PROJET DE LOI DE FINANCES POUR 2021

CYBERDÉFENSE, SÉCURITÉ NATIONALE, RÉSEAUX 5G : DES MOYENS EN HAUSSE POUR UNE MENACE QUI EXPLOSE

PROGRAMME 129 : COORDINATION DU TRAVAIL GOUVERNEMENTAL

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

Avis n° 140 (2020-2021) Tome n° 9

Le programme 129 «Coordination du travail gouvernemental» de la mission « Direction de l'action du gouvernement » regroupe les fonctions d'état-major, de stratégie et de prospective, de coordination et de soutien exercées par les services du Premier ministre.

Au sein de ce programme, la commission des affaires étrangères et de la défense du Sénat examine les crédits inscrits à l'action 2 « Coordination de la sécurité et de la défense », qui sont destinés au financement du Secrétariat général de la défense et de la sécurité nationale (SGDSN), de la cyberdéfense (ANSSI) et de l'opérateur rattaché Institut des Hautes Etudes de la Défense nationale (IHEDN).

Au cours de sa réunion du 18 novembre 2020, la commission des affaires étrangères, de la défense et des forces armées a donné, pour ce qui concerne le programme 129, un avis favorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement » dans le projet de loi de finances pour 2021.

1. UN BUDGET POUR 2021 EN HAUSSE, TIRÉ PAR LES RECRUTEMENTS

Pour 2021, les crédits de l'action 2 du programme 129 s'établissent à **389,56 M€ (en hausse de 3,3 M€) en autorisations d'engagement (AE) e**t à **361,87 M€ (en hausse de 9,1 M€), en crédits de paiement (CP)**. Cette action bénéficiera de 62 recrutements, dont 40 au profit de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

EVOLUTION DES AUTORISATIONS D'ENGAGEMENT[1]

	T2			Hors T2			Total		
AE 2020	80 073 291			306 199 113			386 272 404		
AE 2021	86 304 380			303 261 113			389 565 493		
Δ	**+ 6 231 089**	**+7,8%**	↗	**- 2 938 000**	**- 0,96 %**	↘	**+ 3 293 089**	**+ 0,85 %**	↗

EVOLUTION DES CREDITS DE PAIEMENT[1]

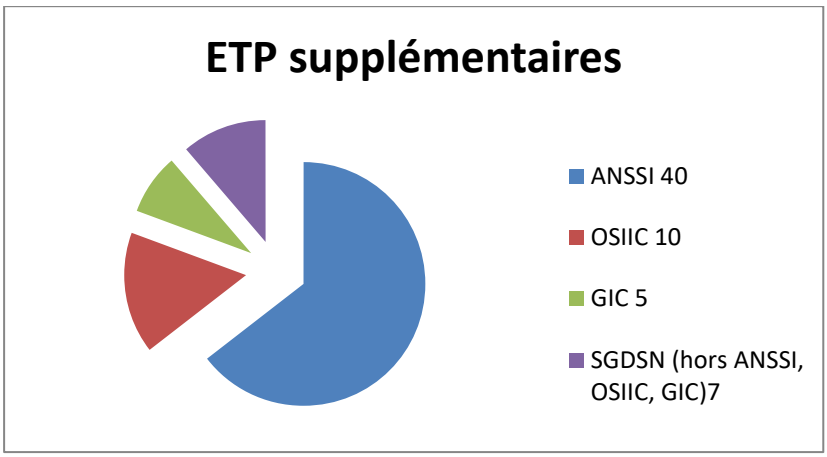
	T2			Hors T2			Total		
CP 2020	80 073 291			272 706 429			352 779 720		
CP 2021	86 304 380			275 568 429			361 872 809		
Δ	**+ 6 231 089**	**+7,8%**	↗	**+ 2 862 000**	**+1,05%**	↗	**+ 9 093 089**	**+2,6%**	↗

Ces crédits comprennent une enveloppe de 76,4 M€ en AE et en CP (reconduite par rapport à 2020) destinés au financement d'actions liées à la sécurité intérieure et extérieure (**fonds spéciaux**), une enveloppe de 28,25 M€ en AE et en CP destinés au financement du **Groupement interministériel de contrôle (GIC)**, service du Premier ministre chargé de centraliser les

[1] Source : PAP 2021

demandes d'autorisation de mise en œuvre des techniques de renseignement émises par les services de renseignement, le reste des crédits étant destiné au SGDSN.

Pour 2021, **l'action 2 bénéficie d'un schéma d'emploi en hausse : +62 ETP** qui se répartissent de la manière suivante : + 40 pour l'ANSSI, + 10 pour l'opérateur des systèmes d'information interministériels classifiés (OSIIC)[1], + 5 pour le GIC et + 7 ETP au SGDSN.



La **croissance des effectifs de l'ANSSI** (+ 40 ETP), similaire à celle de l'an passé, est rendue nécessaire par le développement de ses missions (sécurité des systèmes d'information de l'Etat, des opérateurs d'importance vitale et de services essentiels, mise en œuvre de la loi sur la sécurité des réseaux 5G…). Le plafond d'emploi de l'agence est fixé à **621 ETP**. Compte tenu l'augmentation régulière de ses effectifs et du fort renouvellement des personnels, constitués à 80% de contractuels, le **recrutement constitue un enjeu important**. Néanmoins, malgré un contexte de rareté des ressources humaines dans les métiers du numérique, **l'ANSSI bénéficie d'une réelle attractivité**, un passage dans ses murs constituant un tremplin pour une carrière ultérieure. Ce modèle RH original permet à l'ANSSI de bénéficier de compétences sans cesse renouvelées en même temps qu'il favorise la diffusion d'une culture de la cybersécurité dans le secteur privé et contribue au renforcement de la résilience collective dans ce domaine.

Les crédits hors titre 2 sont destinés à couvrir les dépenses de fonctionnement courant, le recours à des services de veille et d'analyse des menaces, les dépenses de logiciel et de services de sécurité, les dépenses d'acquisition et de fonctionnement de systèmes d'information sécurisés, de programmes interministériels de lutte contre les menaces, le renforcement des procédures de gestion de crise, ou encore des dépenses d'intervention en faveur d'entités tierces (agence nationale pour la recherche, groupement d'intérêt public pour l'assistance aux victimes d'actes de cyber malveillance notamment).

Ils comprennent aussi une **subvention de 7 M€ destinée à l'IHEDN** (en baisse de 250 000 €), celle destinée à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) étant supprimée du fait de la dissolution de cet institut, **effective au 31 décembre 2020**.

Le « pôle cyber » à Rennes

Cette année, les crédits hors titre 2 comprennent une enveloppe de **33,5 M€ en AE et 9,5 M€ en CP** destinée à permettre l'installation d'une antenne de l'ANSSI à Rennes dans le cadre de la constitution d'un **pôle de compétences en cyberdéfense avec le ministère des armées** et pour répondre aux besoins immobiliers de l'agence dont les effectifs et les missions ont beaucoup augmenté ces dernières années. Celle-ci aura une capacité d'accueil de 200 agents.

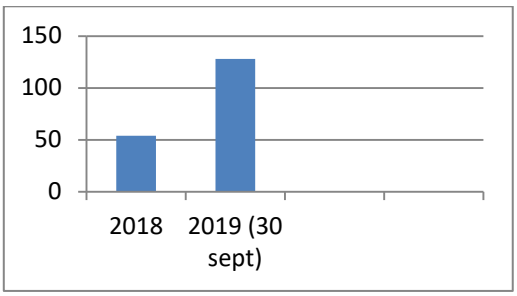
[1] L'opérateur des systèmes d'information interministériels classifiés (OSIIC) est le produit de la fusion, intervenue le 1er juillet 2020, du centre de transmissions gouvernemental et de la sous-direction numérique de l'ANSSI.

2. UNE MENACE CYBER QUI NE CESSE DE S'AMPLIFIER AVEC LE « RANÇONNAGE »

Indissociables de l'évolution technologique et de la généralisation des usages du numérique – qui s'est accentuée avec la crise sanitaire et les mesures de confinement - **les actes malveillants dans l'espace cyber ne cessent de se développer**.

La cybercriminalité s'est beaucoup professionnalisée et se développe à grande échelle grâce à des « rançongiels » de plus en plus performants. La période récente a été marquée par une augmentation significative du nombre d'attaques par rançongiciels : **au 30 septembre 2020, l'ANSSI en avait traité 128 contre 54 sur l'ensemble de l'année 2019**.

Nombre d'attaques par rançongiciels traitées par l'ANSSI



Source : ANSSI

Utilisant un mode opératoire éprouvé, consistant à introduire un virus bloquant le système informatique et à exiger le paiement d'une rançon pour le débloquer, cette **forme de criminalité cible particulièrement les opérateurs en mesure de payer d'importantes sommes**. Les dégâts causés peuvent être considérables : à la perte du matériel informatique et des données s'ajoutent le manque à gagner causé par l'interruption de l'activité et l'atteinte à la réputation liée à l'exposition médiatique, quand bien même l'entreprise est parvenue à contenir l'attaque. **Les organismes publics et secteurs critiques comme les hôpitaux ne sont désormais plus épargnés**, comme l'a montré l'attaque au « rançongiciel » en décembre 2019 contre le CHU de Rouen. Les collectivités territoriales, insuffisamment protégées, pourraient elles aussi constituer une cible, a prévenu le directeur général de l'ANSSI, M. Guillaume Poupard, lors de son audition par la commission.

Il faut noter aussi le **développement des attaques indirectes, visant la chaîne d'approvisionnement** (partenaires et fournisseurs) des entités ciblées, constituée d'entreprises de plus petite taille qui ne disposent pas des mêmes moyens pour se protéger.

Risque plus classique, **l'espionnage tend lui aussi à augmenter**, avec comme objectifs la recherche d'informations stratégiques sur les politiques extérieures et de défense, mais aussi l'accès aux informations industrielles et secrets commerciaux et le vol de données personnelles. En ouvrant des brèches dans les systèmes, le télétravail pourrait fournir de nouvelles facilités aux attaquants. Il est impératif de travailler à la sécurisation et à la robustesse des outils de travail à distance.

Qu'ils émanent de cyberactivistes aux motivations idéologiques ou de cybergroupes à la main de puissances étrangères, **les actes de piratage et de sabotage** se développent eux aussi, **particulièrement contre les institutions et administrations publiques**. Sur l'année 2019, l'ANSSI a été amenée à traiter **81 incidents de sécurité numérique ayant affecté les ministères français**, un chiffre en légère progression (+3%) par rapport à l'année précédente :

Nombre d'incidents, par ministère, consécutifs à des attaques informatiques, traités par l'ANSSI en 2019

Ministères	Nombre d'incidents traités par l'ANSSI	Commentaires
Ministère de l'agriculture et de l'alimentation	8	Dont un incident majeur
Ministère de la cohésion des territoires	1	
Ministère de la culture	6	
Ministère des armées	21	
Ministère de l'économie des finances et de la relance	11	
Ministère de l'éducation nationale, de la jeunesse et des sports	22	
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	1	
Ministère de l'Europe et des affaires étrangères	14	
Ministère de l'intérieur	14	
Ministère de la justice	6	Dont une opération de cyberdéfense
Ministère des outre-mer	1	
Ministère des solidarités et de la santé	3	
Ministère de la transition écologique	8	
Ministère du travail, de l'emploi et de l'insertion	7	

Le ministère des armées, qui assure lui-même, via le commandement de la cyberdéfense (COMCYBER) la détection des attaques informatiques sur ses propres systèmes d'information, a traité 88 événements en 2019, contre 13 en 2018, cette forte augmentation pouvant cependant aussi démontrer une amélioration de la capacité de détection. A cet égard, il faut désormais considérer et se préparer à la **menace de guerre cyber ou de conflit cyber** (le cyber étant désormais intégré dans l'ensemble des capacités militaires), voire de s**abotage à grande échelle et de cyber-terrorisme**. Sans oublier les actions insidieuses qui transitent par les réseaux – manipulations, désinformation, propagande – de plus en plus utilisées par l'ennemi. Celles-ci présentent un grand potentiel de mobilisation en vue de déclencher des opérations terroristes, qui constitue une très grave menace.

3. L'ANSSI : UNE ACTION TOUS AZIMUTS POUR RENFORCER LA CYBERSÉCURITÉ

Face à cette menace de plus en plus présente, l'Etat a développé une réponse comportant à la fois un volet offensif, porté principalement par le ministère des armées (à travers notamment le COM CYBER), et un **volet défensif confié à l'ANSSI**. Dix ans après la mise en place de l'ANSSI, où en est-on ? Des progrès considérables ont été accomplis, sous-tendus par une montée en puissance régulière et forte des moyens alloués à l'Agence. La compétence de notre pays dans le domaine cyber est reconnue et respectée : **sans conteste, nous faisons partie des pays « du premier cercle ».**

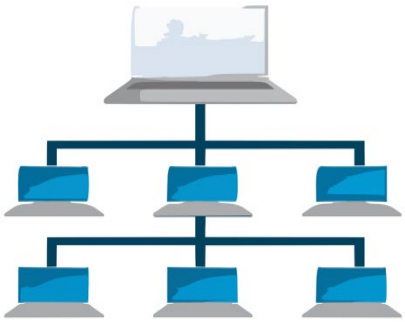
L'ANSSII est connue comme le « pompier du cyber ». Elle intervient en réaction aux incidents cyber, par des engagements opérationnels qui vont du signalement aux opérations de cyberdéfense :

Réponses opérationnelles de l'ANSSI aux incidents cyber en 2019

Elle participe aussi au centre de coordination des crises cyber (c4), dont elle assure le secrétariat. Cependant, **le volet prévention** est bien au cœur de ses missions, l'ANSSI ayant été créée pour protéger et préparer l'Etat et les opérateurs critiques à la menace cyber.

- Son action en direction des **administrations publiques et les opérateurs privés régulés** (opérateurs d'importance vitale et opérateurs de services essentiels) pour contrôler l'application de la réglementation en matière de sécurité numérique et par la réalisation d'inspections et audits (de l'ordre 300 réalisés depuis 2019, dont 200 au profit des opérateurs régulés et une centaine au profit des services de l'Etat) a incontestablement contribué à **un renforcement de la cybersécurité**. Depuis 2017, les ministères sont plus nombreux à se doter de plans de cybersécurité, en cohérence avec les politiques qu'ils mènent (ministère des affaires étrangères, ministères sociaux notamment).

Chargée de la **coordination interministérielle en matière de sécurité informatique**, l'ANSSI fournit un soutien technique à l'ensemble des ministères et se prononce (par un « avis de sécurité ») sur leurs projets informatiques qui lui sont soumis par le directeur interministériel du numérique. Pour autant, certains ministères restent très attachés à leur autonomie et ne coopèrent vraiment qu'après la survenue d'un problème majeur. Notamment, tous ne sont pas encore raccordés au réseau interministériel de l'Etat (RIE), solution technique retenue par l'Etat pour la gestion de crises. En outre, la sécurité informatique reste encore trop souvent considérée comme une question technique, alors qu'elle constitue un risque majeur, au même titre que le risque budgétaire ou juridique et devrait être davantage pris en compte. **Une prise de conscience de la gravité des enjeux par l'ensemble des acteurs publics est nécessaire.**



La **refonte en cours de la politique de sécurité des systèmes d'information de l'Etat (PSSIE)**, validée fin 2019 à l'issue de travaux ministériels, et prévoyant 13 actions, devrait cependant **permettre d'améliorer cette gouver**nance. Elle prévoit notamment la rédaction d'un texte décrivant précisément cette organisation, la signature de conventions entre les ministères et l'ANSSI et la mise au point d'indicateurs permettant de mesurer l'évolution de leur niveau de sécurité. **La commission des affaires étrangères et de la défense plaide pour une entrée en vigueur rapide de ces mesures et continue de recommander, comme l'an passé, un renforcement de la capacité d'action et de contrainte de l'ANSSI sur les services de l'Etat pour mettre en œuvre cette politique de sécurité**.

Par ailleurs, le **processus de désignation des opérateurs de services essentiels, prévu par la loi du 26 février 2018**[1] **transposant la directive NIS**[2]**, doit être accéléré**, en coopération avec les ministères de tutelle des secteurs concernés. En effet, la grande majorité des quelques 150

[1] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

[2] Directive Network and Information System Security (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016.

opérateurs désignés jusqu'à présent sont des opérateurs d'importance vitale (OIV) déjà soumis à des règles de cybersécurité en vertu de la loi du 18 décembre 2013 de programmation militaire. Il **s'agit désormais de toucher des opérateurs essentiels au bon fonctionnement de l'économie et de la société, qui échappent encore à toute réglementation en la matière**.

L'application de l'article 34 de la LPM 2019-2025 qui permet à l'ANSSI de collaborer avec les **opérateurs de communication électronique** (OCE) pour accroître sa capacité de détection des cyberattaques (que ce soit en utilisant les dispositifs déployés par les OCE ou en déployant ses propres dispositifs de détection) rencontre jusqu'à présent **quelques difficultés** : investissement insuffisant des OCE dans ces dispositifs (dans la mesure où ils sont à leur charge), remontée tardive des informations à l'ANSSI (une fois par semaine au mieux alors que les textes réglementaires prévoient une remontée par jour), caractère relativement fastidieux du déploiement par l'ANSSI de ses propres sondes, impossibilité légale d'accéder au contenu des serveurs malveillants notamment…La crise sanitaire a sans doute eu un impact sur la capacité organisationnelle et opérationnelle des OCE et des hébergeurs à mettre en œuvre ce dispositif.

- Au-delà de la mission de surveillance renforcée qu'elle exerce auprès des administrations publiques et des OIV/OSE, l'ANSSI s'attache à mobiliser l'ensemble de l'économie et de la société autour de la **prise en compte du risque numérique** et à **« élever le niveau global de cybersécurité** ».

Pour cela, elle met en œuvre une **politique de labellisation des produits et de certification** des prestataires de services (détection, audit, réponse à incidents) qui contribue à faire émerger une offre de cybersécurité à destination des opérateurs privés, l'ANSSI n'ayant pas vocation à assurer elle-même la protection de l'ensemble de la Nation. Afin de pallier la pénurie de compétences dans ce secteur, l'agence contribue au **développement de formations en cybersécurité** à travers la labellisation de modules ou de filières, la mise à disposition de ressources et de contenus pédagogiques, ainsi que par l'ouverture de son centre de formation. Elle soutient, en outre, l'action du **groupement d'intérêt public (GIP) Action contre la cybermalveillance (Acyma)** qui anime, au moyen d'une plateforme numérique, un dispositif de sensibilisation, prévention et d'assistance aux victimes d'actes de cybermalveillance.

Le Campus Cyber de la Défense

Enfin, **en 2021, l'Agence rejoindra le Campus Cyber** qui va s'ouvrir prochainement dans le quartier de la Défense. Elle entend ainsi participer à la **mise en commun de ressources et de connaissances** avec divers acteurs du secteur cyber (laboratoires, grands groupes, jeunes pousses…) et à la création de synergies visant à permettre la structuration d'un « écosystème français de la cybersécurité ». **Votre commission ne peut que saluer la concrétisation de ce projet phare,** qui s'inspire du Cybersecurity Operations Center (CSOC) d'Austin aux Etats-Unis, **et se féliciter de la part active que l'ANSSI entend y prendre.**

4. L'APPLICATION DE LA LOI SUR LES RÉSEAUX 5G : UN ENJEU STRATÉGIQUE POUR NOTRE SECURITÉ

Alors que la commercialisation des offres 5G est imminente, la commission a souhaité faire le point sur l'application de la loi du 1er août 2019 sur la sécurité des réseaux mobiles de 5e génération, qui confie à l'ANSSI le soin de délivrer aux opérateurs télécoms, sur la base d'une évaluation des risques et pour une durée limitée dans le temps, les autorisations d'utiliser des équipements 5G.

Avec l'avènement de la 5G, les réseaux de téléphonie mobiles vont devenir critiques car ils vont conditionner, via les objets connectés, le fonctionnement de l'ensemble de notre économie mais aussi nos vies quotidiennes. L'exigence de continuité de ces réseaux devient hautement stratégique. Il est donc essentiel que les opérateurs télécoms utilisent des **équipements sûrs et non susceptibles de subir des interruptions de services**. **Or, un tel risque ne peut être exclu lorsque les équipements proviennent d'une entreprise étrangère soumise aux lois de son pays et aux éventuelles pressions de ses gouvernants**, d'autant que ces équipements sont désormais essentiellement composés de logiciels et constituent des portes d'entrée faciles à emprunter. L'hypothèse d'un acte offensif étranger qui emprunterait ce canal doit donc être prise en compte, il s'agit même d'une menace majeure pour notre sécurité.

Pour autant, la France a fait le choix de ne pas exclure *a priori* un fournisseur en particulier. Il était en effet nécessaire de tenir compte également de l'équilibre économique du marché et de la situation initiale des opérateurs de télécoms qui tous ne recourent pas dans les mêmes proportions aux équipements soulevant des problèmes de sécurité. Pour mémoire, le marché français compte seulement trois fournisseurs : Nokia, Ericsson et Huawei. Seuls deux opérateurs (SFR et Bouygues) utilisent jusqu'à présent des équipements Huawei.

La loi du 1er août 2019 vise à répondre à cet enjeu qui consiste à amener les opérateurs à réduire leur exposition au risque de sécurité sans compromettre leur équilibre financier.

Après la publication des textes réglementaires d'application de la loi à la fin de l'année 2019, les quatre opérateurs français ont déposé **157 demandes auprès de l'ANSSI, portant sur un total de près de 65 000 équipements**. Dans un premier temps, il s'agit de « stations de base » (antennes) et non d'infrastructures de « cœur de réseau », qui demeurent en 4G. La totalité des demandes concernait des zones urbaines, prioritaires dans le déploiement de ce réseau.

Pour l'instruction des dossiers ont été pris en compte le niveau de sécurité des appareils, les modalités de leur déploiement et de leur exploitation, la localisation envisagée et l'exposition de l'équipementier au risque d'ingérence d'un Etat non européen.

Sur les **157 demandes examinées au 13 juillet 2020** :

- 82 ont été accordées pour la durée maximale de 8 ans
- 53 ont été accordées pour une durée inférieure à la durée maximale
- 22 ont fait l'objet d'un refus.

En pratique, **toutes les décisions de refus et toutes les autorisations pour des durées réduites ont concerné des équipements Huawei**.

Les refus d'autorisation auront des conséquences économiques, particulièrement lorsque la demande portait sur la mise à jour en 5G d'antennes 4G. Dans ce cas de figure, l'opérateur va devoir remplacer au plus vite l'ensemble de ses équipements par ceux d'un autre fournisseur et sera retardé dans le déploiement de son réseau 5G. Il faut cependant noter que des autorisations

de durée maximale (14) ont aussi été délivrées pour des équipements Huawei, au profit de trois des opérateurs.

Les décisions prises sur le fondement de la loi d'aout 2019 dessinent la ligne prudente et mesurée adoptée par l'ANSSI. **La commission des affaires étrangères en prend acte et suivra attentivement les développements ultérieurs de ce dossier sensible. Il importe de ne pas relâcher la vigilance** et de continuer à sensibiliser les opérateurs de télécommunications aux risques de sécurité inhérents au développement de cette technologie.

Par ailleurs, nous **devons œuvrer à la mise en place d'une approche commune au plan européen**. Une analyse des risques[1] et une boîte à outils[2] comportant des mesures que les Etats-membres s'engagent à décliner au plan national ont été publiées en octobre 2019 et janvier 2020. Avec sa loi d'août 2019, la France se conforme d'ores et déjà à ce cadre et peut constituer une source d'inspiration pour ses partenaires en ce qui concerne la régulation du marché de la 5G.

L'ouverture d'un centre de recherche de Huawei à Paris en septembre 2020, consacré à l'intelligence artificielle, constitue un motif de préoccupation pour la commission. Le groupe technologique chinois fournit des systèmes de surveillance par intelligence artificielle qui permettent le contrôle de population à grande échelle par des régimes autoritaires. Il est sous le coup de sanctions américaines depuis le mois d'août 2020 pour aide à la violation des droits de l'homme en Chine. Il sera nécessaire de veiller à ce que les travaux de recherche sur l'intelligence artificielle localisés chez Huaweï en France ne puissent participer à la violation des droits humains dans le monde.

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 dossier législatif :

http://www.senat.fr/dossier-legislatif/pjlf2021.html

[1] EU coordinated risk assessment of the cybersecurity of 5G networks, Report 9 October 2019.

[2] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 janvier 2020