N° 82

SÉNAT

SESSION ORDINAIRE DE 2019-2020

Enregistré à la Présidence du Sénat le 22 octobre 2019

RAPPORT D'INFORMATION

FAIT

au nom de la commission des finances (1) sur la **sécurité informatique** *des* **pouvoirs publics**,

Par M. Jérôme BASCHER,

Sénateur

(1) Cette commission est composée de : M. Vincent Éblé, *président ;* M. Albéric de Montgolfier, *rapporteur général ;* MM. Éric Bocquet, Emmanuel Capus, Yvon Collin, Bernard Delcros, Philippe Dominati, Charles Guené, Jean-François Husson, Mme Christine Lavarde, MM. Georges Patient, Claude Raynal, *vice-présidents ;* M. Thierry Carcenac, Mme Nathalie Goulet, MM. Alain Joyandet, Marc Laménie, *secrétaires ;* MM. Philippe Adnot, Julien Bargeton, Jérôme Bascher, Arnaud Bazin, Jean Bizet, Yannick Botrel, Michel Canevet, Vincent Capo-Canellas, Philippe Dallier, Vincent Delahaye, Mme Frédérique Espagnac, MM. Rémi Féraud, Jean-Marc Gabouty, Jacques Genest, Alain Houpert, Éric Jeansannetas, Patrice Joly, Roger Karoutchi, Bernard Lalande, Nuihau Laurey, Antoine Lefèvre, Dominique de Legge, Gérard Longuet, Victorin Lurel, Sébastien Meurant, Claude Nougein, Didier Rambaud, Jean-François Rapin, Jean-Claude Requier, Pascal Savoldelli, Mmes Sophie Taillé-Polian, Sylvie Vermeillet, M. Jean Pierre Vogel.

SOMMAIRE

Pages

LES PRINCIPALES OBSERVATIONS ET RECOMMANDATIONS DU RAPPORTEUR SPÉCIAL

Recommandation n° 1 : **conforter le rôle de l'Agence nationale de sécurité des systèmes d'information** (ANSSI) auprès des pouvoirs publics.

Recommandation n° 2 : assurer un **meilleur contrôle du Sénat sur l'acquisition par les sénateurs de leurs équipements informatiques**, afin de faciliter le travail de maintenance des équipes techniques.

Recommandation n° 3 : **reporter l'entrée en vigueur de la disposition organique permettant la transmission par voie électronique des parrainages** pour l'élection présidentielle.

Recommandation n° 4 : **moderniser le système informatique robuste de remontée de résultats** des élections dans les préfectures.

Mesdames, Messieurs,

Le constat d'une croissance des attaques et d'une diversification de la menace d'origine cyber est partagé par l'ensemble des observateurs et des acteurs de la sécurité informatique. Les pouvoirs publics, au cœur des enjeux stratégiques et décisionnels des démocraties, constituent une cible privilégiée des attaquants de toutes origines, étatiques ou non.

Dans ce contexte, il a semblé à votre rapporteur spécial utile d'étudier les conditions dans lesquelles les pouvoirs publics mobilisent leurs moyens matériels et humains afin d'éviter une attaque, mais également d'en minimiser les conséquences sur le fonctionnement des institutions de la République.

Les pouvoirs publics, au même titre que les entreprises ou les particuliers, sont la cible de cyberattaques aussi bien de masse que ciblées. La revue stratégique de cyberdéfense[1], confiée par le Premier ministre Édouard Philippe à Louis Gautier, secrétaire général de la défense et de la sécurité nationale, a mis en évidence quatre grandes catégories de menaces, qui correspondent aux objectifs poursuivis par les attaquants :

- **l'espionnage informatique**. Ce type d'attaque vise à dérober des données et peut être réalisé par les services de renseignement des États qui en ont la capacité, mais pas uniquement. Ces attaques constituent, en nombre, la plus grande partie des offensives majeures ayant visé la France ces dernières années ;

- **la cybercriminalité**. Le développement et la professionnalisation des réseaux cybercriminels dans les années 2000 a conduit à la multiplication des opérations criminelles de vol direct et de rançons. On observe un rapprochement des groupes cybercriminels et des services de renseignements de certains États – de nouvelles officines ;

- **la déstabilisation**. Le développement des réseaux sociaux a permis l'émergence de ce type d'attaques informatiques visant en particulier à propager des faits non vérifiés voire erronés, dits *fake news* ou infox, dont la diffusion est particulièrement rapide ;

- **le sabotage informatique**. Ces attaques visent à paralyser l'activité d'une entité en bloquant ses réseaux voire en détruisant ses équipements les plus critiques.

---

[1] *Revue stratégique de cyberdéfense, Secrétariat général de la défense nationale (SGDN), février 2018.*

Le rapport d'activité de l'Agence nationale de sécurité des systèmes d'information (ANSSI) pour l'année 2018 pointait quant à lui **cinq grandes tendances** observées par sa sous-direction des opérations en France et en Europe : l'exfiltration de données stratégiques ; les attaques indirectes qui exploitent la relation de confiance qui unit la cible finale à la cible intermédiaire ; les opérations de déstabilisation ou d'influence, particulièrement nombreuses ; la génération de cryptomonnaies ; la fraude en ligne, qui se tourne progressivement vers des cibles moins exposées mais plus vulnérables car moins préparées que les grands opérateurs.

Cette catégorisation des cybermenaces, si elle peut paraître théorique, recouvre une réalité que confirment les exemples plus ou moins récents d'attaques d'ampleur qui ont affecté le fonctionnement d'institutions publiques ou d'opérateurs d'importance vitale (OIV) en France ou à l'étranger ces dernières années.

Ainsi, l'Estonie a subi en 2007 une attaque majeure visant les sites internet du Gouvernement, des médias ou encore des grandes banques. Ceux-ci ont été saturés au point d'être paralysés pour des périodes allant de plusieurs heures à quelques jours. Plus récemment, en mai 2015, le Bundestag, chambre basse du Parlement allemand, était victime d'une cyberattaque qui a nécessité plusieurs semaines de travail pour que les conséquences soient surmontées et que la fin de l'attaque soit officiellement annoncée. À nouveau en janvier 2019, l'Allemagne était la cible d'une cyberattaque avec la publication en ligne de nombreuses données confidentielles concernant des responsables politiques allemands. En France, c'est la chaîne TV5 Monde qui a été la cible d'une attaque dont les conséquences ont été durables *(cf. infra)*.

Les échéances électorales sont des moments cruciaux de la vie politique et institutionnelle des grandes démocraties et deviennent à ce titre des occasions propices aux attaques informatiques. C'est ce qu'a démontré la dernière élection présidentielle américaine de 2016 et l'exfiltration de données dont a été victime le parti démocrate aux États-Unis.

L'objet de ce rapport est donc de procéder à un état des lieux non exhaustif de la préparation des pouvoirs publics pour répondre à l'ensemble des cybermenaces qui les visent. Votre rapporteur spécial a ainsi souhaité vérifier que **l'importance des risques pesant sur le fonctionnement des institutions a été prise en compte par les responsables des pouvoirs publics** et qu'en ce sens, même si en la matière il est impossible de se prémunir de toutes les attaques éventuelles, **les dotations accordées à l'Élysée, au Conseil constitutionnel et aux assemblées parlementaires ont été bien employées en mettant en œuvre les actions préventives nécessaires et en mobilisant les compétences appropriées**.

Il s'agit également d'un enjeu de souveraineté auquel le Sénat s'intéresse au travers de sa commission d'enquête sur la souveraineté numérique rapportée par notre collègue Gérard Longuet.

I. LA SÉCURITÉ INFORMATIQUE DES POUVOIRS PUBLICS, ENJEU STRATÉGIQUE ET FINANCIER

A. LES CONSÉQUENCES POTENTIELLEMENT LOURDES DES ATTAQUES IMPLIQUENT UNE PRÉPARATION EN AMONT : L'EXEMPLE DE TV5 MONDE

L'importance de dresser un état des lieux de la préparation des pouvoirs publics aux risques d'attaques informatiques tient en premier lieu à la **lourdeur des conséquences que pourrait avoir une opération d'intrusion ou de déstabilisation visant une institution publique**.

En France, le précédent de l'attaque subie par la chaîne de télévision TV5 Monde constitue à la fois un exemple des importants coûts entraînés par un événement de ce type et une référence quant aux enseignements à tirer en termes de préparation pour les services informatiques des structures concernées.

Le 8 avril 2015, TV5 Monde subissait une attaque dont l'objectif était non seulement de détruire les infrastructures informatiques de l'entreprise, mais également de l'empêcher de produire et de diffuser. Concrètement, le site Internet de la chaîne et ses comptes sur les réseaux sociaux étaient utilisés par les attaquants pour diffuser de la propagande djihadiste. La chaîne ne pouvait plus utiliser son système de production d'images et la diffusion a donc été interrompue, conduisant à l'affichage d'un écran noir.

Afin d'apporter une réponse immédiate pour stopper la cyberattaque dont TV5 Monde était la cible, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a apporté son concours aux équipes techniques de la chaîne. Une importante campagne de reconstruction, de consolidation et de durcissement des infrastructures informatiques a ensuite débuté à compter de l'été 2015, dont **les conséquences financières continuent de peser sur le budget de fonctionnement de l'entreprise**.

Les éléments qui permettent de mesurer le poids de cette cyberattaque dans les dépenses de TV5 Monde sont à apprécier en termes de surcoûts. Ceux-ci ont été évalués de la sorte :

- en 2015, des moyens financiers à hauteur de 4,4 millions d'euros ont été consacrés pour reconstruire le dispositif informatique, lancer le système de supervision et absorber des pertes de recettes. Celles-ci ont été évaluées à 200 000 euros ;

- en 2016, les coûts additionnels ont été évalués à 3,1 millions d'euros ;

- de 2017 à 2019, ces coûts additionnels se sont stabilisés à environ 2,6 millions d'euros par an.

Au regard de l'ensemble du budget de TV5 Monde, ces dépenses supplémentaires impliquées par les suites de la cyberattaque ne sont nullement négligeables : elles représentent 2,4 % des dépenses totales de la chaîne. Celles-ci s'élèvent en 2019 à environ 111 millions d'euros.

L'attaque concernant TV5 Monde ne concernait certes pas un des pouvoirs publics au sens de la mission budgétaire dont votre rapporteur spécial a la charge. Néanmoins, il estime que **ce précédent est particulièrement représentatif des surcoûts budgétaires que peut provoquer une insuffisante prise en compte des impératifs liés à la sécurité informatique**, sans parler des dysfonctionnements immédiats. Cet exemple justifie l'intérêt porté aux conditions dans lesquelles les pouvoirs publics étudiés s'organisent pour faire face aux menaces évoquées ci-dessus. Au-delà des surcoûts potentiels liés à la gestion d'une attaque, il s'avère néanmoins difficile de déterminer le coût de la sécurité informatique des pouvoirs publics.

B. LA DIFFICULTÉ DE DÉTERMINER LE COÛT DE LA SÉCURITÉ INFORMATIQUE DES POUVOIRS PUBLICS

L'analyse budgétaire des coûts liés à la sécurité informatique des pouvoirs publics se heurte à des obstacles qui rendent difficile la détermination du montant exact consacré par les institutions à la protection de leur réseau informatique et donc à la préservation de leur fonctionnement.

En effet, au sein du budget alloué chaque année à la direction des systèmes d'information de chacune des structures concernées, il n'est pas possible d'isoler un ensemble de dépenses spécifiquement consacrées à la sécurité informatique. Tous les responsables techniques ou responsables de la sécurité des systèmes d'information (RSSI) des institutions rencontrés par votre rapporteur spécial ont pu préciser que chaque projet informatique, qu'il concerne le développement d'une application, l'évolution d'une infrastructure ou le remplacement d'équipements, comporte une dimension de sécurité informatique, qui n'est pas toujours quantifiable.

Malgré tout, à titre d'exemple, la direction des systèmes d'information du Sénat estime que 25 % environ de son budget total est consacré aux dépenses « infrastructures et sécurité »[1]. Les dépenses de sécurité à proprement parler représentaient sur la période 2016-2018 entre 150 000 et 300 000 euros, dont la moitié consacrée à la maintenance. Les fortes variations annuelles de budget s'expliquent par des acquisitions d'équipements. Enfin, certaines dépenses rattachées à la sécurité informatique portent sur des équipements ayant plusieurs fonctions, non exclusivement consacrés aux enjeux de sécurité.

---

[1] *Le budget total de la direction des systèmes d'information du Sénat a varié sur la période 2016-2018 entre 3,5 et 4,2 millions d'euros.*

C'est pour cette raison que le travail conduit par votre rapporteur spécial a davantage consisté à échanger sur les problématiques liées à la sécurité informatique et sur leur prise en compte par les pouvoirs publics contrôlés qu'à une analyse quantitative des crédits consacrés à la cybersécurité. La seule évaluation généralement donnée est que 10 % du budget informatique doivent être consacrés aux investissements en matière de sécurité.

De plus, la détermination du coût de la sécurité informatique des pouvoirs publics est également rendue difficile en raison de l'appui extérieur que représente la collaboration avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont chacun des pouvoirs publics bénéficie. Son coût n'apparaît pas dans les dépenses de ces institutions, alors même qu'il est indispensable et au centre du dispositif de cyberdéfense national.

Présentation de l'Agence nationale de la sécurité des systèmes d'information

Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

En collaboration avec les administrations compétentes, l'ANSSI instruit et prépare les décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État. L'agence accompagne ainsi les cabinets du président de la République, du Premier ministre et des membres du Gouvernement dans la sécurisation de leurs systèmes d'information. (…)

En cas d'attaque avérée ou soupçonnée, le Centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la défense des services de l'État et des opérateurs privés les plus sensibles.

Pour mener à bien sa mission, le COSSI met en œuvre des dispositifs de veille, de détection, de collecte, d'analyse et de réponse aux incidents de sécurité.

Source : site internet de l'ANSSI

Votre rapporteur spécial a pu constater en échangeant avec les responsables administratifs et techniques des différents pouvoirs publics qui font l'objet du présent contrôle que **le rôle de l'ANSSI est particulièrement décisif et incontournable**, tant en amont pour préparer les conditions d'une sécurité informatique satisfaisante des institutions françaises qu'en cas d'attaque avérée, où ses équipes peuvent jouer un rôle crucial dans le traitement des conséquences d'une attaque. Son expertise est reconnue, sa fiabilité aussi.

Recommandation n° 1 : Conforter le rôle de l'Agence nationale de sécurité des systèmes d'information (ANSSI) auprès des pouvoirs publics.

II. LA PRÉPARATION DES POUVOIRS PUBLICS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE DÉCOULE DE LA SPÉCIFICITÉ DU RÔLE DE CHACUNE DES INSTITUTIONS

A. LES ASSEMBLÉES PARLEMENTAIRES SONT LA CIBLE PRIVILÉGIÉE DES ATTAQUES VISANT À LA DIFFUSION D'UN MESSAGE POLITIQUE OU PARTISAN

Les assemblées parlementaires, institutions symboliques des démocraties en ce qu'elles sont le lieu dans lequel sont débattues les propositions et projets de loi sur tous les sujets, souvent en prise avec l'actualité, constituent une cible privilégiée des attaques visant principalement à déstabiliser le fonctionnement des institutions ou à porter un message à la connaissance de tous.

En effet, l'ensemble du travail des assemblées étant généralement soumis à la publicité, **peu de renseignements stratégiques en font la cible de tentatives d'intrusion pour extraire des données sensibles. En revanche, en tant que lieu de débat, « vitrine » de la démocratie, elles doivent subir des attaques répétées visant à faire passer des messages, notamment pour contester l'adoption imminente d'une loi**.

1. Le Sénat

Le Sénat est tout d'abord exposé, comme l'ensemble des institutions publiques et des entreprises, à ce qu'il convient de qualifier de **« tout-venant » malveillant**. Il s'agit principalement :

- des spams1, phishings2, sites Internet compromis ou fichiers téléchargés infectés. Les dispositifs de sécurité informatique du Sénat ont ainsi intercepté au total environ 31 000 contenus à risque en 2018 ;

- des scans automatiques incessants des services offerts par le Sénat sur internet, notamment le site Internet, afin de détecter des failles ou d'en détourner l'usage ;

- des attaques qui concernent les services dits « ressources et moyens », principalement des faux ordres de virement.

---

[1] *Courriels indésirables.*

[2] *Ou hameçonnages.*

De plus, des **menaces spécifiques découlent de la nature d'assemblée parlementaire** du Sénat :

- des protestations en ligne ou des pétitions qui concernent l'activité législative et conduisent à un engorgement de la messagerie des parlementaires ;

- des attaques en déni de service (DDOS)1 des réseaux ou des sites web du Sénat ;

- des tentatives de « défacement », c'est-à-dire la modification des pages des sites Internet ;

- des phishings ciblés, appelés spear phishings.

Afin de maintenir une connaissance actualisée des menaces existantes, l'équipe chargée de la sécurité informatique du Sénat procède à **une veille permanente**. À cette fin, un marché public de veille technique spécialisée permet notamment de bénéficier d'une information concernant des vulnérabilités logicielles ou de surveiller l'apparition de noms de domaine contenant « Sénat ». L'ANSSI constitue également une source d'information à travers le Centre gouvernemental de veille, d'alerte, et de réponse aux attaques informatiques (CERT-FR)[2].

Par ailleurs, la diffusion des bonnes pratiques et des recommandations concernant la sécurité informatique est assurée par le relais que constitue le responsable de la sécurité des systèmes d'information au sein de l'institution. Celui-ci participe aux réunions mensuelles organisées par l'ANSSI qui rassemblent l'ensemble des fonctionnaires ou responsables des systèmes d'informations (FSSI et RSSI) des ministères, assemblées, présidence de la République et autres entités ministérielles.

Parmi les principales attaques dont le Sénat a été la cible, l'attaque par déni de service distribué (DDOS) du 25 décembre 2011 a été la plus visible, celle-ci ayant rendu le site internet du Sénat inaccessible pendant plusieurs heures (*cf. infra*).

[1] *Une attaque DDoS (ou attaque par déni de service) vise à rendre un serveur ou une infrastructure indisponible.*
[2] *https://www.cert.ssi.gouv.fr/*

La cyberdéfense : un enjeu mondial, une priorité nationale[1] (extraits)

Peu avant l'adoption par le Parlement français, le 31 janvier dernier, de la loi visant à réprimer la contestation des génocides reconnus par la loi, dont le génocide arménien, de nombreux sites institutionnels, à l'image du site Internet de l'Assemblée nationale ou les sites de plusieurs députés, ont été rendus inaccessibles à la suite d'attaques informatiques. Votre rapporteur a pensé utile de décrire l'attaque subie à cette occasion par la Haute assemblée.

Le dimanche 25 décembre, le service informatique du Sénat a, en effet, été alerté par plusieurs fonctionnaires qui s'étaient rendus compte que le site Internet de la Haute assemblée n'était plus accessible. Dès le lendemain matin, les informaticiens ont constaté que le Sénat avait été victime de ce que les spécialistes appellent une « attaque par déni de service ». Par des moyens techniques, et notamment grâce à une copie du site Internet du Sénat sur un autre serveur, d'une capacité de résistance supérieure, il a été possible de rendre le site Internet de la Haute assemblée à nouveau accessible dès le lundi 26 décembre après-midi.

À l'image du cas de l'Estonie en 2007, ces « attaques par déni de service » (Denial of service - DOS) visent à saturer un ordinateur ou un système en réseau sur internet en dirigeant vers lui un volume considérable de requêtes. On parle également de déni de service distribué (Distributed denial of service - DDOS) pour des attaques fonctionnant sur le même principe, mais dont l'effet est démultiplié par l'utilisation d'ordinateurs compromis et détournés à l'insu de leurs propriétaires. La masse de requêtes qui parvient simultanément sur un même système dépassant ses capacités, celui-ci n'est plus en mesure de fonctionner normalement. La paralysie d'un système d'information par ce type d'attaques est relativement facile à obtenir lorsqu'il s'agit d'un service accessible au public sur le réseau internet, à l'image du site Internet du Sénat.

Dans le cas du Sénat, l'attaque informatique, assez rudimentaire, et ayant mobilisé un nombre relativement faible d'ordinateurs, a eu pour effet de saturer, par un nombre très élevé de requêtes, l'accès au site Internet de la Haute assemblée pendant plusieurs heures. (…) La saturation a brutalement commencé peu après 6 heures du matin le dimanche 25 décembre et s'est achevée le lundi 26 décembre après-midi.

Même si ces attaques informatiques ont été ouvertement revendiquées par des groupes de « hackers » patriotiques turcs, à l'image des groupes « GrayHatz » et « Millikuvvetler », et par d'autres « hackers » indépendants, il est très difficile d'identifier précisément l'auteur de ces attaques. En effet, ces groupes ont recours à des « botnets », c'est-à-dire à des réseaux de machines compromises et utilisées à l'insu de leurs propriétaires. Dans le cas du Sénat, la provenance des attaques informatiques ayant abouti à la saturation du site Internet était très diversifiée puisqu'elles provenaient d'ordinateurs situés partout dans le monde.

Si, depuis cette affaire, des mesures ont été prises au Sénat afin de renforcer la protection des systèmes, il n'en demeure pas moins que les attaques par déni de service visant un site Internet ouvert au public sont très difficiles à éviter et qu'il n'existe pas de parade absolue.

D'autres tentatives d'attaques par déni de service distribué ont été relevées depuis cette date, entraînant des perturbations allant de quelques minutes à deux heures. Néanmoins, ayant tiré les enseignements de l'attaque

[1] *Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.*

de 2011, le Sénat n'a pas eu à subir d'importantes conséquences de ces tentatives de déstabilisation.

En effet, les différents événements auxquels la direction des systèmes d'information du Sénat a dû faire face ces dernières années l'ont conduit à adapter ses infrastructures ou à faire évoluer les solutions extérieures auxquelles elle a recours. L'offre de protection contre les attaques par déni de service a ainsi été renforcée auprès des fournisseurs d'accès à internet du Sénat. Le webmail, qui constituait une porte d'entrée conséquente pour de nombreuses attaques de phishing ou de spam, a été intégré au e-bureau, le portail d'accès à distance aux applications du Sénat, (« derrière le VPN[1] ») et n'est désormais accessible qu'après une authentification renforcée.

De plus, la politique de sensibilisation des utilisateurs constitue un outil de lutte contre ce type d'attaques. Des rappels de la charte informatique du Sénat, des incitations à la modification régulière des mots de passe ou encore des campagnes d'information en cas d'attaques répétées constituent des moyens de prévention utiles.

Néanmoins, les sénateurs constituent un public spécifique au sein de la catégorie des utilisateurs du Sénat. Ils sont en effet déjà sollicités par une masse d'information et de documents importante, qui rend les campagnes de prévention aux risques d'attaques informatiques difficiles. Par ailleurs, votre rapporteur spécial observe que la possibilité laissée aux sénateurs de s'équiper librement, en choisissant pour eux-mêmes et pour leurs collaborateurs les modèles d'ordinateurs et de périphériques qu'ils souhaitent, rend la tâche des équipes du Sénat chargées de la sécurité informatique beaucoup plus complexe. Il souligne qu'un tel fonctionnement est assez peu fréquent et que la plupart des collectivités locales ont fait le choix de garder la maîtrise des équipements mis à la disposition de leurs élus. Aussi, il recommande une évolution de la pratique sénatoriale sur ce point, tout en mesurant les conséquences d'une prise en charge par l'administration sénatoriale de tous les équipements des sénateurs et de leurs collaborateurs eu égard aux coûts supplémentaires et difficultés d'organisation liées aux besoins de recrutement.

Recommandation n° 2 : Assurer un meilleur contrôle du Sénat sur l'acquisition par les sénateurs de leurs équipements informatiques, afin de faciliter le travail de maintenance des équipes techniques.

[1] *Le VPN (virtual private network) est un réseau privé virtuel qui permet de créer un lien direct entre des ordinateurs distants, en isolant leurs échanges du reste du trafic se déroulant sur les réseaux de télécommunication publics.*

Pour compléter le dispositif destiné à assurer la sécurité informatique du Sénat, le Bureau du Sénat a, au cours de sa réunion du 22 mai 2019, approuvé le principe d'une **convention avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour mettre en œuvre un système de détection d'intrusions dans le système d'information du Sénat**.

Les parlements étrangers face à la cybermenace

Dans le cadre d'une consultation des parlements étrangers effectuée au sein du Centre Européen de Recherche et de Documentation Parlementaires (CERDP), votre rapporteur spécial a pu interroger différents responsables informatiques de parlements sur le thème de la sécurité informatique.

Il ressort de cette consultation que l'ensemble des parlements ayant répondu à l'enquête sont confrontés à des menaces similaires à celles qui visent l'Assemblée nationale et le Sénat français, et que les réponses apportées par les pays consultés sont du même ordre.

On retrouve parmi les menaces dont on fait l'objet les parlements étrangers principalement les attaques en déni de service et les tentatives de phishing ou d'intrusion. Ce fut le cas notamment :

- *en 2007, en Estonie* : attaque majeure visant les sites internet du Gouvernement, des médias ou encore des grandes banques. Ceux-ci ont été saturés au point d'être paralysés pour des périodes allant de plusieurs heures à quelques jours ;

- *en 2015 au Bundestag* : cyberattaque qui a nécessité plusieurs semaines de travail pour que les conséquences soient surmontées et que la fin de l'attaque soit officiellement annoncée ;

- *en 2015 au Parlement Canadien* : le groupe de hackers Anonymous a revendiqué une attaque en déni de service contre de nombreux sites internet des départements fédéraux, dont ceux du Parlement. Ces sites ont été inaccessibles au public pendant plus de trois heures ;

- *en 2017 au Parlement britannique* : environ 90 messageries électroniques appartenant à des parlementaires britanniques ont été piratées, et la totalité des comptes des 9 000 adresses des parlementaires ont été visés par une attaque informatique, qui a duré près de douze heures.

L'ensemble des pays consultés ont fait part de l'existence d'un organisme dont les compétences sont proches de celles de l'ANSSI.

En revanche, certains des parlements étrangers consultés n'ont pas mis en place, contrairement à l'Assemblée nationale et au Sénat, de poste équivalent à celui de responsable de la sécurité des systèmes d'information.

Enfin, en février 2019, le parlement australien a été la cible d'une attaque qui a conduit au piratage de son système informatique, ainsi que de plusieurs partis politiques. Les autorités australiennes ont alors imputé cette opération à une entité soutenue par une puissance étrangère.

2. Public Sénat

Le précédent de l'attaque ayant visé TV5 Monde a conduit votre rapporteur spécial à étudier dans le cadre de son contrôle les conditions dans lesquelles Public Sénat se prépare à l'éventualité d'une opération visant à déstabiliser la chaîne. Plusieurs possibilités d'attaques sont ainsi envisagées :

- une chaîne de télévision, au-delà des menaces génériques, est particulièrement exposée au risque d'une attaque visant la **confidentialité des données dont elle dispose**, en particulier à travers la divulgation des contacts des journalistes, alors même que ceux-ci sont protégés par le secret des sources ;

- l'intégrité de l'information délivrée par la chaîne peut être visée par une attaque qui consisterait à la **publication d'une « infox »**, à un défacement, c'est-à-dire à un changement de page d'accueil, ou encore à un détournement de compte Facebook ou Twitter. Il s'agit alors pour l'attaquant d'utiliser les infrastructures de la chaîne pour faire passer un message. Le détournement des comptes de réseaux sociaux présente une technicité plus simple et une exposition plus importante que la substitution de contenu sur la diffusion audiovisuelle. Pour cette raison, elle constitue la menace classée en tête ;

- la disponibilité du site internet peut être attaquée, par déni de service.

Une réflexion globale existe au sein du groupe BCG (Broadcast Cybersecurity Group). Celui-ci a été créé au printemps 2015 à la suite de la proposition de la direction des systèmes d'information de TV5 Monde de se doter d'un groupe de travail et d'échanges sur la cybersécurité qui rassemblerait des chaînes partenaires. Public Sénat a participé aux premières réunions, mais a observé que les problématiques et les surfaces de risques de la chaîne parlementaire s'éloignaient de celles des autres chaînes participantes et a donc poursuivi sa propre réflexion en dehors de ce cadre.

Public Sénat a choisi de **recourir à l'accompagnement d'un cabinet privé de conseil pour l'identification de ses objectifs de sécurité et la détermination de stratégie**. Les analyses de risque qui ont été menées dans le cadre du diagnostic de sécurité ont ainsi permis de déterminer les vulnérabilités existantes afin de mettre en place un plan d'action décliné à travers une série de chantiers. Ceux-ci ont d'ores et déjà été, pour certains d'entre eux, mis en œuvre à la suite de ce travail.

Il existe par ailleurs une série de procédures permettant l'arrêt de la diffusion en cas de difficulté ou d'attaque identifiée, avec la présence permanente d'un opérateur derrière les automates qui assurent la diffusion des contenus.

Enfin, votre rapporteur spécial observe que les grands événements tels que l'organisation et la diffusion de la COP21 permettent de travailler sur des solutions sécurisées de retransmission, dont les enseignements sont ensuite repris pour les activités du quotidien.

3. L'Assemblée nationale

De la même façon que pour le Sénat, la détermination de la part des dépenses de l'Assemblée nationale consacrée à la sécurité informatique est difficile, pour les raisons évoquées ci-dessus. Les dépenses d'investissement de l'Assemblée nationale gérées par le service des systèmes d'information s'élevaient, selon le rapport du Collège des Questeurs à la commission spéciale chargée de vérifier et d'apurer les comptes, à 5,64 millions d'euros en 2018.

Évolution des dépenses d'investissement du service des systèmes d'information de l'Assemblée nationale de 2014 à 2018

(en millions d'euros et en pourcentage)

	2014	2015	2016	2017	2018
Logiciels (M€)	2,43	2,69	2,15	2,46	1,90
Matériel (M€)	1,44	1,68	1,67	3,06	3,74
Total (M€)	**3,87**	**4,37**	**3,81**	**5,54**	**5,64**
% dépenses d'investissement	27,43	25,39	21,14	17,22	28,33

Source : Rapport du Collège des Questeurs à la commission spéciale chargée de vérifier et d'apurer les comptes

L'Assemblée nationale a également conclu un partenariat avec l'ANSSI pour mettre en œuvre des mesures de protection, dont la pose de sondes[1].

B. L'ÉLYSÉE, CIBLE STRATÉGIQUE DE PREMIER PLAN

D'un point de vue stratégique, la présidence de la République constitue **une cible de premier plan en termes de renseignements**. L'intrusion dans les réseaux informatiques est donc l'une des modalités susceptibles de permettre la collecte de données stratégiques, au même titre que d'autres formes d'attaques telles que la surveillance par les ondes électromagnétiques ou les tentatives d'écoutes des moyens sécurisés de communication du Président de la République.

[1] *Rapport d'information n° 1141 (XVe lég.) déposé par la commission de la défense et des forces armées sur la cyberdéfense, p. 139.*

L'une des difficultés rencontrées à la présidence de la République, que l'on peut retrouver également dans d'autres pouvoirs publics, tient au caractère historique des locaux dans lesquels elle est installée. En effet, l'occupation de bâtiments historiques tels que le Palais de l'Élysée rend la gestion des réseaux et des installations d'infrastructures particulièrement difficile en raison de la configuration datée, et donc peu adaptée, des lieux.

L'identification des menaces qui visent l'Élysée correspond aux différentes catégories d'attaques présentées précédemment. Peuvent donc en être à l'origine :

- des États étrangers, que ceux-ci soient considérés comme des alliés de la France ou non ;

- des activistes qui souhaitent faire passer un message ou rendre difficile le fonctionnement de l'institution ;

- des officines criminelles, qui monétisent leurs actions. Cette catégorie se développe depuis plusieurs années ;

- des hackers en recherche de notoriété.

L'organisation du réseau informatique de l'Élysée **prend en compte les impératifs et les recommandations de bonnes pratiques puisque trois types de réseaux cohabitent** : un réseau libre, ouvert pour les événements et les visiteurs, un réseau principal « Présidence de la République » qui est ouvert à l'internet mais très fortement filtré, et un réseau classifié défense, qui est disjoint.

Les attaques standard à l'égard de la Présidence de la République sont quasi quotidiennes, tandis que des offensives plus conséquentes se présentent deux à trois fois par semaine. Les **attaques plus sophistiquées dépendent quant à elle de l'actualité**, par exemple de négociations internationales en cours ou de la survenance de sommets entre chefs d'États tels que le G7.

L'équipe de l'Élysée dédiée à la sécurité informatique est relativement réduite, même si elle a été récemment renforcée. Elle se compose d'un responsable de la sécurité des systèmes d'information, rattaché au directeur général des services, auquel a été associé un responsable adjoint. Deux ingénieurs se consacrent par ailleurs à la sécurité informatique et sont quant à eux rattachés au service informatique, qui compte un total de 27 collaborateurs. Ces personnels dédiés aux questions de cybersécurité sont dans l'ensemble très bien identifiés par les agents qui travaillent à l'Élysée compte tenu de la taille relativement limitée de l'administration de la présidence de la République, ce qui permet aux utilisateurs de contacter aisément les personnes compétentes.

L'Élysée bénéficie comme les autres pouvoirs publics d'une collaboration étroite avec les services de l'ANSSI. Ce travail en commun permet pour les personnels techniques de la présidence de bénéficier d'avis

sur les analyses de risques, dans le cadre d'audits en particulier. Il existe par ailleurs un marché interministériel de prestation de sécurité des systèmes d'information auquel l'Élysée se rattache en tant que de besoin.

Un programme de sensibilisation des personnels, qu'ils soient techniciens ou administrateurs du service informatique de l'Élysée, comporte un volet formation qui conduit ces personnels à suivre des sessions délivrées par l'ANSSI. Le reste des agents de l'Élysée fait l'objet d'actions de sensibilisation plus ou moins ciblées, qui peuvent prendre la forme de réunions de cabinet. Une adresse électronique a notamment été mise en place afin de faciliter les signalements en cas de suspicion d'attaque. Le nombre important de signalements reçus par le service informatique à travers ces dispositifs montre que la sensibilisation du personnel de la présidence de la République est réelle.

C. LE RÔLE DU CONSEIL CONSTITUTIONNEL EN MATIÈRE ÉLECTORALE AU CŒUR DES PRÉOCCUPATIONS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

Le juge constitutionnel constitue, en matière de sécurité informatique, davantage une cible pour des opérations de déstabilisation ou d'atteinte à l'image que pour d'éventuelles attaques visant au sabotage de l'institution à proprement parler. Certains esprits malveillants pourraient également être intéressés par les documents préparatoires confidentiels des délibérés du Conseil.

Concernant l'atteinte à l'image, la préservation de l'intégrité du site internet du Conseil constitutionnel constitue un enjeu central dans la mesure où y sont publiées les décisions prises par l'institution. Une substitution de contenu pourrait en ce sens avoir des conséquences dommageables pour lui. Pour cette raison, un travail de refonte du site a été effectué au cours des deux dernières années et a permis de mettre en place des mécanismes de contrôle visant à anticiper les risques liés à la diffusion de fausses pages internet.

Comme les autres pouvoirs publics, le Conseil est la cible de tentatives de hameçonnage par messagerie, dont le nombre varie en fonction de l'actualité des textes dont il a à connaître. À titre d'illustration, depuis le lancement de la procédure du référendum d'initiative partagée sur la privation d'ADP, une multiplication par 8 du nombre de ces tentatives a été observée. Néanmoins, les pare-feu en place sur le réseau permettent de filtrer ces attaques.

Le service informatique du Conseil constitutionnel est constitué de 8 agents, sur les 70 que l'administration compte au total. Cette équipe a été renforcée ces dernières années pour tenir compte du caractère prioritaire des questions liées en particulier à la sécurité informatique. Le secrétaire général du Conseil, Jean Maïa, a ainsi évoqué lors de l'entretien avec votre

rapporteur spécial la « démarche quasi-paranoïaque » de l'institution à cet égard, liée à la culture du secret des délibérations, qui le **conduit à privilégier la sécurité des dispositifs en place, y compris sur le confort des utilisateurs**. Le montant des investissements informatiques à réaliser dans les deux années à venir est estimé par le secrétariat général du Conseil à 700 000 euros.

Parmi les différentes missions et activités du Conseil constitutionnel, votre rapporteur spécial a choisi **de s'intéresser plus particulièrement à son rôle en matière électorale**, qui, au vu des exemples étrangers notamment, pourrait être prioritairement la cible d'attaques informatiques visant en particulier à discréditer la remontée des résultats ou la collecte des parrainages de l'élection présidentielle.

Aux termes des articles 58 à 60 de la Constitution de 1958, le Conseil constitutionnel veille à la régularité de l'élection du Président de la République et des opérations de référendum, dont il proclame les résultats. Il contrôle également la régularité des résultats des élections des députés et des sénateurs, en cas de contestation.

C'est plus précisément le **rôle central qu'il détient pour l'élection présidentielle qui pourrait faire du Conseil constitutionnel une cible stratégique et qui justifie, en ce sens, une attention renforcée à la sécurité informatique**. En effet, pour cette élection, le Conseil intervient à deux titres : d'une part dans la collecte des parrainages et d'autre part pour le contrôle de la remontée des résultats et la proclamation du résultat du scrutin.

Le Conseil constitutionnel, à cet égard, ne prépare pas les conditions de sa sécurité informatique sans collaboration avec des intervenants extérieurs. Comme les autres pouvoirs publics, il bénéficie là encore d'une relation étroite de collaboration avec l'ANSSI. Par ailleurs, le ministère de l'intérieur, et plus particulièrement le Bureau des élections et études politiques au sein de la Direction générale de la modernisation et de l'administration territoriale (DMAT), est un collaborateur du Conseil constitutionnel puisqu'il élabore les systèmes d'information permettant la remontée des résultats. Le dispositif actuellement en place a été homologué par l'ANSSI.

En revanche, tant le Secrétaire général du Conseil constitutionnel que les représentants du ministère de l'intérieur rencontrés par votre rapporteur spécial ont souligné **l'absence, à ce jour, de garanties concernant la mise en œuvre de la dématérialisation de la collecte des parrainages pour l'élection présidentielle**. La possibilité de collecter les parrainages des candidats à l'élection présidentielle par voie électronique a été introduite par l'article 2 de la loi organique n° 2016-506 du 25 avril 2016 de modernisation des règles applicables à l'élection présidentielle qui dispose que : « *La transmission électronique prévue au quatrième alinéa du I de l'article 3 de la loi n° 62-1292 du 6 novembre 1962 relative à l'élection du Président de la République*

au suffrage universel, dans sa rédaction résultant du I du présent article, est applicable à compter d'une date fixée par décret et au plus tard le 1er janvier 2020. » **Il n'existe pourtant pas, à ce jour, de dispositif technique permettant d'apporter les conditions de sécurité et d'authentification** similaires à la procédure de transmission par courrier, mise au point en lien avec l'Imprimerie nationale.

La dématérialisation de la collecte des parrainages **impliquerait la mise en place d'une identité numérique de niveau élevé**. Un tel dispositif, s'il était déployé auprès des maires, présenterait de nombreux avantages dans la gestion quotidienne des communes. Néanmoins, votre rapporteur spécial s'interroge sur la faisabilité d'une telle opération dans un délai inférieur à deux ans. En effet, les moyens à mobiliser pour mettre en place une solution fiable et présentant toutes les garanties de sécurité semblent importants au regard du gain attendu, compte tenu du caractère opérationnel du dispositif actuel. Il s'interroge donc sur la nécessité de reporter le délai organique pour ne pas, sur ce point, installer durablement une divergence entre les prescriptions du législateur organique et la pratique institutionnelle.

Recommandation n° 3 : reporter l'entrée en vigueur de la disposition organique permettant la transmission par voie électronique des parrainages pour l'élection présidentielle.

S'agissant de la remontée des résultats des élections, ceux-ci sont d'abord centralisés dans des bureaux dits centralisateurs une fois les urnes dépouillées, avant d'être déposés sur une plateforme sous forme de fichier depuis 2019, saisis en ligne ou envoyés par messagerie à la préfecture. Les résultats sont par la suite agrégés au niveau national et rendus publics lorsqu'ils sont complets. L'application « Élections » qui permet cette remontée des résultats a été homologuée par l'ANSSI. Elle a fait l'objet de correctifs afin de renforcer sa sécurité. Des réseaux dédiés, consacrés uniquement aux procédures électorales, sont utilisés pour le fonctionnement de cette application.

Parallèlement, les procès-verbaux de l'ensemble des bureaux de vote sont acheminés à la préfecture et contrôlés un à un avec les résultats saisis dans l'application, avant le lendemain midi, sous le contrôle d'un magistrat. Après leur vérification, les procès-verbaux validés sont envoyés depuis les préfectures vers le Conseil constitutionnel.

Recommandation n° 4 : moderniser le système informatique robuste de remontée de résultats des élections dans les préfectures.

EXAMEN EN COMMISSION

Réunie le mardi 22 octobre 2019, sous la présidence de M. Vincent Éblé, président, la commission a entendu une communication de M. Jérôme Bascher, rapporteur spécial, sur la sécurité informatique des pouvoirs publics.

M. Vincent Éblé, président. – Nous commençons notre réunion par le rapport de Jérôme Bascher, rapporteur spécial de la mission « Pouvoirs publics ». Il poursuivra par une communication sur son contrôle budgétaire sur la sécurité informatique des pouvoirs publics, objet d'une actualité tourmentée ces dernières années.

M. Jérôme Bascher, rapporteur spécial de la mission « Pouvoirs publics ». – Je ferai d'une pierre deux coups en présentant à la fois mon rapport sur les crédits de la mission « Pouvoirs publics » et ma mission de contrôle sur la sécurité informatique des institutions.

La loi organique relative aux lois de finances (LOLF) prévoit qu'une mission spécifique regroupe les crédits alloués sous forme de dotations aux pouvoirs publics, pour lesquels le juge constitutionnel a rappelé le principe d'autonomie financière, qui relève de la séparation des pouvoirs. Les marges de manœuvre du Parlement et du Gouvernement sur la détermination de ces crédits sont donc assez limitées.

Le périmètre de la mission « Pouvoirs publics » inclut la présidence de la République, les deux assemblées – Assemblée nationale et Sénat –, le Conseil constitutionnel, les deux chaînes de télévision LCP-AN et Public-Sénat ainsi que la Cour de justice de la République.

Ce budget a une caractéristique : il est constant. Depuis 2012, il se situe légèrement sous le milliard d'euros pour l'ensemble des institutions de la République. Voilà le coût de la démocratie.

La dotation de la présidence de la République connaît une légère augmentation cette année, de 103 à 105,3 millions d'euros, essentiellement due à une consolidation des crédits de la nouvelle direction de la sécurité de la présidence de la République, puisque la sécurité ne relève plus des crédits du ministère de l'intérieur, mais de ceux de l'Élysée. C'était une demande de la Cour des comptes, qui souhaite disposer d'un budget affichant le coût complet de la présidence de la République. Je reviendrai sur cette notion de coût complet.

Les dotations des assemblées parlementaires sont complètement stables depuis 2012, à 518 millions d'euros pour l'Assemblée nationale et 323 millions d'euros pour le Sénat. Avec l'inflation, cela signifie qu'elles ont perdu sur cette période l'équivalent d'une année de dotation par rapport à 2011. Les assemblées ont réalisé un effort important de maîtrise de leurs

dépenses – avec un bémol : pour compléter leur budget, elles puisent dans leurs réserves, année après année, pour pouvoir fonctionner, investir et faire face aux surcoûts, comme le renouvellement partiel de 2020, qui coûtera au Sénat 5 millions d'euros supplémentaires. Si l'on puise tous les ans entre 30 et 40 millions d'euros dans les réserves, elles s'épuisent. En 2022 à l'Assemblée nationale et en 2023 au Sénat, il y aura la vérité des prix. Les assemblées seront plus qu'à l'os. L'Assemblée nationale et le Sénat avaient anticipé une baisse du nombre de parlementaires, mais puisque celle-ci n'entraînerait pas de baisse des coûts pour permettre d'accroître les moyens d'action du Parlement, le sujet est en suspens.

Soulignons l'augmentation des crédits du Conseil constitutionnel sur un point tout à fait particulier : le référendum d'initiative partagée (RIP), pour lequel une enveloppe supplémentaire de 785 000 euros est consacrée.

La Cour de justice de la République a travaillé en 2019 ; elle travaillera aussi, en principe, en 2020. Tant que la réforme constitutionnelle ne la supprime pas, elle doit être financée.

Certains ont été chagrinés par un élément concernant les investissements de l'Élysée. La présidence de la République a commencé un schéma directeur de réaménagement du palais de l'Élysée et du site de l'Alma. Cette opération est menée par l'Élysée en propre et par l'opérateur du patrimoine et des projets immobiliers de la culture (Oppic) qui assure la maîtrise d'ouvrage pour tous les grands monuments historiques. Le ministère de la culture a inscrit des crédits pour le schéma directeur de l'Élysée. La présidence, de son côté, fait traditionnellement inscrire ses travaux sur les crédits alloués aux résidences présidentielles – dont Rambouillet et Brégançon –, qui représentent 5 millions d'euros chaque année dans le budget du ministère de la culture. L'élément nouveau tient au fait que dans le cas présent les crédits provenant de l'OPPIC sont et seront jusqu'en 2022 uniquement portés sur le schéma directeur. Nous ne sommes donc plus dans le budget consolidé, contrairement à ce qui est pratiqué par les assemblées : à titre d'exemple, l'Assemblée nationale va financer elle-même les travaux de son hémicycle, dont le toit menace de s'effondrer, en puisant dans ses réserves. Concernant ce même schéma directeur, on note de surcroît une inscription au compte d'affectation spéciale (CAS) « Gestion du patrimoine immobilier de l'État », qui concerne l'immobilier vendu par l'État et en finance les travaux. En 2019 et en 2020, 5,5 millions d'euros puis 6 millions d'euros de ce CAS seront mobilisés pour le programme immobilier de la présidence de la République. Celle-ci informe qu'elle vendra un immeuble rue de l'Élysée en 2022 pour 27 millions d'euros et que l'argent des travaux est pris sur cette somme future. La procédure est assez classique, sauf que l'on a omis de nous le préciser l'an dernier, alors que j'avais posé la question lors des auditions. J'ai ainsi découvert que des crédits ont été inscrits sur le CAS en cours d'année 2019. C'est pourquoi il me semblerait opportun que le Gouvernement dépose un amendement de périmètre pour

mieux retracer tous les crédits et les consolider au sein du budget de l'Élysée, comme cela avait été demandé par la Cour des comptes concernant les dépenses du ministère de l'intérieur, ou qu'à tout le moins un réel effort de transparence soit réalisé sur ce sujet. Il y a en effet un problème de cohérence. Dans le cadre de la LOLF, en tant que parlementaires, nous ne pouvons pas déposer cet amendement nous-mêmes.

Le programme immobilier doit être clairement expliqué, tant pour les recettes que pour les dépenses. L'an prochain, si le bureau de la commission des finances en est d'accord, ma mission de contrôle pourrait porter sur les programmes immobiliers des différentes institutions. Il y a là un besoin d'éclaircissements et de transparence.

J'en viens à ma mission de contrôle sur la sécurité informatique des pouvoirs publics. Nos institutions sont la cible régulière de cyberattaques : espionnage informatique ; cybercriminalité – avec des demandes de rançon – ; déstabilisation par de fausses nouvelles propagées parfois par de faux comptes qui laissent penser que nous en sommes les auteurs ; sabotage par déni de service. La menace n'est pas récente : le meilleur exemple est celui de l'attaque d'ampleur qu'avait subi l'Estonie en 2007. En France, en 2015, TV5 Monde a subi une attaque retentissante et a dû faire apparaître un écran noir pour que le message initial de cet instrument d'influence de la France ne soit pas détourné. Le surcoût entraîné par cette attaque a été de 2,4 % de son budget total, qui est estimé à 111 millions d'euros. En effet, ne pas tenir compte à temps de la sécurité informatique entraîne des surcoûts. Tout bon informaticien vous dira qu'il faut consacrer au moins 10 % de son budget informatique à la sécurité, sinon l'on est notoirement sous-protégé.

Tout cela démontre le rôle essentiel de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Toutes les institutions de la mission Pouvoirs publics font appel à sa compétence. C'est l'agence qui nous protège des attaques majeures. J'en appelle au maintien et au renforcement de ses crédits pour que notre sécurité informatique soit au bon niveau.

Je rappelle que le Bundestag a été attaqué en 2015, comme le site internet du Sénat français en 2011.

Public Sénat, de son côté, fait appel à une agence privée, surtout sur des points de droit.

L'Élysée, cible de premier plan, s'appuie sur plusieurs réseaux informatiques : un permanent pour les agents de l'Élysée, un extérieur et un destiné aux grands événements tels que le G7 à Biarritz.

La menace qui pèse sur le Conseil constitutionnel est plutôt liée aux résultats de l'élection présidentielle, qu'il proclame, contrairement aux résultats des autres élections qui relèvent du ministère de l'intérieur. Le Conseil constitutionnel s'appuie sur un réseau dédié du ministère de l'intérieur doté de logiciels qui datent du XX^{e} siècle, alimenté sur des postes dédiés par des agents dédiés, dans les préfectures, qui font remonter les

données au ministère de l'intérieur qui les transmet au Conseil constitutionnel. C'est verrouillé, car ce n'est pas très compatible avec internet. Néanmoins, ce réseau présente des risques de défaillance. Il faut donc investir assez rapidement pour que l'élection présidentielle de 2022 soit sûre. J'appelle le ministère de l'intérieur à investir dans ce domaine.

Une disposition organique prévoit des parrainages par voie électronique pour 2022. C'est pour l'instant hors de portée du ministère de l'intérieur, qui devra vérifier l'identité des signataires. Cette disposition était peut-être prématurée et ne sera pas applicable. Il ne faudrait pas que des candidats fantômes soient parrainés par des parrains et des marraines tout aussi fantômes. Si nous sommes amenés à examiner prochainement un projet de loi organique, il serait bon de retirer cette disposition.

Je vous propose d'adopter les crédits de la mission, moyennant la question de périmètre évoquée sur le budget de la présidence de la République.

M. Roger Karoutchi. – Après les différents rapports de la Cour des comptes, l'Élysée a accepté de se doter d'un budget propre et d'un système comptable incluant tous ses agents dans les effectifs de la présidence de la République. Or on me dit que, depuis l'année dernière, les ministères sont à nouveau sollicités pour envoyer des fonctionnaires supplémentaires à l'Élysée. Est-ce le cas ?

L'Assemblée nationale et le Sénat puisent dans leurs réserves, qui ne sont pas inépuisables. Une éventuelle réduction du nombre de parlementaires remettrait en cause l'équilibre des comptes des assemblées, notamment de leurs caisses de retraite. A-t-on imaginé ce que ces deux institutions pourraient vendre comme biens immobiliers ? Elles n'auraient plus besoin d'autant d'immeubles qu'aujourd'hui.

Mme Nathalie Goulet. – On pourrait calculer le coût des institutions au prorata de la population.

M. Jérôme Bascher, rapporteur spécial. – C'est cinq euros par Français pour le Sénat.

Mme Nathalie Goulet. – Le rapport budgétaire pourrait souligner que la démocratie ne coûte pas si cher.

Se soucier de la sécurité informatique, c'est bien, mais quel est l'état du parc informatique ? Le matériel de base est généralement extrêmement obsolète et ne peut pas supporter l'intégration de logiciels modernes, notamment de sécurité.

Mme Christine Lavarde. – En matière de sécurité informatique des différentes instances publiques, des questions se posent sur le fonctionnement de la messagerie du Sénat. Appuyée sur une solution libre, elle ne bénéficie pas d'un agenda associé. La plupart des sénateurs utilisent donc un agenda partagé avec leurs collaborateurs sur Google. C'est un

premier Gafam (Google, Apple, Facebook, Amazon, Microsoft). Les paramètres du serveur sortant de la messagerie n'étant acceptés que par les systèmes d'exploitation d'Apple, nous utilisons tous un iPhone ou un iPad pour répondre en direct à nos e-mails. C'est un deuxième Gafam. Est-ce la solution la plus appropriée pour sécuriser les échanges électroniques du palais du Luxembourg ?

M. Thierry Carcenac. – Le rapport est très intéressant – je rappelle que je suis rapporteur spécial du CAS « Gestion du patrimoine immobilier de l'État ». Monsieur Bascher, vous envisagez des contrôles. Sachez que la commission spéciale chargée du contrôle des comptes et de l'évaluation interne du Sénat, dont plusieurs d'entre nous sommes membres, publie un rapport annuel et a étudié, notamment dans son dernier rapport, les cycles d'investissement du Sénat. Généralement, les prélèvements sur réserve financent les investissements, dont les cycles sont très lourds. En 2017, le montant s'élevait à 24,4 millions d'euros et en 2018 à 19,6 millions d'euros. Entre les autorisations d'engagement et la réalisation, les écarts sont importants. Je suppose que l'Assemblée nationale a publié le même rapport.

Du côté de l'immobilier de l'État, on a aussi essayé de modifier l'approche. Il n'est plus nécessairement envisagé de céder du patrimoine, mais plutôt de privilégier les revenus fixes.

L'immeuble de la rue de l'Élysée dont il est question ne figurait pas, en 2019, dans la liste des biens susceptibles d'être vendus.

J'ajoute que généralement, le CAS « Gestion du patrimoine immobilier de l'État » est présenté à l'équilibre. Puisqu'il y a moins de cessions, il est en déséquilibre et l'on en consomme des sommes très importantes. On devrait peut-être avoir une autre vision que celle de ce CAS. Chacun des ministères gère son patrimoine à sa façon et la vision globale est limitée.

Mme Sylvie Vermeillet. – Je félicite Jérôme Bascher pour son rapport très intéressant. Le renouvellement de la moitié du Sénat coûte 5 millions d'euros. Combien coûte le renouvellement de l'Assemblée nationale ?

Quelles sont les perspectives d'investissement du Sénat ? Celles de l'Assemblée nationale sont lourdes. Il faudrait peut-être séparer le jardin du Luxembourg du reste des dépenses. En effet, que le jardin relève du budget global du Sénat ne tombe pas sous le sens, et 1,4 million d'euros représentent une somme importante.

M. Michel Canévet. – Quelle sont les perspectives, au regard des réserves dont chaque institution dispose ? Les réserves de l'Assemblée nationale sont estimées à 261 millions d'euros. Pourquoi ne sont-elles pas toutes totalement mobilisables ? Les réserves du Sénat sont estimées à 133 millions d'euros. À combien s'élèvent celles de la présidence de la République ? Ces montants sont à mettre en rapport avec les programmes

pluriannuels d'investissement. Ceux-ci peuvent-ils être mis en œuvre, au regard des disponibilités en réserve, les budgets étant bloqués, pour mener à bien les indispensables programmes de réhabilitation du patrimoine dont les assemblées et la présidence de la République ont la charge ? Les pouvoirs publics peuvent-ils tenir longtemps dans la configuration actuelle ?

M. Jean-Claude Requier. – Le jardin du Luxembourg appartient au Sénat et est ouvert au public. C'est un immense avantage pour la ville de Paris que de pouvoir profiter de ce magnifique jardin très bien entretenu par des jardiniers qui ratissent et nettoient. Les citadins s'imaginent que leur vision, c'est la nature comme partout ailleurs, ce qui n'est malheureusement pas le cas. Je me félicite que la variation de l'amplitude horaire d'ouverture rappelle le rythme de la nature.

Pour le jardin, 1,4 million d'euros sont prélevés sur les disponibilités. Je me réjouis que les recettes augmentent de 10,5 %. C'est bien de rentabiliser ce jardin, même modestement.

M. Marc Laménie. – Merci à notre rapporteur spécial. L'État dote le Sénat de 323 millions d'euros, ce qui est stable. Mais si le Sénat fonctionne bien, c'est grâce aux moyens humains. Les effectifs ont légèrement baissé. A-t-on une idée précise de la répartition des emplois et de l'évolution des effectifs, pour le fonctionnement de notre institution et du jardin ?

M. Jean-Marc Gabouty. – Je souhaite revenir sur les chiffres d'investissement et de fonctionnement, et, pour ces derniers, sur la partie structurelle et la partie conjoncturelle, notamment liée au renouvellement. Celui-ci induit un fort taux de rotation des collaborateurs. Le budget de l'Association pour la gestion des assistants de sénateurs (Agas) représente 58 millions d'euros en année normale, comme 2019, soit 7 % du budget du Sénat. La rotation accélérée en cas de renouvellement augmente encore les besoins financiers.

Pour les deux assemblées réunies, l'insuffisance financière s'élève à 86 millions d'euros. N'ayant pas connaissance du montant des réserves disponibles affectables au comblement de ces déficits, il est difficile d'apprécier les risques de cette gestion non durable.

M. Jean-François Rapin. – Jérôme Bascher dit que le Sénat sera à l'os en 2023. Quelle est la stratégie envisagée ? Que fait-on ? Quels emprunts ? Le Gouvernement contracte des emprunts considérables puisque les taux sont très bas. Qu'en est-il du Sénat ?

M. Victorin Lurel. – Quels sont les indicateurs d'efficacité ? L'autonomie financière des assemblées implique l'absence de projet annuel de performances. Les objectifs fixés sont-ils respectés ?

La Cour des comptes vérifie les comptes des deux assemblées et de l'Élysée. De quand son dernier rapport date-t-il ? Quel est son avis ?

J'ai lu dans la presse que l'Élysée vendait des t-shirts et des colifichets. Cela apparaît-il dans « produits divers » ?

Combien de temps le Sénat tiendra-t-il encore, en prélevant sur les réserves, notamment pour financer les investissements ? Quelles sont les perspectives ? J'ai cru comprendre que l'échéance était fixée à 2023.

Dispose-t-on du détail de ce qui est affecté au Président de la République pour ses actions militaires et diplomatiques ?

M. Jérôme Bascher, rapporteur spécial. – Il est difficile de répondre à toutes les questions car avec cette mission, tel le coucou, on est obligé de venir nicher dans les budgets et les missions des uns et des autres.

Roger Karoutchi a posé une question sur les caisses de retraite. L'Assemblée nationale, qui a soumis la retraite des députés au droit commun, envisage sa mise en gestion à la Caisse des dépôts et consignations, comme c'est déjà le cas pour son personnel. Les réserves prévues pour la caisse « ancien format » sont correctement dotées. Les caisses de retraite du Sénat sont largement provisionnées et ne sont pas fongibles avec le reste des réserves.

Pour répondre à Victorin Lurel et Jean-François Rapin, au rythme actuel de consommation des réserves courantes, l'année de vérité sera 2022 pour l'Assemblée nationale et 2023 pour le Sénat.

Comme l'a dit Thierry Carcenac, on peut tout à fait ralentir les investissements, car il y a toujours des glissements. Chaque institution a sa dotation, mais elle bâtit ensuite son propre budget, avec ses réserves et ses recettes propres.

Les *goodies* de l'Élysée ne font pas vraiment recette ; en revanche, l'Assemblée nationale s'est lancée avec succès dans la vente en ligne ; c'est une très bonne idée, dont pourrait s'inspirer le Sénat.

À votre suggestion, Nathalie Goulet, je mentionnerai dans mon rapport le coût par habitant du Sénat et de l'Assemblée nationale, sur le modèle de ce qui est indiqué sur le site internet du Sénat.

Les matériels informatiques de l'Élysée sont tellement sécurisés qu'ils n'admettent aucun autre logiciel ; cohabitent alors, comme à la gendarmerie, des outils ultra-sécurisés et peu ergonomiques et des outils achetés sur étagère et dont la sécurité laisse à désirer. S'agissant du Sénat, nos matériels sont relativement récents ; le fait que nous ayons tous des matériels différents n'est pas optimal en termes de sécurité, mais le coût d'une standardisation serait disproportionné au regard de la menace, à l'exception peut-être des parlementaires astreints au secret de la défense nationale dans le cadre de la délégation parlementaire au renseignement. Comme le souligne justement Christine Lavarde, toutes nos données sont déjà chez Google, Apple et surtout Amazon !

La vente d'un immeuble de l'Élysée pour 27 millions d'euros en 2022 n'a rien de scandaleux *a priori.* C'est en effet le propre du CAS « Immobilier de l'État » que d'être à l'équilibre et de réaliser des opérations de trésorerie. Je regrette cependant que la présidence de la République ne m'ait pas répondu en 2019 alors que je l'avais spécifiquement interrogée sur ce point.

Si le bureau de la commission en décide ainsi, je conduirai l'an prochain une mission de contrôle budgétaire consacrée à l'immobilier au cours de laquelle je pourrai examiner les schémas directeurs et les plans de financement de chaque institution.

Les réserves immobilières de l'Élysée ont été constituées sous le quinquennat de François Hollande à la faveur d'une sous-consommation des crédits ; elles s'élèvent aujourd'hui à moins de dix millions d'euros, et diminuent chaque année.

Jean-Claude Requier m'a demandé si le Sénat perçoit des recettes propres et j'y ai je crois répondu pour partie. S'agissant de la valorisation des jardins du Sénat, en me rappelant mes responsabilités professionnelles antérieures au ministère de la culture, il me semble qu'ils pourraient intéresser des organisateurs de défilés de mode.

Les effectifs du jardin du Luxembourg ont diminué de 111 à 109 emplois budgétaires. À l'Assemblée nationale, les effectifs devraient baisser plus fortement, car la question de l'externalisation de certaines fonctions a été clairement posée, et pas seulement pour les fonctions informatiques. Il me semble que des marges d'externalisation existent aussi au Sénat, notamment au jardin.

Le Sénat et l'Assemblée nationale reçoivent une dotation qu'ils sont libres d'affecter entre investissement et fonctionnement. Leurs réserves sont aussi totalement fongibles et peuvent être indifféremment affectées à l'investissement ou au fonctionnement. C'est une situation hors normes publiques habituelles.

Les réserves de l'Élysée seront probablement épuisées en 2021, celles de l'Assemblée nationale en 2022 et celles du Sénat en 2023. L'Assemblée nationale et le Sénat n'ont pas recours à l'emprunt, car ils disposent de réserves ; en revanche, ils effectuent des placements sur les marchés financiers, notamment pour financer leurs régimes de retraite.

La mission « Pouvoirs publics » est une mission particulière qui ne comporte aucun indicateur de performance. Toutefois, dans ses réponses au questionnaire budgétaire, le Conseil constitutionnel mentionne le délai moyen de jugement qui s'apparente à un indicateur.

Les comptes de l'Assemblée nationale et du Sénat sont certifiés, mais ne donnent pas lieu à un rapport d'observations de la Cour des comptes. En revanche, l'Élysée a demandé que la Cour des comptes examine son budget et fasse des recommandations.

La fonction de représentation du Président de la République apparaît dans le budget de l'Élysée où 16 millions d'euros sont consacrés à l'action diplomatique, déplacements présidentiels inclus. Mais tout cela n'est pas toujours très clair : l'an dernier, la ligne augmentait à cause du G7 à Biarritz, cette année c'est parce qu'il y a un G20 en Arabie saoudite et un G7 aux États-Unis. Par ailleurs, l'immobilisation de l'A330 présidentiel pendant trois mois pour révision occasionnera probablement des surcoûts.

Dans l'attente de plus amples explications concernant le budget de l'Élysée, je vous propose de réserver notre position sur les crédits de la mission « Pouvoirs publics ».

La commission a donné acte de sa communication à M. Jérôme Bascher, rapporteur spécial, et en a autorisé la publication sous la forme d'un rapport d'information.

LISTE DES PERSONNES ENTENDUES

Sénat

- M. Laurent LAURELUT, responsable de la sécurité des systèmes d'information (RSSI).

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- M. Guillaume POUPARD, directeur général.

Présidence de la République

- M. Jérôme RIVOISI, directeur adjoint de cabinet, directeur général des services.

Public Sénat

- Mme Muriel SIGNORET, secrétaire générale, en charge de la transformation numérique ;

- M. Cédric LAVEAU, directeur de la production et des services supports.

Conseil constitutionnel

- M. Jean MAÏA, secrétaire général ;

- M. Pierre HUREAUX, chef du service informatique.

Ministère de l'intérieur – Direction de la modernisation et de l'administration territoriale

- M. François PESNEAU, adjoint au directeur de la modernisation et de l'administration territoriale ;

- M. Zoheir BOUAOUICHE, chef de projet.