…l'avis de la commission sur le projet de loi de finances pour 2023

DOTER LA STRATÉGIE DE CYBERDÉFENSE ET D'INFLUENCE D'UNE COMPOSANTE OFFENSIVE

Rapport pour avis de MM. Olivier CADIC et Mickaël VALLET sur les crédits de l'action n° 2 « Coordination de la sécurité et de la défense » du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

Les menaces de cybersécurité croissent suivant un rythme exponentiel *(173 000 demandes d'assistance en 2021 sur le site cybermalveillance.gouv.fr et 1082 signalements d'incidents traités par l'ANSSI)* ***sans que l'augmentation des moyens humains (+61 ETP) et budgétaires (+9 M€) du SGDSN ne semble pouvoir en ralentir la course****.*

Des attaques très graves ont perturbé les services publics, collectivités territoriales et établissements de santé. *Le rapport apporte des éléments sur les préjudices subis, financiers mais aussi humains, qui peuvent aller jusqu'à atteindre la sécurité nationale.*

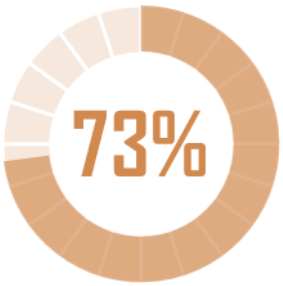
Le rapport revient sur la première année de fonctionnement de ***VIGINUM*** *et salue la création du* ***Campus Cyber*** *qui offre l'opportunité de créer un écosystème public-privé de cybersécurité. Par ailleurs, le rapport souligne des points de vigilance sur la sécurité du tissu économique et social dans les* ***régions*** *ainsi que la nécessité absolue de faire monter en gamme la sécurité informatique et la résilience du système de santé dans les* ***Outre-mer****.*

Enfin, il propose d'intégrer dans la stratégie de cyberdéfense une ***composante offensive*** *dans l'esprit de la nouvelle fonction stratégique d'influence prévue par la revue nationale stratégique.*

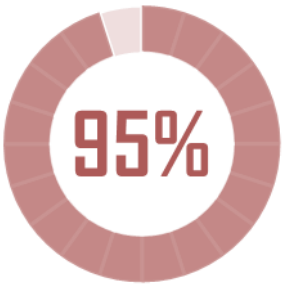
Le mercredi 16 novembre 2022, sous la présidence de M. Christian Cambon, président, la commission a émis un avis favorable à l'adoption des crédits relatifs à l'action n° 2 du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

1. LES MENACES CROISSENT PLUS VITE QUE LES MOYENS

A. LE TABLEAU DE BORD ANNUEL DES ATTAQUES CYBER : DES MENACES PLUS NOMBREUSES, PLUS DIVERSIFIÉES ET PLUS PRÉJUDICIABLES



État et administrations : l'ANSSI a traité 222 incidents cyber affectant des ministères en 2021 ; c'est 73 % de plus qu'en 2020



Entreprises : en hausse de 95 % en 2021, les rançongiciels sont la première menace pour les professionnels

Grand public : 2,5 millions de visiteurs et 173 000 demandes d'assistance en 2021sur le site *cybermalveillance.gouv.fr*

La cyber menace n'évolue pas dans le bon sens et le SGDSN qualifie sa **croissance d'exponentielle** dans trois domaines particulièrement préoccupants : le secteur criminel, l'activité d'espionnage et l'action militaire.

Dans le domaine spécifique de compétence de l'ANSSI en matière de supervision de la sécurité des systèmes d'information de l'État, **222 incidents cyber ont affecté des ministères, soit une progression de 73 % par rapport à 2020** (128 incidents). Il s'agit d'un quasi triplement en deux ans, rapporté aux 81 incidents traités en 2019.

Si la plupart de ces incidents ont pu se révéler mineurs pour 200 d'entre eux (dont 179 compromissions de comptes de messagerie), 22 attaques ont nécessité l'expertise et l'engagement de l'ANSSI, y compris 5 opérations de cyberdéfense concernant des incidents majeurs de sécurité sur des organisations d'importance vitale (OIV).

Tableau des cyber incidents par ministère traités par l'ANSSI

Ministères	Nombre d'incidents traités par l'ANSSI			Commentaires
	2019	2020	2021	
Ministère de l'agriculture et de l'alimentation	8	14	3	Dont une opération de cyberdéfense
Ministère de la cohésion des territoires	0	2	2	
Ministère de la culture	6	11	10	
Ministère des armées	22	4	5	
Ministère de l'économie des finances et de la relance	11	18	24	Dont une opération de cyberdéfense
Ministère de l'éducation nationale, de la jeunesse et des sports	22	58	149	Dont 144 compromissions de comptes de messagerie
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	1	3	0	
Ministère de l'Europe et des affaires étrangères	14	14	10	Dont 4 opérations de cyberdéfense et un incident majeur
Ministère de l'intérieur *et des outre mer**	14	13	11	
Ministère de la justice	6	4	4	Dont un incident majeur
Ministère des outre-mer	1	2	*	* regroupé avec le chiffrage du ministère de l'intérieur
Ministère de la santé et des préventions	3	14	6	
Ministère de la transition écologique	8	18	12	Dont 2 opérations de cyberdéfense
Ministère du travail, de l'emploi et de l'insertion	7	6	1	

Source : réponse au questionnaire budgétaire

Le seul tableau de bord des attaques de la sphère des ministères ne suffit pas à retracer l'ampleur du phénomène :

- Plus largement, en intégrant l'élargissement de sa mission de pilotage de la sécurité des opérateurs de services essentiels (OSE) et des collectivités territoriales au titre du plan France Relance 2021-2022, l'ANSSI a reçu **1 082 signalements en 2021**, contre 786 l'année précédente, soit une hausse de 37 % ;

- S'agissant de la **cybercriminalité, avec 1 945 demandes d'assistance** à la plateforme cybermalveillance.gouv.fr, contre 996 l'année précédente, **les rançongiciels sont la première menace pour les professionnels (entreprises, associations et collectivités) avec une hausse de 95 % des attaques**, l'Anssi s'étant impliquée sur à peu près 200 opérations ;

- Les **affaires d'espionnage** peuvent sembler modestes en nombre, mais il faut noter que **14 opérations en 2021, dont 9 pouvant être attribuées à des modes opératoires d'origine chinoise, ont nécessité une intervention massive de l'ANSSI** avec le support de partenaires et de prestataires privés (la lutte contre l'espionnage représente 80 % de l'activité de l'Anssi) ;

- Sur le **volet militaire**, le commandement de la cyberdéfense (COMCYBER) a traité **150 événements de sécurité numérique touchant au périmètre du ministère des armées** (hors services de renseignements).

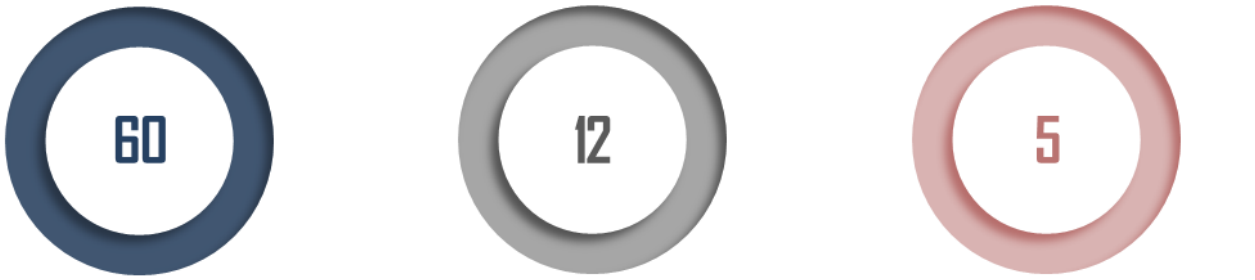
Il convient également de ne pas ignorer **le caractère massif que la menace cyber fait planer sur la population** dans son ensemble. La stratégie nationale pour la sécurité du numérique de 2015 a confié au groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA) une mission de sensibilisation, de prévention et d'assistance aux victimes d'attaques pour les particuliers, les entreprises et les collectivités territoriales. **La plateforme en ligne *cybermalveillance.gouv.fr***, créée en 2017, constitue un baromètre utile de l'état des principales menaces :

- **2,5 millions de visiteurs en 2021**, soit 101 % de plus en un an ;

- **173 000 demandes d'assistance** émanent dans 94 % des cas de collectivités territoriales, 3 % de particuliers et 3 % d'entreprises ;

- **Les grandes menaces sont l'hameçonnage, le piratage de compte et le rançongiciel** (50 % des demandes d'assistance des particuliers concernent le hameçonnage et le piratage de comptes, 42 % des demandes des entreprises concernent les rançongiciels et le piratage de compte, tandis que les collectivités recherchent une assistance dans 36 % des cas concernant le rançongiciel et l'hameçonnage).

Enfin, le nouveau service de l'État chargé depuis juillet 2021 de la **vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM)** a dressé un bilan de sa première année d'activité. Dans le cadre de la protection du débat public numérique touchant aux élections présidentielle et législatives de 2022, **VIGINUM a détecté** :



phénomènes inauthentiques sur les plateformes numériques

ont fait l'objet d'investigations approfondies

ont été caractérisés comme une ingérence numérique étrangère

Mais au-delà du constat que fait-on ? Aucun chiffrage des préjudices causés, des arrestations ou entraves aux activités des cybercriminels n'est disponible.

La réalité qui se cache derrière la progression exponentielle des chiffres de la menace cyber, n'est autre que l'extrême rentabilité du cybercrime pour des organisations, voire des États qui allient appât du gain et guerre hybride contre des cibles (OIV, OSE, hôpitaux, infrastructures de transport ou énergétiques, etc.) pouvant porter atteinte à la sécurité nationale. Quelques repères permettent de prendre la mesure de certains préjudices, lesquels ne sont pas tous d'ordre financier :

- Lorsque le système informatique de **l'hôpital de Corbeil-Essonnes** s'est trouvé paralysé par une attaque au rançongiciel perpétré par l'organisation criminelle russophone *Lockbit* réclamant 10 millions d'euros, le véritable préjudice ne s'évalue pas

par le coût d'une rançon qu'un établissement hospitalier public est dans l'incapacité de payer, mais, dans un premier temps, par la paralysie de tout l'hôpital, le reversement des patients vers d'autres établissements, avec le risque de perte de chance thérapeutique que cela implique (**ce risque serait majeur dans le cas d'un tel événement outre-mer, sans possibilité de transfert des patients**), puis le coût de la lutte contre la cyberattaque et la reconfiguration de tout le système informatique (estimées respectivement à 2 M€ et 5 M€ par l'hôpital de Corbeil-Essonnes). La multiplication des attaques contre le système de santé illustre d'une part leur caractère aveugle et peu rentable mais d'autre part, elle met en évidence une menace sur un intérêt vital touchant potentiellement à la sécurité nationale ;

- En revanche, l'aspect financier de la cybercriminalité prend toute sa mesure lorsqu'elle s'attaque aux entreprises quel qu'en soit le montant. En 2021, un rançongiciel a touché plusieurs multinationales françaises, avec des demandes de rançon allant de 5 à 70 millions de dollars. Une PME ou TPE peut voir son système informatique crypté et rendu inutilisable sauf à ce qu'une rançon de quelques centaines ou milliers d'euros ne soit versée. Il est impossible d'estimer le nombre et le coût global des rançons effectivement payées, l'ANSSI laissant entendre que le cas est fréquent, en témoigne la mesure prévue par l'article 4 du projet de loi d'orientation et de programmation du ministère de l'intérieur visant, en cas d'attaque au rançongiciel, de conditionner la possibilité, pour une victime, d'être indemnisée par son assureur au dépôt d'une plainte au plus tard 48 heures après le paiement de la rançon. Ce dispositif qui tend à légitimer le remboursement d'une rançon entre en contradiction avec **le message de l'ANSSI de ne pas payer de rançon pour ne pas financer la cybercriminalité**. Cela suppose que pour se prémunir du paiement d'une rançon, l'entreprise ait au préalable mis en œuvre les mesures de sécurité nécessaires et qu'elle ait bien été informée et, le cas échéant, accompagnée.

L'ensemble du dispositif est fondé sur des indicateurs de détection et un système essentiellement défensif. **Très peu de cas d'arrestation de pirates sont mentionnés par les acteurs français de la cybersécurité** : hormis la médiatisation d'une opération conduite par le commandement cyber de la Gendarmerie (COMCyberGEND) avec l'appui d'EUROPOL et plusieurs partenaires, dont le FBI, qui a permis d'interpeller en 2021 deux individus en Ukraine, ainsi que la saisie de plus de 1,5 million de dollars, **les stratégies de traque des groupes cybercriminels semblent l'apanage des Etats-Unis**, *via* le CyberCom ou le FBI. C'est ce dernier qui aurait fait arrêter fin juillet 2022 au Maroc un étudiant français soupçonné de piratage sur des entreprises américaines. Se pose la question de savoir si les services français ont été sollicités dans cette affaire.

Même si la compétence du SGDSN, sous la direction duquel œuvrent l'ANSSI, VIGINUM et le GIP ACYMA, se limite à un rôle de coordination - il ne lui appartient pas de décider des actions de contre-offensive à conduire – au niveau interministériel et avec le cas échéant les services de renseignement, un **suivi des signalements** effectués et des suites données contribuerait à porter un message plus dissuasif ainsi qu'une dimension plus offensive à la stratégie de cyberdéfense.

B. DES MOYENS HUMAINS ET BUDGÉTAIRES EN HAUSSE POUR 2023

Pour 2023, **les effectifs du SGDSN vont s'accroitre de 61 ETP, dont la majorité (+46 ETP) sera dirigée vers l'ANSSI**. À cet égard, il faut noter l'effort important ainsi consenti à l'échelle du plafond d'emploi du SGDSN qui s'établit à 937 ETPT dont plus de 600 sont affectés à l'ANSSI. C'est à la fois une priorité clairement donnée à cette agence, dont il faut se féliciter, mais aussi un facteur limitatif. En effet, sans remettre en cause la légitimité du rattachement d'un tel service au Premier ministre, le besoin de croissance des effectifs dédiés à la lutte contre la menace cyber pourrait à terme se trouver budgétairement à l'étroit dans le Programme 129.

- Sur le plan budgétaire, **les crédits du SGDSN** vont progresser de 36,3 M€ en AE et de 9 M€ en CP. Cette enveloppe comprend les augmentations d'effectifs en titre 2, ainsi que 29 M€ en AE pour l'acquisition d'une nouvelle emprise à Rennes et 4 M€ en CP pour le renforcement des opérations de cyberdéfense de l'ANSSI. Les autres

crédits sont destinés au fonctionnement du centre de données de l'opérateur des systèmes d'information interministériels classifiés (OSIIC) à hauteur de 4 M€, à des travaux immobiliers (3,15 M€) et au resoclage de la subvention pour charges de service public de l'IHEDN (0,95 M€).

	LFI 2022		PLF 2023		Δ 2022-2023	
en €	*AE*	*CP*	*AE*	*CP*	*AE*	*CP*
SGDSN	**268 035 875**	**273 352 956**	**304 651 167**	**282 376 623**	**+36,6 M€**	**+9 M€**
Titre2	78 784 691	78 784 691	84 428 650	84 428 650	+5,6 M€	+5,6 M€
Hors titre 2	189 251 184	194 568 265	220 222 517	197 947 973	+30,9 M€	+3,4 M€
Fonds spéciaux	**75 976 462**	**75 976 462**	**75 976 462**	**75 976 462**	**0**	**0**
GIC	**31 478 809**	**31 490 626**	**42 191 836**	**42 192 167**	**+10,7 M€**	**+10,7 M€**
Titre2	12 851 474	12 851 474	17 041 948	17 041 948	+4,2 M€	+4,2 M€
Hors titre 2	18 627 335	18 639 152	25 149 888	25 150 219	+6,5 M€	+6,5 M€
Total action 2	**375 491 146**	**380 820 044**	**422 819 465**	**400 545 252**	**+47,3 M€**	**+19,7 M€**

- Le montant attribué aux fonds spéciaux (76 M€ en AE et CP) reste inchangé depuis 2021. Seule une enveloppe globale est publiée, la ventilation qui en est faite entre les différents services de la communauté du renseignement est classifiée. Le contrôle parlementaire de l'exécution des dépenses relève de la compétence de la seule commission de vérification des fonds spéciaux (CVFS) en application de l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002.
- Les crédits du Groupement Interministériel de Contrôle (GIC) progressent de 10,7 M€ afin d'engager les dépenses nécessaire à l'installation d'une nouvelle emprise immobilière, des projets techniques et l'augmentation du plafond d'emploi de +34 ETP (soit 247 ETPT en 2023).

2. DE NOUVEAUX D'OUTILS POUR DÉVELOPPER UN ÉCOSYSTÈME DE CYBERSÉCURITÉ ET COMBLER CERTAINS ANGLES MORTS

L'année 2023 se caractérisera par la montée en puissance de **deux nouveaux dispositifs** dont la création est issue de l'impulsion du Président de la République : **VIGINUM** dans le domaine de la lutte informationnelle et le **Campus Cyber** pour la création d'un écosystème public-privé de cybersécurité. À l'inverse, les projets issus du plan de relance 2021-2022, notamment pour la sécurisation numérique des collectivités territoriales et des établissements de santé, devront continuer à fonctionner et se développer par d'autres moyens budgétaires. La fin du plan de relance pose en particulier la question de la pérennité des centres de réponse à incidents (CSIRT) régionaux et sectoriels et de la nécessaire prise en compte des enjeux cybersécuritaires spécifiques aux Outre-mer.

A. VIGINUM : UN SERVICE QUI RESTE À ÉVALUER À L'AUNE DE LA FONCTION STRATÉGIQUE CONFÉRÉE AU DOMAINE DE L'INFLUENCE

Dès après sa création en juillet 2021, vos rapporteurs avaient relevé l'étroitesse du champ des compétences attribuées à VIGINUM dont le rôle devait se limiter à deux fonctions : la détection de « situations inauthentiques » et la caractérisation de critères d'implication et d'ingérence numériques étrangères. La réponse à apporter dans la lutte informationnelle ne relève pas de ce service, lequel « se contente » de signaler des faits caractérisés au SGDSN dont le comité interministériel examine et transmet une réponse éventuelle. A ce stade, on est très loin de l'intégration à laquelle est parvenue Taïwan dans le traitement à la fois des

faits de désinformation et de réponse par le *National security council* dont l'objectif est de répondre en moins de 2 heures et 200 mots à toute menace informationnelle.

A la décharge de VIGINUM, la première année de mise en œuvre a été essentiellement consacrée à la consolidation des conditions juridiques de fonctionnement, au recrutement et à l'installation technique des équipes. Doté de 42 effectifs en septembre 2022 (la cible étant de 65 personnels), l'enjeu sera pour le service de fidéliser et de développer son activité malgré le cadre juridique très contraint et des objectifs opérationnels qui semblent très éloignés des capacités massives de vérification de l'information mises en œuvre par Google ou d'autres consortium de médias.

Un suivi étroit de l'activité de VIGINUM sera d'autant plus nécessaire qu'il permettra d'identifier des synergies avec le ComCyber ou l'écosystème médiatique, ou des axes d'amélioration de certaines méthodes de travail, comme l'automatisation de l'analyse des données de certains « petits » réseaux sociaux qui véhiculent potentiellement dans le débat public des contenus inauthentiques d'origine étrangère touchant aux intérêts fondamentaux de la Nation.

B. SÉCURISER LA FIN DU PLAN FRANCE RELANCE ET PÉRENNISER LE SOUTIEN AUX COLLECTIVITÉS TERRITORIALES, AUX ÉTABLISSEMENTS DE SANTÉ ET AUX OUTRE-MER

Parmi les objectifs du plan de relance figurait celui de constituer une « capacité mutualisée de cybersécurité » :

- il s'agissait en premier lieu d'éclairer un angle mort entre l'ANSSI (sphère étatique, OIV et OSE) et le GIP ACYMA en charge des particuliers, associations et entreprises à travers une plateforme numérique. Or, il s'est avéré « que le trou dans la raquette » se situait dans le tissu économique et social local. La création de centres de réponses à incident (CSIRT) au niveau des régions – en raison de leur compétence économique – avait pour mission de fournir aux acteurs de taille intermédiaire un service de réponse pour des incidents de premier niveau. Cet échelon d'intervention s'avère crucial mais plusieurs questions sont soulevées par leur première année de fonctionnement :
  - à ce jour 12 régions métropolitaines sur 13 se sont inscrites dans le programme de soutien aux CSIRT (à l'exception de la région Auvergne-Rhône-Alpes) ;
  - la pérennité financière du dispositif est fragilisé par la fin des financements du plan France relance, la subvention de 1 M€ de subvention de l'Etat par région devant être complété localement ;
  - enfin, le niveau de service a pu s'avérer, selon les témoignages d'entreprises, assez disparate selon les régions, les effectifs, les compétences ou même les horaires d'assistance
- Ensuite se pose la question de la montée en puissance effective des centres de réponses sectoriels, d'abord pour **les Outre-mer** où le tissu industriel de cybersécurité demeure faible alors même que les risques y sont maximaux en cas d'attaque des infrastructures de communication, de transport, d'énergie et, surtout, de menace sur des établissements hospitaliers. En métropole, **des CSIRT sectoriels dans le secteur social et dans celui de la santé** doivent impérativement, sous quelque forme que ce soit, veiller à ce que les établissements de santé mettent en œuvre les moyens labellisés nécessaires de sécurité informatiques. **Il s'agit de missions prioritaires pour lesquelles les moyens du plan de relance non encore engagés doivent être fléchés**.
- Enfin, plusieurs projets de renforcement des capacités techniques de l'ANSSI ont été rendue possibles grâce aux crédits du plan France Relance. Ces capacités de détection, de traitement et d'analyse « automatisées » pour prévenir et entraver

des cyberattaques devront dorénavant être supportées par le budget du programme 129.

3. AMÉLIORER LA COORDINATION ET LA COMPOSANTE OFFENSIVE DE LA STRATÉGIE NATIONALE

A. FAIRE DE CYBERMALVEILLANCE.GOUV.FR LE CENTRE D'APPEL UNIQUE POUR LES PARTICULIERS, ENTREPRISES ET COLLECTIVITÉS

Les moyens du GIP ACYMA (14 ETP) et 2,3 M€ de dépenses annuelles, dont 800 000 € de subvention du SGDSN, semblent dérisoire au regard du champ d'action qui lui est assigné : le grand public, les collectivités locales, les petites entreprises et associations.

Une synergie avec les CSIRT et les régions pourrait être recherchée afin d'homogénéiser le service rendu, à la condition que la plateforme numérique cybermalveillance.gouv.fr se transforme en véritable centre d'appel apte à traiter les incidents de premier niveau et à rediriger les cas les plus graves à des prestataires locaux ou à l'ANSSI. Quand il y a le feu, on appelle le 18. Les SDIS disposent de la compétence en matière de traitement des appels. Celle-ci peut-être expertisée au même titre que d'autres dispositifs.

Vos rapporteurs réitèrent donc leur recommandation dans le sens d'un changement de dimension du GIP ACYMA vers un statut équivalent à celui de la prévention routière, doté d'un budget de communication nationale dimensionné en conséquence.

> Faire du GIP ACYMA le véritable point de coordination unique de la cybermalveillance pour tout ce qui ne relève pas de l'ANSSI.

B. SOUTENIR MAIS AUSSI DAVANTAGE RESPONSABILISER LES ACTEURS

La responsabilité des incidents est naturellement à rechercher du côté des cybercriminels. En pratique, dans un contexte de généralisation des attaques informatiques, on peut distinguer trois autres niveaux de responsabilité :

- Les utilisateurs vers lesquels les messages de prévention doivent être orientés ;
- Les entreprises pour lesquelles un écosystème de sécurité (label, certification, etc.) doit être développé de pair avec une obligation de moyen ;
- Les pouvoirs publics qui face au niveau croissant d'attaques étatiques doivent élargir le périmètre du champ de détection et de protection de l'Etat, des ministères, des OIV et OSE pour faire monter d'urgence en compétence les secteurs à risques, notamment les établissements de santé et les Outre-mer.

> La responsabilité de chaque acteur est en jeu selon son niveau dans la chaîne numérique

C. ASSUMER UNE STRATÉGIE OFFENSIVE POUR MIEUX SE DÉFENDRE ET DISSUADER

« Une attitude qui serait seulement réactive, voire défensive, pourrait passer pour une forme de passivité »[1]

Appliquée au domaine de l'influence et à la guerre informationnelle, la nouvelle fonction stratégique annoncée par le Président de la République est la marque d'un virage vers

[1] Emmanuel Macron, Président de la République, discours du 9 novembre 2022 sur la revue nationale stratégique.

l'offensive. C'est le signe d'un avant et d'un après « Bounti », du nom d'un village au Mali où l'armée française a fait l'objet d'une opération de désinformation, qui l'accusait du bombardement d'un mariage en janvier 2021. C'est par une forme initiale de passivité que cette accusation a pu faire l'effet d'une bulle médiatique, elle-même alimentée par un rapport controversé des Nations unies.

De la même manière que la nouvelle stratégie française de lutte active contre la désinformation a permis de déjouer, en avril 2022, l'attribution par des éléments maliens et de la milice Wagner à la France de la responsabilité d'un charnier à Gossi, toujours au Mali. Cette pratique offensive montre l'avantage que le ComCyber tire à intégrer dans un même circuit d'analyse la détection et la réponse à apporter. Cet élément est à prendre en compte dans l'évolution possible des missions de VIGNINUM, ainsi que dans la coordination civilo-militaire (VIGINUM/ComCyber).

Une stratégie offensive est également mise en œuvre par les États-Unis et le Royaume-Uni en matière de cyberattaques, notamment en améliorant la coordination entre les différentes agences civiles et militaires chargées tant du cyber que de l'influence.

Ainsi, les américains ont-ils créé en 2021 un poste de *national cybersecurity director* à la Maison blanche afin notamment de coordonner l'*US Cyber Command* avec le *Cybersecurity and Infrastructure Security Agency* (CISA). Du côté britanniques le *National Cyber Security Center* (NCSC) a mis en place début 2022 une *national cyber force*. Dans les deux cas, leur mission intègre une dimension d'offensive préventive ou de contre-offensive. Aussi est-il proposé de **se doter d'un directeur national de la cybersécurité** chargé de la coordination nationale et avec nos principaux partenaires dans ce combat sans frontières.

POUR EN SAVOIR +

- **Audition de MM. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale, et de Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (5 octobre 2022)**

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

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

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

Commission des affaires étrangères, de la défense et des forces armées

http://www.senat.fr/commission/etr/index.html

Consulter le rapport :