Mais quand il s'agit d'agir, dans le domaine de l'influence, nous sommes assez mauvais dans la construction des discours et des narratifs. Le contre-narratif est laissé au ministère des affaires européennes et étrangères. Nous devons définir si nous nous autorisons, face à la désinformation, nous aussi la divulgation de fausses informations. Cela paraît compliqué pour un État de droit.

En revanche, quel discours tenons-nous. Notre problème repose sur un désarmement intellectuel de l'État. On lance beaucoup d'études et on crée un observatoire des ingérences étrangères mais on n'en définit pas le périmètre. C'est notre rôle de parlementaire que d'alerter sur la nécessité d'une approche plus inclusive notamment à l'égard du monde de la rechercher pour conduire des travaux duaux, c'est-à-dire à double usages, surtout si nous voulons construire une pensée et une doctrine, au-delà des seuls aspects techniques. Il faut aussi définir quels sont les ennemis ou les ennemis potentiels.

Cela nécessite davantage de coordination et c'est à mon sens essentiel pour les années à venir.

Mme Hélène Conway-Mouret. - Merci pour ce rapport qui pose les bonnes questions et qui va au fond des sujets. Ma question s'adresse à Olivier Cadic pour savoir si les observations formulées sont personnelles ou collectives, les co-rapporteurs pouvant ne pas être sur la même ligne, et si l'intention est de traduire les propositions en amendements à la LPM ?

M. Olivier Cadic. - Nous travaillons en bonne intelligence, ce qui ne veut pas dire que nous pensons pareil sur tout, et il est important de pouvoir exprimer des nuances personnelles. D'ailleurs, Mickaël Vallet a exprimé des constats qui lui sont propres, mais que je partage et prends à mon compte.

M. Mickaël Vallet. - Par exemple sur la question du rôle de l'ANSSI, de l'ARCEP et de la fin de l'assermentation judiciaire de certains agents, nous avons fait une présentation factuelle de ces points d'attention car il est possible que dans les débats, des amendements viennent modifier des seuils d'alerte avant que le texte ne soit transmis au Sénat. Nous souhaitions pointer du doigt des évolutions notables du droit existant.

M. Christian Cambon, président. - Je note la pertinence de la méthode que nous avons utilisée en confiant à des parlementaires la préparation de la discussion de la LPM, chacun dans son secteur de

compétence, au lieu de se fondre dans les groupes de travail qui nous étaient proposés par le gouvernement et dont aucune proposition, à part peut-être pour la condition militaire, n'est véritablement sortie.

Les recommandations sont adoptées.

La commission adopte, à l'unanimité, le rapport d'information et en autorise la publication.

PERSONNES AUDITIONNÉES ET DÉPLACEMENTS

Personnes auditionnées :

- **M. Vincent Strubel**, directeur général de l'agence nationale de sécurité des systèmes d'information (ANSSI), **M. Benjamin Delannoy**, conseiller juridique (SGDSN), **Mme Julie Holveck**, conseillère judiciaire (SGDSN) et **M. Gwénaël Jézéquel**, conseiller pour les relations institutionnelles (SGDSN) ;

- **Vice-amiral Arnaud Coustillière**, président du Pôle d'excellence cyber de Rennes ;

- **M. Philip M. Stupak**, directeur fédéral de la cybersécurité des Etats-Unis ;

- **Mme Blandine Eggrickx**, responsable des affaires publiques d'OVH ;

- **M. Frédéric Géraud**, directeur des affaires publiques de Google Cloud, et **M. Thiébaut Meyer**, directeur cybersécurité de Google Cloud.

Déplacements :

- **Pôle d'excellence cyber, groupement de la cyberdéfense des armées, Délégation générale à l'armement – Maîtrise de l'information (DGA-MI), ANSSI** (Bruz et Rennes, 9 mai 2023) :

  - **IGA Lionel Morin**, directeur de la DGA-MI, **M. Frédéric Maurel**, adjoint au sous-directeur du domaine CYBER 2, et les équipes des services et laboratoires spécialisés ;

  - **M. Jérôme Tré-Hardy**, conseiller régional délégué à la cybersécurité et la transition numérique

  - **Mme Gwenaëlle Martinet**, conseillère auprès du directeur général de l'ANSSI, en charge de l'installation à Rennes ;

  - **CV Vincent Sébastien,** Chef d'état-major du commandement de la cyberdéfense, et **Colonel Pierre-Arnaud Borrelly,** commandant le groupement de la cyberdéfense des Armées.

- **Campus Cyber Nouvelle-Aquitaine** (Pessac, 12 mai 2023) :

  - **M. Mathieu Hazouard**, conseiller régional délégué aux enjeux numériques, président du Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine ;

  - **M. Guy Flament**, directeur du Campus Cyber Nouvelle-Aquitaine ;

- **M. Thibault Chenevière**, adjoint au Maire de Pau en charge du commerce et du numérique, responsable du département veille et cybersécurité de la CCI Pau Béarn ;
- **M. Martin Veron**, Délégué régional ANSSI ;
- **M. Paul Bousquet**, commissaire divisionnaire, chef de la division de lutte contre la criminalité financière à la DZPJ Sud-Ouest ;
- **M. Ludovic Boncompain**, Lieutenant-Colonel, officier sécurité des systèmes d'information, référent région zonale de nouvelle Aquitaine cyber sécurité ;
- **Mme Karine Amieva-Camos**, Déléguée à l'information stratégique et à la sécurité économiques du ministère de l'économie, des finances et de la souveraineté industrielle et numérique ;
- **Mme Eléna Poincet**, fondatrice et CEO de la société spécialisée en cybersécurité TEHTRIS ;
- **M. Michaël Ferrec,** co-fondateur de la société de sauvegarde informatique INSPEERE ;
- **M. Damien Lescos**, fondateur de la société de cybersécurité SITINCLOUD.