

N° 117

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 17 novembre 2022

AVIS

PRÉSENTÉ

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi de finances, considéré comme adopté par l'Assemblée nationale en application de l'article 49, alinéa 3, de la Constitution, pour 2023,

TOME IX

DIRECTION DE L'ACTION DU GOUVERNEMENT
Coordination du travail gouvernemental (Programme 129)

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.

Voir les numéros :

Assemblée nationale (16^{ème} législ.) : 273, 285, 286 rect., 292, 337, 341, 364, 369, 374, 386 et T.A. 26

Sénat : 114 et 115 à 121 (2022-2023)

SOMMAIRE

	<u>Pages</u>
L'ESSENTIEL.....	5
I. LES MENACES CROISSENT PLUS VITE QUE LES MOYENS	6
A. LE TABLEAU DE BORD ANNUEL DES ATTAQUES CYBER : DES MENACES PLUS NOMBREUSES, PLUS DIVERSIFIEES ET PLUS PREJUDICIALES	6
B. DES MOYENS HUMAINS ET BUDGETAIRES EN HAUSSE POUR 2023	10
II. DE NOUVEAUX OUTILS POUR DEVELOPPER UN ECOSYSTEME DE CYBERSECURITE ET COMBLER CERTAINS ANGLES MORTS.....	11
A. VIGINUM : UN SERVICE QUI RESTE A EVALUER A L'AUNE DE LA FONCTION STRATEGIQUE CONFEREES AU DOMAINE DE L'INFLUENCE.....	12
B. LA CREATION DU CAMPUS CYBER : POUR UN ECOSYSTEME PUBLIC-PRIVE DE CYBERSECURITE	13
C. SECURISER LA FIN DU PLAN FRANCE RELANCE ET PERENNISER LE SOUTIEN AUX COLLECTIVITES TERRITORIALES, AUX ETABLISSEMENTS DE SANTE ET AUX OUTRE-MER.....	14
III. AMELIORER LA COORDINATION ET LA COMPOSANTE OFFENSIVE DE LA STRATEGIE NATIONALE.....	15
A. FAIRE DE CYBERMALVEILLANCE.GOUV.FR LE CENTRE D'APPEL UNIQUE POUR LES PARTICULIERS, ENTREPRISES ET COLLECTIVITES	15
B. SOUTENIR MAIS AUSSI DAVANTAGE RESPONSABILISER LES ACTEURS	16
C. ASSUMER UNE STRATEGIE OFFENSIVE POUR MIEUX SE DEFENDRE ET DISSUADER	16
EXAMEN EN COMMISSION.....	19
I. EXAMEN DU RAPPORT (16 NOVEMBRE 2022).....	19
II. AUDITION DE MM. STEPHANE BOUILLON, SECRETAIRE GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE, ET DE GUILLAUME POUPARD, DIRECTEUR GENERAL DE L'AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (5 OCTOBRE 2022).....	23
LISTE DES PERSONNES AUDITIONNEES	39

L'ESSENTIEL

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

*Emmanuel Macron,
Président de la République¹*

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.

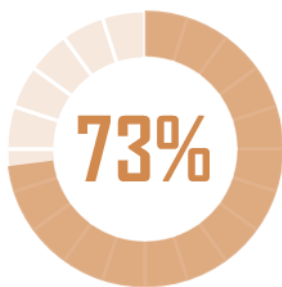
Le mercredi 16 novembre 2022, sous la présidence de M. Christian Cambon, président, la commission a émis un avis favorable à l'adoption des crédits relatifs à l'action n° 2 du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

¹ Extrait du discours de Toulon du 9 novembre 2022 sur la revue nationale stratégique.

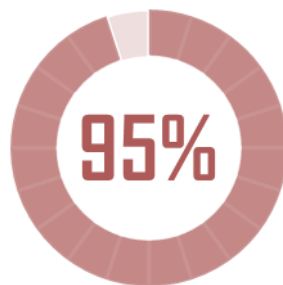
I. LES MENACES CROISSENT PLUS VITE QUE LES MOYENS

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

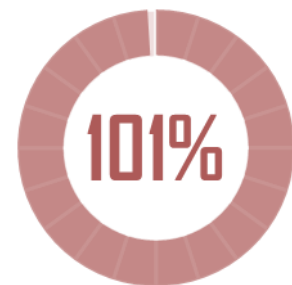
La cyber menace n'évolue pas dans le bon sens et le SGDSN qualifie sa **croissance d'exponentielle** dans trois domaines particulièrement préoccupants : le secteur criminel, l'activité d'espionnage et l'action militaire.



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 2021 sur le site cybermalveillance.gouv.fr

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 cybersécurité 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 chiffre 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 ;

(CSIRT) régionaux et sectoriels et de la nécessaire prise en compte des enjeux cybersécuritaires spécifiques aux Outre-mer.

A. VIGINUM : UN SERVICE QUI RESTE A EVALUER A L'AUNE DE LA FONCTION STRATEGIQUE CONFEREE 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.

Les missions de VIGINUM

Trois rôles :

- **Détecter** par le constat d'une agitation numérique et la recherche de traces de manipulation étrangère ;
- **Caractériser** par l'analyse des modes opératoires utilisés et l'attribution de la menace ;
- **Prévenir** en informant les autorités compétentes, en l'occurrence le SGDSN, chargées de la coordination et de préparation d'une réponse adéquate.

Quatre critères d'intervention :

- 1) Atteinte aux intérêts fondamentaux de la nation (critère principal et nécessaire) ;
- 2) Données et contenus inauthentiques ;
- 3) Diffusion artificielle, automatisée, massive et délibérée ;
- 4) Caractère étranger de la source.

À 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.

Il en ressort que le champ d'intervention de VIGINUM se limite à un rôle de « bouclier » défensif (détection, caractérisation et information des autorités) sans compétence sur la suite, c'est-à-dire la coordination et le volet offensif de la réponse à apporter. À cet égard, si l'encadrement par un comité

d'éthique et scientifique est de nature à garantir le cadre d'emploi de VIGINUM, on peut s'interroger d'une part sur sa composition (membres du CSA, deux représentants de la presse, un diplomate, un chercheur), d'autre part sur la démultiplication des délais qu'il peut occasionner sur l'activité de détection et d'imputation de l'opération.

Préconisation de vos rapporteurs :

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. LA CREATION DU CAMPUS CYBER : POUR UN ECOSYSTEME PUBLIC-PRIVE DE CYBERSECURITE

En application de la volonté du Président de la République de créer un campus cyber à la française, s'inspirant d'exemples étrangers (notamment Beer-Sheva en Israël), pour réunir en un même lieu des acteurs publics et privés de la cybersécurité, une société co-détenue à 45 % par l'État, *via* l'Agence des participations de l'État (APE), et à 55 % par des partenaires privés (120 entités) a été créée puis installée à partir de février 2022 dans une tour du quartier de La Défense à Puteaux. Dans le cadre de ses actions de politique industrielle visant à consolider la filière française de cybersécurité, l'ANSSI y a installé ses équipes dédiées à l'industrie, aux technologies, à l'innovation, à la formation et à la coordination avec les centres de réponse aux incidents de cybersécurité.

La visite effectuée par vos rapporteurs le 25 octobre 2022 a permis de rencontrer un panel de société représentant le secteur de la formation (EPITA), celui de l'offre de sécurité (Sekoia et Yes We Hack) ainsi que de constater la proximité immédiate des entreprises actrices ou bénéficiaires de cybersécurité telles que Thalès, Atos ou Cap Gemini. Pour la partie publique, il a été indiqué qu'outre l'installation de l'ANSSI, l'INRIA et le ComCyber participaient également au programme.

L'interpénétration et le croisement d'expérience des différents acteurs est de nature à faciliter les processus de formation et de recrutement de techniciens et d'ingénieurs ; les étudiants trouvant sur place leurs futures entreprises d'accueil pour un stage ou une embauche. À terme, près de 1 800 personnes sont appelées à participer au Campus, dont 1 200 présents sur le site.

Il est naturellement trop tôt pour présenter un bilan de l'activité du Campus Cyber mais l'on peut déjà noter plusieurs facteurs positifs tels que la montée en puissance très rapide des locations d'espace aux entreprises

(tout l'immeuble est occupé) et l'aboutissement d'un premier tour de table financier associant l'Etat, la Région Ile-de-France (2 millions d'euros) et, selon le président du Campus cyber, toutes les sociétés du CAC 40.

L'enjeu du dispositif, considéré d'ores et déjà comme un succès par les participants à la société, sera d'assurer sa **pérennité au-delà de la durée du plan France Relance 2021-2022** à partir duquel il a été financé au titre des actions de politique industrielle du volet cybersécurité du plan de relance.

C. SECURISER LA FIN DU PLAN FRANCE RELANCE ET PERENNISER LE SOUTIEN AUX COLLECTIVITES TERRITORIALES, AUX ETABLISSEMENTS DE SANTE 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

II. AUDITION DE MM. STEPHANE BOUILLON, SECRETAIRE GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE, ET DE GUILLAUME POUPARD, DIRECTEUR GENERAL DE L'AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (5 OCTOBRE 2022)

Au cours de sa réunion du mercredi 5 octobre 2022, la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Christian Cambon, président, a procédé à l'audition de MM. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), et de Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

M. Christian Cambon, président. - Dans le cadre de l'examen du projet de loi de finances (PLF) pour 2023, et plus particulièrement des crédits du programme 129 « Coordination du travail gouvernemental », nous accueillons aujourd'hui MM. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), et Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Il faut d'abord rappeler que l'Anssi n'est pas une autorité administrative indépendante, mais qu'elle est l'un des services en charge de la cybersécurité des services publics et du tissu économique et social français - elle est placée sous la direction du SGDSN. Cette audition est l'occasion de compléter le point annuel sur l'activité de gestion de crise et de coordination des conseils de défense dont le SGDSN a la charge par un focus plus particulier sur les attaques informatiques auquel notre pays, notamment les collectivités territoriales et les hôpitaux, doit faire face. Je pense à l'hôpital de Corbeil-Essonnes et à la ville de Caen, qui font l'actualité de la cybercriminalité.

Le PLF pour 2023 prévoit une augmentation des moyens du SGDSN, principalement destinée, comme les années précédentes, à renforcer nos moyens de lutte contre les cybermenaces. Pourrez-vous nous préciser dans le détail à quoi seront consacrés ces crédits supplémentaires ?

Par ailleurs, je rappelle que pour compléter notre arsenal cyberdéfensif dans le champ de la désinformation et des influences extérieures, un service à compétence nationale, dénommé Viginum, a été créé par voie réglementaire en juillet 2021. L'occasion vous est ici donnée de nous en présenter un premier bilan.

Enfin, dans le contexte de la guerre en Ukraine et de la multiplication des menaces étatiques, mais aussi criminelles, les deux pouvant d'ailleurs être liées, il nous apparaît tout à fait primordial que vous puissiez éclairer la représentation nationale sur les priorités qui seront données à vos services pour 2023 et les années suivantes. J'ai noté que le

budget du SGDSN progresserait en 2023 de 20 millions d'euros pour atteindre un total de près de 325 millions d'euros. Vers quels dispositifs ces crédits supplémentaires sont-ils fléchés ?

Par ailleurs, vous disposiez également de crédits du plan de relance pour 2022 pour mettre en place un dispositif spécifique de protection des systèmes d'information des collectivités territoriales et établissements publics. Comment et avec quels moyens allez-vous pérenniser ce programme en 2023 et les années suivantes ?

Je rappelle à tous que cette audition fait l'objet d'une captation vidéo qui est retransmise en direct sur le site internet du Sénat.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. - Durant les douze derniers mois, le SGDSN a dû s'occuper d'événements de nature très différente.

Les élections présidentielle et législatives nous ont amenés à travailler très étroitement avec les autorités chargées du contrôle de la campagne et du bon déroulement du processus électoral, notamment le Conseil constitutionnel, la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle ou encore l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), pour tenter de déceler les attaques informatiques contre les institutions ou les candidats, ainsi que les tentatives de manipulation de l'information.

Nous avons aussi suivi les effets de la reprise économique à la suite de la phase aiguë de la pandémie de covid-19 : inflation, tensions sur les microprocesseurs ou sur certains produits alimentaires, etc. Cela pèse naturellement sur la construction du budget de l'État.

C'est bien sûr la guerre en Ukraine qui nous occupe beaucoup. Elle fait vaciller les cadres conceptuels, remet en cause notre travail sur la non-prolifération, interroge sur la mise en œuvre du droit international. L'ensemble des équilibres géostratégiques sont remis en cause du fait de la désinhibition totale du chef d'un pays doté de l'arme nucléaire. De surcroît, ce pays utilise à grande échelle ce que l'on appelle les « menaces hybrides », c'est-à-dire des actions menées sous le seuil de conflictualité, sans que l'on puisse les attribuer, et ayant pour objectif de déstabiliser l'adversaire, voire de le neutraliser sans avoir à combattre directement. Je fais référence aux attaques cyber et aux manipulations de l'information, mais on peut aussi s'interroger sur les conditions dans lesquelles les gazoducs Nord Stream ont été coupés ces jours derniers. Une bonne part du travail du SGDSN a été consacrée au suivi de cette guerre.

Nous avons également travaillé sur la question de l'Indo-Pacifique. La montée en puissance de la Chine se traduit notamment par une activité cyber extrêmement importante, peut-être plus importante ces derniers mois que celle de la Russie. La Chine a ainsi essayé de pénétrer des réseaux pour faire de l'espionnage industriel à grande échelle.

Enfin, au Sahel, la pression de compétiteurs voulant attaquer la politique de la France et s'installer en Afrique a beaucoup occupé les différents services concernés.

Toutes ces questions ont évidemment été abordées au sein du Conseil de défense et de sécurité nationale. Je rappelle que l'organisation de ce Conseil est prévue par les textes et qu'il permet aux directeurs d'administration et aux chefs de service de donner la vision administrative des dossiers pour que le Président de la République puisse prendre les décisions qui relèvent de son pouvoir exécutif.

En 2023, notre action restera concentrée sur l'ensemble de ces enjeux majeurs.

Nous avons commencé à travailler sur la prochaine loi de programmation militaire (LPM) ; elle vous sera soumise au premier semestre 2023 et vous aurez un rôle éminent à jouer en la matière, y compris en amont de la présentation du texte. Nous devons prendre en compte le nouveau cadre d'action, dont j'ai évoqué certains éléments - c'est ce que certains appellent « la fin des dividendes de la paix ». Le Président de la République nous a fixé deux orientations : il souhaite articuler notre stratégie nationale autour de priorités simples, lisibles et adaptées à nos théâtres d'intérêts et à nos alliances ; il souhaite ensuite comprendre la déclinaison physico-financière des choix qui seront arrêtés.

Nous serons donc amenés à discuter des choix stratégiques avant d'aborder les questions de programmation, mais aussi à travailler sur ce que le Président de la République a appelé « l'économie de guerre ». Il s'agira notamment de regarder dans quelles conditions l'industrie de défense et toutes les entreprises qui travaillent pour ce secteur peuvent modifier leur façon de travailler afin d'être plus rapides et capables de reconstituer les stocks. Un exemple : les séries devront peut-être être un peu moins sophistiquées, mais plus régulières afin de répondre rapidement à nos besoins.

Nous sommes dans un processus de réflexion et de maturation et nous aurons besoin de votre appréciation et de votre avis dans cette phase.

Le PLF pour 2023 subit les conséquences de cette nouvelle donne.

Depuis plusieurs années, le SGDSN est de plus en plus sollicité et a pris en charge de nouvelles missions. Des services à compétence nationale ont été créés pour assurer le portage juridique de ces missions. Je ne citerai que quelques exemples : l'Anssi ; le groupement interministériel de contrôle (GIC), qui s'occupe des interceptions de sécurité, sur lequel je n'ai pas autorité, mais que nous gérons ; un opérateur de services informatiques destiné à regrouper l'ensemble des moyens de façon à répondre aux attentes techniques de l'État ; le nouveau service Viginum, service de vigilance et de protection contre les ingérences numériques étrangères.

Le budget opérationnel de programme (BOP) du SGDSN représente plus de 50 % des crédits totaux du programme 129 « Coordination du travail gouvernemental » : 37 % de ses crédits du titre 2 et 58 % des crédits hors titre 2. Le PLF pour 2023 prévoit de doter le SGDSN de 346,8 millions d'euros en autorisations d'engagement (AE) et de 324,5 millions en crédits de paiement (CP), soit une augmentation de 15,8 % en AE et de 6,5 % en CP par rapport à 2022. Près du tiers de ce budget est porté par des dépenses de masse salariale - 101,6 millions en CP -, les deux tiers restants constituant pour l'essentiel des dépenses de fonctionnement et d'investissement, à hauteur de 222,9 millions en CP.

La trajectoire financière pour 2023-2027 est déterminée par plusieurs éléments.

Elle est d'abord déterminée par les missions répondant à une demande particulière du Président de la République ou du Premier ministre.

Je pense notamment au plan « cyber » pour la France, à l'animation et au pilotage de la stratégie nationale de résilience - ce sont des sujets qui ont été inscrits dans le programme présidentiel - et au développement des dispositifs de communication sécurisée au profit des hautes autorités et des services territoriaux de l'État, en particulier le téléphone Osiris. Nous devons ainsi travailler, en lien avec l'affaire Pegasus, sur la question des téléphones sécurisés : ce seront des téléphones plus sécurisés, mais moins ergonomiques - ils ne permettront pas de naviguer sur internet, mais nous serons sûrs qu'il n'y aura pas d'oreilles indiscrettes...

Parmi ces missions, je citerai également la prise en compte des enjeux spatiaux tant sur le plan industriel qu'au niveau européen : nous devons nous adapter aux évolutions géostratégiques - dans ce secteur, beaucoup d'équipements étaient produits en Ukraine, parfois en connexion avec la Russie. Nous avons ainsi créé un bureau en charge des affaires spatiales au sein du SGDSN. Je citerai enfin la lutte contre les agences numériques étrangères et la mise en œuvre de la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement - le GIC disposera d'un nouveau bâtiment à Montrouge, que nous devons protéger.

Ensuite, la trajectoire financière est déterminée par la consolidation de la montée en puissance organique du SGDSN. Nous avons un important programme d'opérations immobilières, par exemple pour l'Anssi, qui disposera d'un nouveau bâtiment à Rennes - 25 millions d'euros sont consacrés à ce projet.

À la suite de la réforme de l'Institut des hautes études de défense nationale (IHEDN), nous avons obtenu une hausse de 750 000 euros de la subvention qui lui est versée. L'Institut réduira ses frais de fonctionnement, mais accueillera davantage de stagiaires et augmentera son rayonnement.

Par ailleurs, un certain nombre de postes de dépenses du SGDSN se rigidifient, en particulier les crédits de transfert au bénéfice de capacités

techniques interministérielles (CTIM). Et il faut prendre en compte des dépenses nouvelles comme Viginum ou le campus cyber, inauguré l'an passé et pour lequel 14,2 millions d'euros sont prévus sur six ans. Je veux aussi évoquer dans ce cadre l'importance du volume des restes à payer - 104,3 millions d'euros au début de 2022 - induits par les indispensables opérations d'investissement et immobilières conduites ces dernières années.

Ce phénomène de rigidification sera accentué en 2023 sous l'effet de la hausse significative des coûts de l'énergie, plus particulièrement ceux de l'électricité, hausse qui se traduira par une multiplication par 3,5 de ce poste de dépenses - 5 millions d'euros contre 1,5 million.

Pour en revenir à nos missions, je veux dire que l'évolution chaotique du cadre géopolitique, le retour de la violence à grande échelle et haute intensité en Europe ou encore la multiplication des crises donnent une acuité particulière aux travaux que nous avons engagés au printemps sur la question de la résilience. Jean Castex, alors Premier ministre, avait confié au SGDSN une mission de réflexion et de rédaction d'une stratégie nationale de résilience. Un projet, issu d'un travail mené avec les ministères, lui a été remis au mois de mai. L'idée générale est de mieux identifier nos faiblesses et de mettre en œuvre des actions correctives, faisant l'objet d'indicateurs de suivi. L'idée est de réformer la planification et les outils de gestion de la crise dans le sens d'une plus grande polyvalence des plans et d'une simplification des outils de réponse à la crise, en nous attachant notamment à la question des stocks - nous avons appris que nous devons compter sur nos propres efforts en la matière.

Encore plus loin, l'objectif final est d'« embarquer » la population, grâce au concours de ceux que nous n'avons pas assez associés jusque-là : collectivités territoriales, associations ou encore comités communaux - ces comités sont, par exemple, essentiels pour prévenir et gérer les feux de forêts et leurs conséquences. Le but ultime est de parvenir à préparer l'ensemble de la population à faire face à une situation de crise. Il s'agit de faire de nos concitoyens des « consom'acteurs », pour reprendre l'expression d'une parlementaire.

La guerre en Ukraine donne une nouvelle perspective à nos réflexions. La destruction d'éléments des gazoducs Nord Stream I et II démontre que les infrastructures civiles - satellites, câbles... - sont des cibles pour des États sans scrupules. Parallèlement, le prix des hydrocarbures et les risques de pénurie d'énergie sont des moyens de pression utilisés par la Russie sur les populations européennes. Nous travaillons donc à organiser les choses de façon que, par exemple, d'éventuels délestages, que nous faisons tout pour éviter, n'aient pas d'effets mal maîtrisés.

Les ministères dialoguent avec les opérateurs, y compris dans le domaine des télécoms. En complément, nous avons organisé et nous continuerons à organiser plusieurs exercices de gestion de crise afin de

mettre à jour d'éventuelles faiblesses, de corriger nos plans et de veiller à ce que l'ensemble de nos concitoyens puissent faire face à la situation.

Nous devons faire face à une menace forte d'États comme la Chine ou les États-Unis, qui peuvent être tentés d'imposer leur mainmise et dominer les autres États sur un plan technique, réglementaire ou judiciaire. Il nous faut donc nous organiser aux niveaux national et européen.

Viginum a été créé en 2021 pour lutter contre les attaques informationnelles de l'étranger. La lutte informationnelle est devenue l'un des principaux enjeux de notre temps et la principale mission de Viginum. Il y a actuellement 42 agents dédiés, et ils seront 65 à terme pour détecter les attaques informationnelles venant de l'étranger. Le service a été mis à l'épreuve lors des élections et lors du référendum en Nouvelle-Calédonie. Nous avons rendu compte au Conseil constitutionnel de tout ce que nous avons pu observer.

Dans le cadre de cette mission, je préside également deux comités interministériels pour coordonner l'action de tous les services de l'État. Nous avons vocation à être des boucliers. Notre rôle n'est pas de dire ce qu'est la vérité, mais de mettre au jour des phénomènes potentiellement « inauthentiques » ayant cours sur des plateformes en ligne et susceptibles de révéler une ingérence numérique étrangère. Pour ce faire, Viginum recherche des marqueurs d'inauthenticité dans le débat public numérique : comptes atypiques, contenus susceptibles d'être inexacts ou trompeurs, comportements aberrants, anormaux ou coordonnés. Viginum s'appuie notamment sur des indicateurs mathématiques ou des outils informatiques conçus par ses spécialistes en analyse de la donnée.

À partir de là, on observe la menace et on essaie de la caractériser pour vérifier si les phénomènes répondent ou non aux critères établis dans le décret pour définir une ingérence numérique étrangère et, partant, s'ils sont susceptibles d'entraîner une réponse des autorités, qui peut être politique, par un contre-discours, diplomatique ou judiciaire, au moyen de la loi de 2018 sur les manipulations de l'information ou de la loi de 1884 sur la liberté de la presse.

Sur une année d'existence, le service a identifié 84 phénomènes qualifiés d'inauthentiques. Le principal enseignement de cette année d'existence est donc l'omniprésence de tels phénomènes, même s'ils ne sont pas tous massifs ni dangereux. Néanmoins, ils ont tendance à augmenter, notamment lors des échéances électorales. Il s'agit principalement d'essayer de discréditer nos institutions démocratiques. Pour contrer ce phénomène, nous travaillons en étroite collaboration avec nos partenaires étrangers, comme le Royaume-Uni ou les États-Unis.

Je termine par la cybermenace, sur laquelle Guillaume Poupard sera évidemment beaucoup plus complet que moi. Je peux simplement dire que celle-ci augmente d'année en année. Nous avons, l'année dernière, mis au

point avec le Premier ministre toute une série d'actions pour vérifier que nos administrations, nos ministères, nos établissements publics n'étaient pas susceptibles d'être attaqués, ou en tout cas que nous pouvions être en capacité de répondre à ces événements. L'Anssi a donc beaucoup travaillé et continue à travailler avec toutes ces administrations pour renforcer la résistance de leurs systèmes informatiques aux attaques qui pourraient se produire, et elle fait évidemment de même, à travers le plan de relance, avec les établissements publics. Nous essayons de décentraliser cette action. Ainsi des centres de réponse aux alertes et aux attaques ont été créés dans toutes les régions, à l'exception d'une, pour faire face aux attaques.

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information. - La menace n'évolue clairement pas dans le bon sens. Il n'y a pas de bonne nouvelle, mais nous pouvons être optimistes sur notre capacité à y répondre.

En 2020, nous avons reçu 786 signalements d'attaque. Il y en a eu certainement plus, mais seules 786 étaient du niveau de l'Anssi. En 2021, il y en a eu 1082, soit une hausse de 37 %. La croissance peut donc être qualifiée d'exponentielle au sens mathématique du terme.

Trois grandes menaces nous préoccupent : secteur criminel, activité d'espionnage, action militaire, c'est-à-dire destructive. Ce sont trois menaces différentes, qu'il ne faut pas mélanger.

La menace criminelle, comme à l'hôpital de Corbeil-Essonnes, est en voie de stabilisation sur un palier très haut, puisque l'Anssi est impliquée sur à peu près 200 opérations. Le mode opératoire est peu ou prou toujours le même : il s'agit d'entrer dans un système d'informations pour en bloquer et en voler les données, puis se livrer à un chantage. Dans le cas d'un hôpital, il y a alors un vrai risque pour la sécurité médicale des personnes et la crainte de voir des données intimes diffusées, ce qui rend les arnaques financières plus aisées. Les cibles sont le plus souvent des entreprises de taille intermédiaire (ETI).

Nous essayons d'anticiper en diffusant des messages de prudence pour que les systèmes d'information des victimes potentielles soient les plus robustes possible. Quand on en est à se poser la question de payer ou non la rançon, il est déjà trop tard.

Nous avons mené 17 opérations en 2021. Une opération, c'est quelque chose de très grave, car cela implique une intervention massive de moyens de la part de l'agence, de nos partenaires et de prestataires privés. Sur ces 17 opérations, 14 concernaient des affaires d'espionnage, dont 9 semblaient correspondre à des modes opératoires d'origine chinoise. Ce sont des opérations très complexes faisant intervenir tout un écosystème obscur mêlant acteurs publics et privés. En résumé, l'espionnage, c'est 80 % de l'activité de l'Anssi.

La menace militaire, c'est celle qui vise non pas à espionner ou à faire chanter, mais à détruire des systèmes d'information. C'est notre priorité, car cela pourrait avoir des conséquences dramatiques en matière de sécurité nationale. Le premier constat à faire, c'est qu'une telle attaque ne s'est pas encore réalisée, même depuis le début de la crise ukrainienne. Il ne faut pas pour autant sous-estimer la Russie en la matière. On l'a vu avec SolarWinds en 2020.

La clé réside dans la construction d'un véritable écosystème. Un travail étroit est mené avec un certain nombre de partenaires afin d'aboutir à une compréhension fine des modes opératoires et de proposer des stratégies efficaces. Aujourd'hui, je peux dire que nous sommes arrivés à un système de cyberdéfense performant.

À ce stade, permettez-moi de faire la publicité de notre plateforme d'information cybermalveillance.gouv.fr, qui peut permettre à tout un chacun de réviser les règles élémentaires en matière de cybersécurité.

Enfin, je veux revenir sur le Campus Cyber, qui est une initiative public-privé remarquable. Sur 26 000 mètres carrés à La Défense, il associe l'Anssi, des chercheurs, des représentants de grands groupes dans une alchimie très précieuse pour diffuser l'information et proposer des formations en matière de cybersécurité.

Pour conclure, je rappelle que notre action doit nécessairement s'inscrire dans un cadre européen. La cybersécurité a d'ailleurs été l'un des marqueurs de la présidence française de l'Union européenne. L'entraide européenne est absolument fondamentale.

M. Olivier Cadic, rapporteur pour avis des crédits du programme "Coordination du travail gouvernemental". - Messieurs, vous avez évoqué devant nous le nombre d'attaques en 2020 et 2021, mais pouvez-vous faire un point plus détaillé, à date, de la situation en 2022 ? Quelles sont vos prévisions pour 2023, et vous estimez-vous suffisamment dotés en effectifs pour y faire face ?

Par ailleurs, vous avez souligné que les attaques par rançongiciel et blocage des systèmes d'information de collectivités, comme la ville de Caen, et d'hôpitaux, comme celui de Corbeil-Essonnes, se multipliaient. Quelle a été l'action de l'Anssi dans les cas cités ? Où se situent les responsabilités ? Si les recommandations de l'Anssi ne sont pas appliquées, n'est-ce pas la responsabilité des hôpitaux ou des collectivités qui risque d'être engagée ? Pour ma part, je pense qu'il serait totalement contreproductif, voire dangereux de banaliser un quelconque paiement des rançons.

Vous avez évoqué les questions d'espionnage, notamment de la Chine, de manière très diplomatique. Quelles sont les nouvelles menaces ? La pression se faisant toujours plus forte, faut-il s'inquiéter ?

Les câbles sous-marins peuvent-ils constituer un point de danger pour nos systèmes informatiques ?

J'aimerais également évoquer la dissuasion. Que pouvez-vous nous dire sur les pirates ? Sommes-nous en mesure de les bloquer ? Combien d'entre eux ont été arrêtés ces dernières années ? La stratégie américaine est très offensive : le FBI recherche les auteurs des faits, bloque les serveurs, délivre des mandats d'arrêt internationaux - un de nos jeunes compatriotes a récemment été arrêté au Maroc en lien présumé avec une attaque cyber aux États-Unis. Pouvons-nous procéder de la sorte pour envoyer un message de fermeté aux États et organisations hostiles ?

Nous avons observé les narratifs, dont celui de la Chine, repris par la Russie. J'ai consulté un site d'histoire, par exemple, qui reprenait très exactement le narratif de la Chine sur Taïwan. Il suffit de suivre un discours du Président de la République pour observer l'action des robots installés en Russie qui cherchent à décrédibiliser la parole du Président sur Facebook ou Twitter au moment même où elle est prononcée. Le week-end dernier, au Burkina Faso, certains sites étaient animés depuis la Russie pour inciter la population à mettre le feu à l'ambassade de France. On pouvait même voir des drapeaux russes au sein des manifestations. Envisagez-vous de contre-attaquer et, si oui, comment ?

M. Mickaël Vallet, rapporteur pour avis des crédits du programme "Coordination du travail gouvernemental". - Le plan de relance allouait 136 millions d'euros au financement de prestations et à la création de centres régionaux de réponses cyber de proximité. Quel est le taux de participation des conseils régionaux ? Disposez-vous encore de marges de manœuvre ?

Un urgentiste expliquait hier, sur *La Chaîne parlementaire*, que l'attaque contre l'hôpital de Corbeil-Essonnes avait eu des conséquences très concrètes, notamment un « délestage » sur les hôpitaux voisins. Que se passerait-il si une attaque de cette ampleur frappait un hôpital où les possibilités de délestage sont moindres, comme dans certains territoires d'outre-mer ?

Vous avez évoqué la plateforme cybermalveillance.gouv.fr : quel en est le bilan chiffré ? Il s'agit d'un dispositif extrêmement concret pour nos concitoyens. Avez-vous constaté une augmentation des plaintes ?

Certains esprits plus ou moins chagrins se sont émus de la concomitance entre un accord de fourniture d'énergie par les Américains et un autre accord sur les systèmes numériques, qui aurait été trouvé après plusieurs annulations par la justice européenne. Ferions-nous preuve de naïveté dans la façon dont nous partageons nos données avec un partenaire dont l'action serait, selon certains, « à géométrie variable » en fonction des sujets ?

Allez-vous mettre en place une organisation particulière pour les jeux Olympiques de Paris de 2024 ?

Un article du projet de loi d'orientation et de programmation du ministère de l'intérieur précise qu'il faut porter plainte après avoir payé une rançon. Le problème est non pas tant de porter plainte que d'inscrire dans le marbre de la loi la possibilité de payer une rançon. Quel signal envoie une telle disposition ?

M. Stéphane Bouillon. - En raison du principe de libre administration des collectivités locales et des établissements publics, il revient au directeur général d'un hôpital et à son conseil d'administration de bien prendre en compte les menaces existantes et la manière dont il faut y répondre. Il en va de même des mairies - la mairie de Caen a pu s'appuyer sur un solide service informatique, qui a su prendre les mesures de précaution immédiates nécessaires. Une attaque récente contre l'hôpital de Cahors a également pu être déjouée assez facilement, car les investissements nécessaires avaient été réalisés.

De mémoire, 25 millions d'euros de crédits étaient inscrits au budget l'année dernière pour soutenir les hôpitaux ; le Gouvernement vient de décider de rajouter 20 millions cette année. Des crédits similaires sont alloués aux collectivités locales. Il appartient ensuite à chacune de ces structures de prendre les solutions nécessaires.

Nous sommes extrêmement sensibilisés à la question de la protection des câbles sous-marins. Il est plus complexe d'interrompre internet qu'un gazoduc, la redondance du système permettant au circuit de passer d'un câble à un autre. Nous réfléchissons, dans le cadre de la prochaine loi de programmation militaire, à la question des grands fonds marins et à la prévention des attaques. Nos sociétés étant de plus en plus numérisées, une interruption d'internet aurait des conséquences extrêmement dramatiques.

Lorsqu'il est possible de poursuivre les auteurs d'attaques sur le plan juridique, nous essayons de le faire. Toutefois, il est extrêmement difficile d'attribuer une cyberattaque à un pays. Il en va de même en matière d'ingérence numérique étrangère. Cela pose également un problème en termes d'assurance : la Lloyd's a décidé de ne plus réassurer les sinistres commis par des États à partir de 2023. La difficulté va résider dans notre capacité à attribuer une attaque à un État. Il s'agit d'un acte à la fois technique, juridique et politique.

La plus célèbre attribution est celle de l'aveuglement du satellite ViaSat, le matin de l'offensive russe en Ukraine. Il s'agissait d'aveugler les communications sur le champ de bataille, ce qui a également neutralisé les modems de ce satellite sur une bonne partie de l'Europe.

Il est sans doute possible de contre-attaquer, mais il faudra que vous interrogiez d'autres que moi sur cette question. Nous avons tous noté que les chemins de fer biélorusses, au début de l'attaque, ont connu des désagréments sans doute dus à la vétusté de certains appareils. C'est

simplement arrivé au mauvais moment pour eux, et au bon moment pour les Ukrainiens...

Il s'agit également d'une guerre dissymétrique : en cas de coupure d'un service public en France, les médias en parleront et on nous demandera des comptes ; dans un certain nombre d'autres pays, personne n'osera protester...

On peut essayer d'identifier les hackers, de les rechercher et de mener des enquêtes efficaces. Ce fut le cas l'année dernière, les polices européennes réussissant à neutraliser plusieurs hackers agissant comme des relais russes. Un certain nombre de poursuites ont aussi pu être engagées, toujours contre des hackers russes, grâce aux renseignements fournis par leurs anciens associés pro-ukrainiens.

Lors du comité Olympique de juillet dernier, le chef de l'État et la Première ministre ont décidé que l'Anssi serait en charge du pilotage de la sécurité des Jeux Olympiques 2024. L'Agence est en train de mettre en place une série de dispositifs. Les opérateurs les plus sensibles feront l'objet d'une surveillance constante.

Nos relations avec les États-Unis sont à la fois indispensables et de qualité. La semaine prochaine, je me rendrai à Washington pour rencontrer mes homologues et discuter de ces questions. En général, ils nous ouvrent assez largement leurs portes. Bien évidemment, la formule selon laquelle un État n'a pas d'ami, mais seulement des intérêts, est toujours de mise. Il n'en demeure pas moins que les États-Unis sont pour nous un allié majeur, essentiel, de longue date, avec lequel nous avons pu avoir des différends, mais avec qui nous travaillons en confiance à la fois pour nous développer et pour assurer notre propre sécurité. Les services américains nous ont beaucoup aidés sur le sujet des menaces hybrides. Nous poursuivons cette collaboration, que nous souhaitons confiante et efficace.

M. Guillaume Poupard. - Les chiffres de 2021 montrent une stabilisation, sur un palier haut, des attaques par rançongiciel et une pression toujours plus forte de l'espionnage. Il existe une vraie crainte autour des attaques pouvant engendrer des dégâts physiques. Les choses vont probablement continuer selon ce schéma en 2023 et 2024.

La question de la responsabilité se pose et se posera de plus en plus. Aujourd'hui, les responsables des hôpitaux sont davantage des victimes que des coupables. Nous les aidons et les incitons fortement à développer leurs défenses. En concertation avec le ministère de la santé, nous avons désigné plus d'une centaine d'hôpitaux « opérateurs de services essentiels ». Ce statut les oblige à se protéger, à mettre en œuvre les règles de sécurité que nous imposons et à financer ces dispositifs. S'ils ne le faisaient pas, ce serait une forme de négligence que nous pourrions leur opposer dans une dizaine d'années, mais pas aujourd'hui.

En parallèle, le plan de relance est arrivé au bon moment pour aider les hôpitaux à faire un bilan. Nous avons financé des prestataires pour les aider à élaborer un plan d'action. Ces crédits, à hauteur d'une centaine de milliers d'euros par structure aidée, ont permis de débloquer les choses. Charge aux hôpitaux d'effectuer ce travail de rattrapage.

Dès lors que l'on s'interroge sur le paiement d'une rançon, il est déjà trop tard. Il n'y a plus alors de bonne solution. Il ne faut pas se tromper de message et dissuader fortement le paiement des rançons, qui va alimenter le crime organisé. Cet argent sera réutilisé pour attaquer encore plus de victimes. Toute disposition, quand bien même elle semblerait de bon sens, qui pourrait laisser croire que le paiement d'une rançon est quelque chose d'anodin enverrait un terrible message.

Bien évidemment, quand on n'a pas eu le choix, il faut systématiquement déposer plainte après paiement - le rappeler n'est pas forcément inutile. De même, cela permet de rassurer les assureurs qui peuvent ainsi intégrer le paiement dans une stratégie d'accompagnement de leurs clients. Pour autant, laisser penser qu'il suffit de payer pour tout régler serait totalement contreproductif.

La dissuasion est essentielle. Il nous faut durcir le ton. La voie judiciaire commence à donner des fruits grâce à l'entraide internationale. Nous avons rencontré de très beaux succès, qui nous encouragent dans cette voie. Mais nous savons que les attaquants et experts des services de renseignement de certains grands pays adverses resteront toujours hors d'atteinte. La voie judiciaire ne peut tout régler.

Je veux tout d'abord rappeler que la meilleure défense, c'est la défense, et que la prévention est absolument essentielle. À côté, il nous faut également disposer de capacités offensives mobilisables pour mettre une pression sur nos adversaires. Nous y réfléchissons avec nos partenaires américains. Il s'agit d'élever le coût des attaques pour nos adversaires.

Nous avons lancé des centres opérationnels en lien avec les conseils régionaux et les préfetures de région. Les choses se mettent en place dans douze de nos régions. Ce dispositif permet d'impliquer tout le tissu intermédiaire économique, ce que l'Anssi ne saurait faire seule. Disposer d'un centre opérationnel capable de répondre soit en amont, soit en cas de véritable attaque est essentiel.

Nous avons également mis en place les parcours de sécurité des collectivités locales et de quelques opérateurs publics, ce qui représente beaucoup d'argent, mais a permis d'élever véritablement le niveau de sécurité. Je dois vous avouer avoir utilisé une partie des crédits du plan de relance pour équiper l'Anssi à des fins de détection. Ces crédits, qui ne figurent pas techniquement au programme 129, me manqueront en 2023, ce qui risque d'entraîner une tension sur le budget de l'Anssi.

Une attaque systémique sur les hôpitaux serait catastrophique, mais difficilement réalisable en raison de l'hétérogénéité des systèmes numériques des établissements. Par contre, il ne serait pas possible de réaliser de délestage dans certains territoires ultramarins. Nous portons une attention particulière à ces questions et le plan de relance a également permis de développer des centres de ressources mutualisés dans les territoires d'outre-mer. Ces initiatives vont permettre de disposer de personnes compétentes sur place, ce qui est souvent la principale carence dont souffrent ces territoires.

Je ne dispose pas encore des chiffres de la plateforme cybermalveillance.gouv.fr, mais nous pourrions vous les faire parvenir. La plateforme permet d'aider de plus en plus de personnes à mesure qu'elle gagne en notoriété, comme le montrent les études. Elle devient même une sorte de capteur, qui nous permet d'anticiper certains phénomènes de cybercriminalité.

En ce qui concerne les accords entre l'Union européenne et les États-Unis sur le traitement des données, c'est une histoire qui se répète : l'accord *Safe Harbor* a été cassé par la justice européenne ; un deuxième accord, *Privacy Shield*, a également été cassé ; un troisième accord, que je ne connais pas, est en cours de négociation, mais je ne doute pas qu'il sera aussi cassé dans quatre ans. Plutôt que de nous lamenter, nous développons un référentiel, dénommé « SecNumCloud », pour détailler ce que nous attendons d'un système d'informatique nuagique à un haut niveau de sécurité. Le référentiel indique clairement que le contrôle des sociétés opérant ces services ne doit pas être extra-européen, afin de nous prémunir contre les arrêts de la justice européenne.

Les Jeux Olympiques vont beaucoup nous occuper. Le travail est en cours. Il est mené en lien étroit avec le ministère de l'intérieur. Nous allons devoir protéger deux types d'acteurs : ceux que l'on connaît déjà, avec lesquels les liens sont déjà établis, et ceux, beaucoup plus éphémères, qui sont liés à l'événement. À nous de nouer des liens rapidement pour que tout fonctionne le jour J. Nous savons déjà qu'il y aura des attaques. Il s'agit d'un moment idéal pour nos adversaires, alors que toutes les caméras du monde seront braquées sur nous.

M. Olivier Cigolotti. - La question de cyberattaques d'ampleur sur les systèmes informatiques est souvent soulevée, mais il existe aussi une menace sur les câbles sous-marins, alors même qu'ils permettent de faire transiter plus de 99 % des données. Avons-nous les moyens d'assurer la surveillance et la sécurité de ces infrastructures ? Existe-t-il une stratégie européenne coordonnée en la matière ?

Mme Marie-Arlette Carlotti. - Constatez-vous des difficultés pour recruter et conserver dans les armées des spécialistes de la cybersécurité ? La

concurrence du secteur privé est très forte, et on nous a indiqué que la moitié des effectifs partait dans les cinq ans suivant leur recrutement.

M. Hugues Saury. - Les prix du gaz, de l'électricité et des biens de consommation courante ont augmenté de façon importante, mettant nos concitoyens dans des situations critiques. Certaines voix appellent à ne pas minimiser le risque d'un mouvement citoyen de masse et invitent à écouter les signaux faibles. Les menaces terroristes et numériques font l'objet d'une grande et salutaire attention, mais de quels moyens est doté le SGDSN pour analyser les risques de fractures et d'émergence de mouvements sociaux qui pourraient basculer demain dans la violence ?

M. François Bonneau. - Des champions français, comme OVH, Atos ou Thales, sont présents dans le secteur du *cloud*, dans lequel les enjeux de souveraineté et de confiance deviennent prégnants, mais ces champions sont tous adossés à des Gafam - Google, Apple, Facebook, Amazon, Microsoft. Comment pouvez-vous garantir que des données sensibles ne puissent pas être lues par des puissances étrangères au travers du *cloud* ?

M. Guillaume Gontard. - Nous connaissons un certain nombre de crises : le covid-19, la guerre en Ukraine, la canicule et, plus globalement, le dérèglement climatique. Les aléas climatiques notamment font peser une menace très forte sur la stabilité mondiale, la santé, l'alimentation, l'approvisionnement en énergie ; ils entraînent des déplacements de population. Menez-vous une réflexion sur l'adaptation de nos sociétés et sur la résilience ? Êtes-vous en contact avec des centres de recherche sur ces sujets ?

En ce qui concerne les cyberattaques sur les petites et moyennes entreprises (PME), on nous dit parfois que les rançons, souvent petites, sont payées, en particulier parce que cela coûte moins cher que de faire venir des spécialistes. Comment faire évoluer les choses ?

M. André Gattolin. - L'Anssi a publié en mars dernier un excellent rapport sur les menaces informatiques, lequel fait état d'une augmentation des intrusions avérées de 37 %. Les attaques par rançongiciel augmentent particulièrement à l'encontre des très petites entreprises (TPE), des PME et des ETI. Cette augmentation provient-elle d'une meilleure déclaration de la part des entreprises - on nous a souvent dit qu'elles avaient peur quant à leur réputation en cas d'attaque -, donc d'une plus grande confiance de leur part ? Je sais que la question de la confiance se pose aussi dans le secteur universitaire.

M. Joël Guerriau. - Disposez-vous d'éléments d'évaluation au niveau national pour apprécier le niveau global de préjudice en cas de rançongiciel ? Quel est le coût de l'ensemble des moyens mis en œuvre pour lutter contre les cybermenaces ?

Mme Joëlle Garriaud-Maylam. - Le ministère des armées dépend beaucoup de Microsoft, alors que la gendarmerie et d'autres ministères

européens de la défense utilisent des logiciels libres. La dépendance vis-à-vis de Microsoft ne constitue-t-elle pas une forme de fragilité ?

Vous avez évoqué des coopérations avec l'Union européenne, mais vous n'avez pas mentionné l'Otan. Or cette organisation réfléchit à l'idée d'intégrer les cyberattaques dans le champ de l'article 5 du traité.

M. Stéphane Bouillon. - Monsieur Cigolotti, nous discutons avec l'Union européenne de la question des câbles sous-marins, mais il n'y a pas de stratégie commune. Nous regardons ensemble comment monter des structures de résilience, mais chaque État est indépendant en la matière et travaille avec les opérateurs pour parer la menace et trouver des moyens de contournement en cas de problème.

Madame Carlotti, l'Anssi comme Viginum réussissent à attirer des talents, notamment grâce à leur image de marque - il est valorisant d'avoir travaillé à l'Anssi - et au sens du service public de nombreuses personnes, qui apprécient de contribuer à la protection de leurs concitoyens, quitte à être moins bien payées que dans le privé.

Monsieur Saury, le SGDSN n'est pas un service de renseignement, Viginum non plus. Nous travaillons sur les agences numériques étrangères et nous nous sommes interdit de surveiller le théâtre politique français - cela relève notamment du renseignement territorial en ce qui concerne le ministère de l'intérieur.

Monsieur Gontard, pour ce qui concerne les crises climatiques, nous travaillons effectivement avec un certain nombre de laboratoires. Je suis en train de passer un accord avec Climat 21 pour faire en sorte que nous puissions mieux anticiper et évaluer ce genre de menaces.

Madame Garriaud-Maylam, nous travaillons aussi avec l'Otan, mais nous restons prudents, car il s'agit d'une alliance militaire, et il convient de résister aux tentatives hégémoniques de certains membres qui ne sont pas membres de l'Union européenne.

M. Guillaume Poupard. - Le taux de départ des cybercombattants s'établit entre 15 % et 20 %, ce qui, pour des contractuels, est plutôt raisonnable. Qu'ils partent dans le privé n'est pas une catastrophe. C'est même plutôt une chance selon moi, car cela renforce l'écosystème dont je parlais précédemment.

Monsieur Bonneau, on n'est pas capable de faire du *cloud* de haut niveau en France aujourd'hui avec des technologies exclusivement françaises et développées en France. Il faut travailler avec des fournisseurs de technologie, notamment américains, ce qui nuit à notre souveraineté. Néanmoins, nous sommes en mesure de conserver un certain contrôle.

Avec les Gafam, le niveau de sécurité est très important. Il y a des risques résiduels, notamment juridiques, et il est important de travailler sur

des solutions qui permettent d'éliminer le plus possible ces risques, raison pour laquelle on voit apparaître des associations qualifiées d'hybrides.

Monsieur Gattolin, sur la sécurité des PME, la tendance est à l'augmentation des attaques. Il faut savoir que les rançons sont bien proportionnées à la taille des entreprises, ce qui explique la tentation très forte des victimes ou des assureurs de payer, la reconstruction pouvant coûter beaucoup plus cher. Cependant, c'est la garantie de se faire de nouveau attaquer dans la foulée par d'autres.

Sur l'espionnage, il y a de l'inquiétude. Il faut aussi avoir de la chance pour détecter certaines attaques masquées derrière une activité criminelle.

Monsieur Guerriau, sur les préjudices financiers, je n'ai pas de chiffres fiables, mais cela peut aller jusqu'au dépôt de bilan.

Je termine sur les logiciels américains. Dire que le logiciel libre est plus sûr que les logiciels américains est une légende. Tout est une question de maîtrise des outils. Vous avez cité la gendarmerie nationale, qui a cette culture, mais cela a un coût important en matière d'expertise.

LISTE DES PERSONNES AUDITIONNEES

Auditions de la commission

Mercredi 5 octobre 2022 :

- **M. Stéphane Bouillon**, secrétaire général de la défense et de la sécurité nationale (SGDSN) et **M. Guillaume Poupard**, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Déplacements et auditions des rapporteurs

Jeudi 22 septembre 2022 :

- **M. Gabriel Ferriol**, Chef du Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) ; **Mme Claire Benoit**, cheffe du pôle coordination et stratégie de Viginum ; **M. Gwenaël Jézéquel**, Conseiller pour les relations institutionnelles et la communication du SGDSN.

Mardi 4 octobre 2022 :

- **M. Guillaume Poupard**, Directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Jeudi 6 octobre 2022 : Table ronde avec le Cyber cercle :

- **Mme Stéphanie Bourlois**, CEO, cabinet SB & BD ; **M. Christian Daviot**, senior advisor, CyberCercle ; **Mme Ingrid Dumont**, responsable du projet de recherches, DRIF FH ; **M. Michel Dubois**, adjoint au directeur de la cybersécurité, Groupe La Poste ; **Mme Astrid Froidure**, chargée de mission cybersécurité, centres de gestion Calvados et Seine-Maritime - senior advisor, CyberCercle ; **M. Fabien Malbranque**, RSSI, Health Data Hub ; **M. Stéphane Meynet**, président, CERTitude NUMERIQUE - senior advisor, CyberCercle ; **M. Jérôme Notin**, directeur général, Cybermalveillance.gouv.fr ; **Mme Bénédicte Pilliet**, présidente, CyberCercle.

Mardi 25 octobre 2022 :

- **Général Pascal Ianni**, porte-parole du chef d'état-major des armées ;

- Visite du Campus Cyber : **M. Michel Van Den Berghe**, Président du Cyber Campus ; **M. Emmanuel Naegelen**, directeur adjoint de l'ANSSI ; **M. Philippe Dewost**, Directeur général de l'EPITA ; **M. Antonin Caors**, Sekoia, M. Guillaume Vassault-Houlière, Yes We Hack.

Jeudi 27 octobre 2022 :

Ambassade des États-Unis d'Amérique.

Vendredi 28 octobre 2022 :

- **Mme Nathalie Kestener**, Administratrice, Crédit Coopératif ;
- **Ambassade de Grande-Bretagne.**

Mercredi 2 novembre 2022 :

- **M. Thiébaud Meyer**, directeur Google Cloud et **M. Frédéric Géraud**, directeur affaires publiques Google Cloud.

Vendredi 4 novembre 2022 :

M. Andrew Howard, CEO, Kudelski Security ; **M. Sy Goodman**, Professeur à la School of Cybersecurity de l'université Georgia Tech ; **M. Richard DeMillo**, Professeur à la Warren Chair of Computing de l'université Georgia Tech ; **M. Larry Williams**, Président-Directeur general du National Technology Security Coalition (NTSC).