SGDSN : UN BUDGET CONFORTÉ POUR RENFORCER LA CYBERSÉCURITÉ ET LA LUTTE CONTRE LES INGÉRENCES NUMÉRIQUES

Rapport d'information de MM. Olivier CADIC et Mickaël VALLET,
au nom de la commission des affaires étrangères, de la défense et des forces armées

Rapport d'information n° 219 (2021-2022)

Pour 2022, ***les crédits destinés à la coordination de la sécurité et de la défense,*** *qui comprennent les moyens du Secrétariat général de la défense et de la sécurité nationale (SGDSN), les fonds spéciaux et les crédits du groupement interministériel de contrôle (GIC),* ***sont confortés (+21,13 M€ en crédits de paiement).***

Les crédits du SGDSN *notamment augmentent (+18,4 M€) en crédits de paiement afin d'****accompagner la montée en puissance de ses missions en matière de cybersécurité et de contre-ingérence numérique.***

Le rapport salue, à cet égard, la récente ***création du Service de vigilance et de protection contre les ingérences numériques (VIGINUM) tout en regrettant une certaine timidité dans l'approche retenue,*** *le développement à grande échelle d'opérations de désinformation plaidant en faveur d'un* ***positionnement ferme et d'une capacité de réaction forte de cette structure.***

Par ailleurs, le rapport souligne que ***beaucoup reste à faire pour consolider la réponse à la cyber-menace qui ne cesse de se renforcer.*** *Il examine la mise en œuvre* ***du volet cyber du plan de relance, s'interroge sur les moyens mis à la disposition du groupement d'intérêt public ACYMA et évoque les dossiers importants de la Présidence française de l'Union européenne dans le domaine de la cybersécurité.***

1. DES MOYENS EN HAUSSE POUR DES MISSIONS QUI SE DÉVELOPPENT

Pour 2022, les crédits de l'action 2 du programme 129 s'établissent à **376,18 M€** (en baisse de 11,9 M€) **en autorisations d'engagement** (AE) et à **381,51 M€** (en hausse de 21,13 M€), **en crédits de paiement** (CP).

	LFI 2021		PLF 2022		Δ 2021-2022	
en €	*AE*	*CP*	*AE*	*CP*	*AE*	*CP*
SGDSN	***283 203 217***	***255 498 716***	***268 565 666***	***273 882 747***	***-14,6 M€***	***+18,4M€***
Titre2	74 200 660	74 200 660	78 784 691	78 784 691	+4,58 M€	+4,58 M€
Hors titre 2	209 002 557	181 298 056	189 780 975	195 098 056	-19,22 M€	+13,8 M€
Fonds spéciaux	***75 976 462***	***75 976 462***	***75 976 462***	***75 976 462***	**-**	**-**
GIC	***28 890 985***	***28 902 802***	***31 638 739***	***31 650 556***	***+2,75 M€***	***+2,75 M€***
Titre2	12 103 720	12 103 720	12 851 474	12 851 474	+0,75M€	+0,75 M€
Hors titre 2	16 787 265	16 799 082	18 787 265	18 799 082	+2 M€	+2 M€
Total action 2	**388 070 664**	**360 377 980**	**376 180 867**	**381 509 765**	**-11,9 M€**	**+ 21, 13 M€**

● **Les crédits destinés au SGDSN**, qui représentent plus des deux tiers (71,4 % en AE et 71,8% en CP) des crédits de cette action, diminuent eux aussi en AE et augmentent en CP, ces évolutions résultant notamment de :

- une augmentation de 4,6 M€ des crédits de titre 2 ;

- la finalisation de l'acquisition de l'antenne de l'ANSSI à Rennes : 13,12 M€ en CP ; il s'agit de répondre aux besoins de locaux de l'agence dont l'effectif s'est considérablement accru ces dernières années tout en contribuant à la structuration d'un pôle de compétences en cyberdéfense à Rennes avec le ministère des armées ;

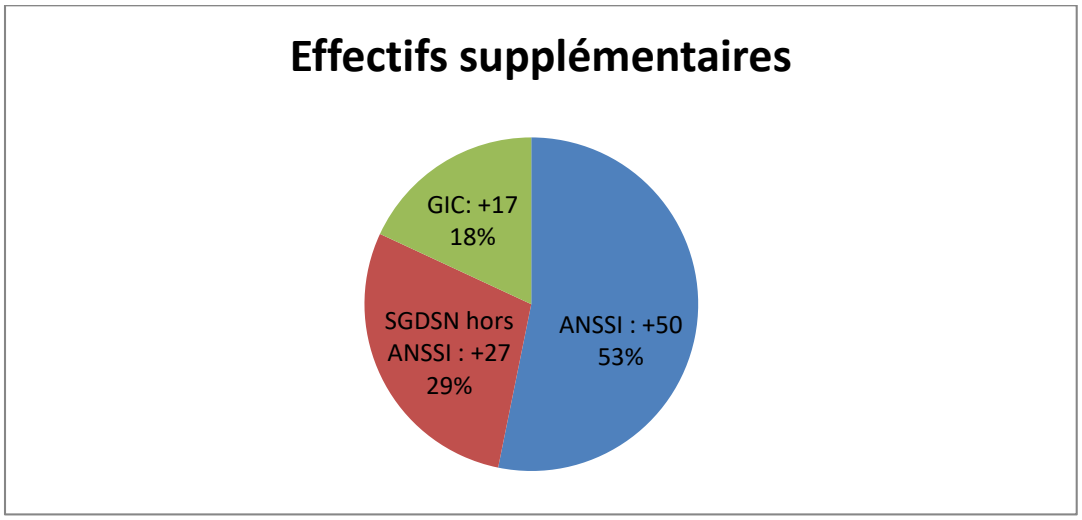
- la mise à disposition de crédits pour le **service de vigilance et de protection contre les ingérences numériques étrangères** (« VIGINUM »), nouveau service à compétence nationale placé auprès du SGDSN, pour 6,63 M€ en AE et 7,18 M€ en CP (cf. *infra* 2), les dépenses pour ce service créé en 2021 ayant été réalisées sous enveloppe par des redéploiements ;

- l'octroi d'une enveloppe de 9 M€ en AE et de 1 M€ en CP pour le financement de divers travaux immobiliers dont notamment le renouvellement des huisseries de l'Hôtel national des Invalides.

● Le montant des fonds spéciaux (76 M€ en AE et en CP) est reconduit à l'identique par rapport à 2021.

● Le GIC, quant à lui, est bénéficiaire d'une progression de ses crédits de titre II (+6,2 %) et d'une augmentation de 2 M€ en AE et en CP de ses crédits hors titre II destinés à plusieurs nouveaux projets classifiés et aux dépenses de fonctionnement supplémentaires liées à la nouvelle emprise de Montrouge.

Sur l'ensemble de l'action 2, les crédits de titre 2 s'élèvent à 91,64 M€, en hausse de 5,33 M€ (+ 6,2%) en 2022. De fait, l'action 2 bénéficiera **d'un schéma d'emploi en hausse : +94 ETP** répartis ainsi : + 77 ETP pour le SGDSN (dont 50 pour l'ANSSI et 27 pour le SGDSN hors ANSSI) et +17 ETP pour le GIC.



2. VIGINUM, UN NOUVEAU SERVICE DÉDIÉ A LA CONTRE-INGÉRENCE NUMÉRIQUE

La création [1] en septembre 2021 du « Service de vigilance et de protection contre les ingérences numériques étrangères » (VIGINUM)» est, après le vote de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, une nouvelle étape dans **l'élaboration d'une politique de lutte contre le développement des fausses informations**. La commission des affaires étrangères, de la défense et des forces armées se félicite de cette avancée.

[1] Décret n° 2021-922 du 13 juillet 2021, portant modification des attributions du SGDSN.;

Ce service à compétence nationale rattaché au SGDSN aura pour mission de **détecter les opérations de désinformation** qui se déploient sur les plateformes en ligne et d'en informer les pouvoirs publics afin qu'ils déterminent la réponse à y apporter. Il est appelé à jouer un rôle important pendant les périodes électorales en fournissant toute information utile au Conseil supérieur de l'audiovisuel, au Conseil constitutionnel et à la commission nationale de contrôle de la campagne électorale.

Une trentaine de personnes ont été affectées en 2021 à ce service, d'ores et déjà actif, à partir de redéploiements internes au SGDSN, complétés par quelques mises à disposition du ministère de l'intérieur. Grâce aux crédits alloués par le PLF pour 2022, ces effectifs seront portés à 50 en 2022, les agents recrutés étant compétents dans les domaines des technologies des réseaux sociaux, des sciences humaines et sociales, de la géopolitique et du *big data*. Il s'agit de personnes disposant déjà d'une solide expérience en matière de recherche des menaces sur internet pour le compte d'administration de l'État et, pour certains d'entre eux, pour le compte d'entreprises privées.

Le coût en termes de RH devrait tourner autour de 7,8 M€, auquel il faut ajouter 5,5 M€ de crédits pour les besoins techniques (achat d'outils de collecte et d'hébergement de données…) et 1,1 M€ de frais de fonctionnement, **soit un budget total de 14,4 M€.**

La commission des affaires étrangères, de la défense et des forces armées **salue la mise en place de cette structure qu'elle appelle de ses vœux depuis plusieurs années** – dans le contexte de recrudescence de fausses informations liée à la pandémie, les rapporteurs avaient notamment appelé à la mise en place d'une « force de réaction rapide » contre les « infox »[1] **- tout en regrettant le choix d'un positionnement prudent** puisqu'il nous a été dit en audition que VIGINUM ne serait pas en charge de la réaction aux campagnes de désinformation. Il **nous semble au contraire indispensable que cette structure monte en puissance pour jouer un rôle moteur dans le pilotage de la réponse à apporter à ces attaques hybrides**, même si bien entendu, elle n'en serait pas chargée seule. Elle pourrait ainsi proposer au Gouvernement des modalités de réponse aux attaques, comme par exemple bloquer le site d'une ambassade étrangère diffusant de fausses informations. Le travail de concertation qu'elle mène avec les plateformes, réseaux sociaux et médias et sociaux et l'étude de leurs méthodes de vérification des faits*g* vont évidemment dans le bon sens.

3. LA CYBERSÉCURITÉ : UNE PRIORITÉ A CONFORTER

La menace dans le cyberespace ne faiblit pas. Au contraire, **les actes cyber-malveillants** (cyber-rançonnage, mais aussi l'espionnage, mené par certaines puissances, le sabotage….) **ont augmenté avec la pandémie** qui a accru significativement l'exposition au risque de la société et des acteurs économiques par le développement sans précédent des usages du numérique.

Selon le SGDSN, le nombre de cyber-attaques recensées sur les neuf premiers mois de 2021 a doublé par rapport à celui recensé sur l'ensemble de l'année 2020.

[1] « Désinformation, cyber-attaques et cyber-malveillance, l'autre guerre du covid-19 », rapport d'information de MM. Olivier CADIC et Rachel MAZUIR, fait au nom de la commission des affaires étrangères, de la défense et des forces armées n° 502 (2019-2020) - 10 juin 2020.

Ces cyber-attaques touchent particulièrement les acteurs publics. En 2020, 128 incidents cyber ayant affecté les ministères ont été traités par l'ANSSI, contre 81 en 2019, soit une augmentation de 58%. En 2020 toujours, 20 % des victimes de rançongiciels signalées à l'ANSSI étaient des collectivités territoriales et 11% étaient des hôpitaux.

Nombre de cyber-incidents par ministère traités par l'ANSSI en 2020 (et variation par rapport à 2019)

Ministères	Nombre d'incidents traités par l'ANSSI	Commentaires
Ministère de l'agriculture et de l'alimentation	14 (+6)	
Ministère de la cohésion des territoires	2 (+2)	
Ministère de la culture	11(+5)	
Ministère des armées	4 (-17)	
Ministère de l'économie des finances et de la relance	18 (+7)	Dont une opération de cyberdéfense
Ministère de l'éducation nationale, de la jeunesse et des sports	58 (+ 36)	
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	3 (+2)	
Ministère de l'Europe et des affaires étrangères	14 (-)	Dont une opération de cyberdéfense et un incident majeur
Ministère de l'intérieur	13 (-1)	
Ministère de la justice	4 (-2)	
Ministère des outre-mer	2 (+1)	
Ministère des solidarités et de la santé	14 (+11)	
Ministère de la transition écologique	18 (+10)	
Ministère du travail, de l'emploi et de l'insertion	6 (-1)	

Source : réponse au questionnaire budgétaire

Face à cette menace en expansion, l'État ne cesse d'adapter sa réponse, qui vise à renforcer la sécurité des acteurs publics et à accompagner les acteurs privés dans leur démarche de sécurisation. Mais beaucoup reste à faire.

a) Le volet « cybersécurité » du plan de relance

En février 2021, le gouvernement a lancé une **stratégie d'accélération « cybersécurité** » dans le cadre du plan de relance et du programme d'investissement d'avenir dont l'ambition est de développer la filière (tripler son chiffre d'affaires, doubler le nombre d'emplois, faire émerger trois « licornes », stimuler la recherche et l'innovation…) et qui se décline en cinq axes.

Les 5 axes de la stratégie d'accélération « cybersécurité » »

1°) Développer des solutions souveraines de cybersécurité via le soutien à la R&D
2°) Renforcer les liens et synergies entre les acteurs de la filière (par la mise en place du Campus cyber à Paris et d'antennes régionales)
3°) Soutenir l'adoption de solutions de cybersécurité par les acteurs publics et privés
4°) Former plus de jeunes et de professionnels aux métiers de la cybersécurité
5°) Apporter un soutien en fonds propres à l'écosystème de cybersécurité

L'ANSSI s'est vu confier un volet cybersécurité visant à mettre en œuvre l'axe n°3, assorti d'une **enveloppe de 136 millions d'euros** à utiliser avant fin 2022. L'Agence s'y emploie à travers :

- d'une part, le financement de prestations destinées à renforcer la cybersécurité d'acteurs publics : collectivités territoriales (60 M€), hôpitaux (25 M€) et ministères et établissements publics (30 M€) ;

Aux acteurs les plus vulnérables est proposé un « **parcours de sécurisation** » consistant en l'établissement d'un audit et d'un plan d'action pour se mettre en conformité. Ce dispositif a mis un certain temps à démarrer, ce **dont les rapporteurs s'étaient inquiétés en mai dernier**. Depuis lors, il est monté en puissance et 400 entités (sur plus de 700 concernés) ont d'ores et déjà bénéficié du parcours de sécurisation (dont plus de 260 collectivités territoriales et 84 établissements de santé), pour un montant d'aide par dossier compris entre 90 000 et 140 000 euros.

Il faudra bien s'assurer qu'au-delà du **diagnostic, les collectivités auditées ont bien la capacité de réaliser les adaptations recommandées.** Par ailleurs, une attention particulière devra être portée **aux collectivités qui ne sont pas encore entrées dans le dispositif** et qui sont sûrement les moins bien « outillées » pour solliciter cet accompagnement. Enfin, il faudra envisager d'autres mesures pour **les milliers de collectivités** qui n'ont pas vocation à être prises en charge au titre du plan mais **qui sont souvent les plus vulnérables et ont besoin d'une véritable acculturation au risque cyber**.

Les acteurs disposant déjà d'un certain niveau de cybersécurité peuvent, quant à eux, solliciter des cofinancements pour mener des actions ponctuelles de renforcement en répondant à des appels à projets. Deux ont été lancés à ce jour, l'un en direction des ministères, pour un montant de 6 M€, l'autre en direction de collectivités territoriales, pour 3 M€.

- d'autre part, la création de « centres régionaux de réponse cyber de proximité » ou « centres de réponse à incidents » (CSIRT) destinés à constituer au plan local un premier niveau de soutien aux acteurs de taille intermédiaire (PME, ETI, collectivités territoriales) victimes de cyber-attaques ;

Le rôle de ces centres sera de mettre en relation les victimes avec des prestataires de cybersécurité agréés et d'être l'interface des échanges de cybersécurité au plan régional (relations avec l'association nationale des CSIRT pilotée par l'ANSSI et qui sera localisée sur le Campus cyber, relations avec les services judiciaires). Mis en place en partenariat avec les régions[1], ces centres bénéficient chacun d'une subvention de 1 M€ et d'un accompagnement technique de l'ANSSI au démarrage mais devront ensuite trouver un mode de financement pérenne en s'appuyant sur l'écosystème local. Pour l'heure, seules 4 régions sur 13 se sont engagées dans le dispositif, ce qui est insuffisant. **Nous voulons souligner son importance et appeler les autres à le rejoindre. Il faudra aussi définir une articulation logique et efficace entre ce réseau de centres de proximité et la structure ACYMA,** plus connue sous le nom de «*Cybermalveillance.gouv.fr*». Tout l'enjeu est de parvenir à une **architecture lisible et cohérente,** permettant d'orienter efficacement et rapidement les victimes, **en évitant tout fonctionnement en silo.**

- Enfin, une partie des crédits du plan (20M€) est consacrée au **renforcement de la capacité nationale de cybersécurité pilotée par l'ANSSI**, via la mise en place de solutions avancées « automatisées » au profit des ministères (ex : création d'une plateforme anti-virus de l'Etat).

Au total, 70 M€ seront dépensés en 2021 dans le cadre du plan de relance et le solde de 66 M€ devrait l'être au cours de l'année 2022.

[1] A noter aussi que quelques CSIRT sectoriels ont été créés (CSIRT maritime, CERT-Santé) et d'autres sont envisagés (notamment dans le transport aérien).

b) Le GIP ACYMA : un dispositif original et utile mais qui manque cruellement de moyens

Créé en 2017, le groupement d'intérêt public Actions contre la Cybermalveillance (GIP ACYMA) a trois grandes missions : assister les victimes d'actes de cybermalveillance/ prévenir les risques et sensibiliser les populations sur la cybersécurité et observer et anticiper le risque numérique par la création d'un observatoire.

En quatre ans, le GIP est notamment parvenu à **fédérer en son sein la majeure partie de l'écosystème de la lutte contre la cybermalveillance** en réunissant plus de 50 des principaux acteurs étatiques et du secteur privé impliqués (ministères et services de l'État, associations de consommateurs et d'aide aux victimes, organisations professionnelles, assureurs, éditeurs logiciels, constructeurs, opérateurs de service…).

Il a développé une offre de service de qualité dont témoigne la **progression forte et constante de l'utilisation de la plateforme** *cybermalveillance.gouv.fr* (+155 % de visiteurs en 2020, + 2 millions de visiteurs attendus en 2021). Il a également mis en place un réseau national de plus de 1 200 prestataires accessibles au travers de la plateforme, en mesure d'apporter une assistance technique de proximité aux victimes.

En outre, son positionnement original et unique, en amont du dépôt de plainte, lui a permis d'identifier et d'alerter les services judiciaires sur l'ampleur de plusieurs phénomènes cybercriminels (escroqueries à la panne informatique, cyber-chantage aux contenus compromettants, piratage de comptes professionnels de formation…).

Pourtant, faute de moyens suffisants, cette structure indispensable au regard du développement de la menace cyber **n'est pas en mesure d'assurer véritablement qu'une seule de ses missions** : l'assistance aux petites victimes (encore ce service est-il dispensé via une plateforme numérique alors que le bon format, défendu par les rapporteurs, serait celui d'une plateforme d'appel permettant de donner les premiers conseils pratiques aux victimes).

Si ACYMA utilise toutes les ressources dont il dispose pour faire passer ses messages (en profitant notamment des vecteurs que lui offrent ses membres, comme les écrans dans les agences de la Poste ou dans les Transiliens), la **mission de sensibilisation et de prévention pâtit de l'absence de moyens à consacrer à la communication**. Par ailleurs, le GIP n'a pas encore pu mettre en place l'observatoire national, indispensable à la bonne connaissance de la menace.

Fonctionnant actuellement avec un **budget de 1,6 M€** (provenant pour moitié de contributions publiques et pour moitié de contributions privées) qui lui permet d'employer 12 agents, **cette structure, unique en son genre à l'échelle mondiale pour la mise en relation de victimes avec des prestataires de cybersécurité, est malheureusement sous-dotée financièrement.** Sans remettre en cause la forme juridique du GIP, qui est ici particulièrement adaptée, il est urgent d'augmenter significativement (c'est-à-dire les porter au moins à 3 M€) les moyens alloués à ACYMA. Au vu des enjeux et de l'ampleur des risques encourus dans le champ cyber, un tel effort est indispensable et ne paraît pas hors de portée, surtout s'il est partagé entre ses différents membres. En outre, il faut garder à l'esprit que **le développement des actes cyber-malveillants du fait de l'absence ou de l'insuffisance de la politique de prévention a un coût pour la société** (le préjudice pour l'Etat de l'arnaque au compte professionnel de formation représente plusieurs dizaines de millions d'euros).

La commission des affaires étrangères, de la défense et des forces armées soutient en outre l'idée de mener une **grande campagne nationale de prévention contre la cyber-malveillance**, dotée d'une enveloppe de communication exceptionnelle et qui serait mise en œuvre par ACYMA.

c) La Présidence française de l'UE : une fenêtre d'opportunité pour les dossiers cyber

Par ailleurs, notre pays entend mettre à profit la Présidence française de l'Union européenne au 1er semestre 2022 pour faire avancer au plan européen les dossiers liés à la cybersécurité.

Cela concerne d'abord la **révision** de la directive relative à la sécurité des réseaux et des systèmes d'information, dite **directive NIS**, adoptée en 2016, qui vise à étendre le champ des secteurs considérés comme critiques (traitement des eaux usées, espace, administrations…) et rehausser les obligations imposées à leurs opérateurs.

Par ailleurs, la France souhaite œuvrer au **renforcement de la sécurité des institutions européennes**, insuffisamment protégées, par la mise en place de règles spécifiques.

Elle souhaite également favoriser le **développement d'un « tissu industriel de confiance » à l'échelle européenne**, par la mise en place à Bucarest du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et des avancées en matière de certification de sécurité, plusieurs schémas étant en cours d'élaboration, notamment le « European Common Criteria ». La France cherche notamment à étendre à l'échelle européenne son approche de la certification dans le domaine du « *nuage* » (certification SecNumCloud). Si la certification est nécessaire pour produire de la confiance, attention toutefois à ne pas tomber dans **l'écueil de l'excès de normes** qui ont un coût élevé pour les entreprises et *in fine* restreignent l'offre. Une idée intéressante et relativement simple, qui a été évoquée lors des auditions, serait de créer un label de qualité associé à un niveau de confiance correspondant à une lettre (A,B,C,D) sur le modèle de celui qui existe en matière de consommation énergétique.

Pour mémoire, la stratégie nationale pour le *cloud* publiée en mai 2021 oblige les organismes publics et les OIV/OSE à recourir à des hébergeurs disposant du nouveau label « Cloud de confiance » qui implique que les infrastructures soient certifiées, localisées en Europe et opérées par des acteurs européens. Il s'agit de garantir que les données européennes ne tombent pas sous le coup de législations étrangères comme le *Cloud Act* américain.

Nous sommes également très favorables au développement au plan européen de mesures de sécurisation des réseaux 5G, telles que recommandées par la Commission européenne[1] et au déploiement de la boîte à outils (« Toolbox 5G ») adoptée en 2020.

Enfin, la France soutient activement la mise en place de **mécanismes de solidarité à l'échelle européenne**, à savoir le cadre européen de réponse aux crises cyber *Blueprint* et le réseau de liaison *CyCLONe* (Cyber Crisis Liaison Organisation Network) qui doit être déployé dans tous les Etats membres.

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 :

http://www.senat.fr/notice-rapport/2021/r21-219-notice.html

[1] Recommandation de la Commission européenne de mars 2019 sur la cybersécurité des réseaux 5G.