ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête concernant l'organisation des élections en France

Mercredi
5 mars 2025
Séance de 19 heures

Compte rendu n° 19

SESSION ORDINAIRE DE 2024-2025

Présidence de
M. Thomas Cazenave,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-neuf heures.

M. le président Thomas Cazenave. Nous recevons aujourd'hui M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI, créée en 2009, est un service du Premier ministre rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN). En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, son action s'articule autour de quatre missions principales : défendre, connaître, partager et accompagner.

Votre positionnement interministériel vous permet de collaborer avec tous les acteurs publics concernés par ces enjeux. Dans le cadre de notre commission d'enquête sur l'organisation des élections en France, il nous semblait essentiel de vous entendre, notamment sur les aspects numériques liés au vote à distance, au vote par internet et aux machines à voter. Dans un contexte où les risques d'intrusion et de manipulation semblent s'accroître, la fiabilité de nos outils électoraux est primordiale pour garantir le bon déroulement des scrutins.

Je vous rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

(M. Vincent Strubel prête serment.)

M. Vincent Strubel, directeur général de l'ANSSI. Je commencerai mon propos liminaire par un bref rappel du rôle de l'ANSSI avant de me concentrer sur notre intervention dans le domaine des élections, en accordant une attention particulière à la dimension électronique que vous avez soulignée.

La France a opté pour un modèle particulier en matière de cybersécurité avec la création de l'ANSSI en 2009. Notre agence, interministérielle, est placée sous l'autorité du Premier ministre, ce qui nous permet d'intervenir dans tous les domaines en tant qu'arbitre impartial. Contrairement à ce qui a été mis en place dans d'autres pays, l'ANSSI est spécialisée et ne s'occupe que de cybersécurité dans son volet défensif, sans être un service de renseignement ou d'enquête. Cette spécialisation a été maintenue lors de l'émergence des problématiques de manipulation de l'information. Une agence sœur, le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), a été créée afin de détecter les phénomènes d'ingérence étrangère par le biais de manipulation de l'information, un domaine connexe mais distinct de nos missions centrées sur les intrusions informatiques.

Les missions de l'ANSSI, qui compte aujourd'hui environ 650 agents, peuvent être déclinées en trois axes principaux. Il s'agit tout d'abord de la coordination des réponses aux cyberattaques, qui inclut la détection des attaques sur les systèmes d'information de l'État, la connaissance de la menace pour permettre l'anticipation et la remédiation pour mettre fin aux attaques et prévenir leur récurrence. Il s'agit ensuite de la sécurisation de l'État et de ses activités d'importance vitale, à travers la prescription de règles, l'injonction vis-à-vis des ministères ou des administrations et un rôle de régulation qui s'étend aux opérateurs d'importance vitale, y compris sous statut privé. Ce rôle devrait s'élargir avec la transposition de la directive NIS2, actuellement en examen au Parlement. Nous sommes enfin chargés de la promotion générale de la cybersécurité au profit de l'ensemble de la Nation, non pas dans une logique coercitive, mais pour permettre aux entités souhaitant se protéger d'en avoir les moyens. Cela passe par des actions dans les domaines de la formation, de la structuration de l'offre privée, du conseil et de la coordination des politiques publiques.

Ces missions doivent nous permettre de faire face à trois types de menaces principales, au premier rang desquelles la criminalité organisée, qui cherche à générer des profits par l'extorsion de rançons, le vol de données et leur monnayage. Vient ensuite la menace étatique, qui se traduit par de l'espionnage mais également par des risques de sabotage, de destruction d'infrastructures ou de déstabilisation. La dernière menace, davantage protéiforme, émane d'activistes de différentes natures qui utilisent des actions moins techniques, mais à forte visibilité, telles que la saturation de sites web, pour faire passer leurs messages.

Bien que la classification en trois catégories, à savoir le crime organisé, les États et les activistes, soit logique, elle masque une certaine porosité entre ces acteurs. Les États réutilisent parfois les outils des cybercriminels, voire se font passer pour des groupes criminels organisés, et inversement. Les activistes, généralement engagés pour une cause, peuvent également agir en faveur de certains États.

Nous observons en outre une massification de la menace. Autrefois centrée sur quelques acteurs stratégiques et principalement liée à l'espionnage, elle touche désormais un large éventail d'entités, y compris des PME, des collectivités et des associations, qui peuvent être victimes du crime organisé cherchant à extorquer des rançons.

Un autre phénomène récent est la généralisation des tentatives de déstabilisation. Au-delà de l'espionnage et des attaques discrètes, nous observons des actions visant à saturer des sites web et des ressources informatiques ainsi que des actes de sabotage ou de destruction d'infrastructures, y compris physiques. Cette réalité, déjà connue dans des régions telles que l'Ukraine, est également susceptible de toucher la partie occidentale de l'Europe. Le « *hack and leak* », qui consiste à voler des données puis à les publier, parfois avec des modifications subtiles, est utilisé pour perturber le débat public, nuire à l'image d'une entité ou déstabiliser de manière générale.

Cette pratique menace également le processus démocratique et les scrutins électoraux. Ce phénomène a été particulièrement mis en lumière lors de l'élection présidentielle américaine de 2016, lorsque l'équipe de campagne d'Hillary Clinton a subi un vol de données suivi de leur publication progressive. La campagne présidentielle française de 2017 en a également fait les frais, bien que l'impact ait été limité. Les partis politiques sont également victimes de vols de données et d'attaques par déni de service et le processus électoral peut être affecté indirectement par les effets de bord de cyberattaques. Par exemple, une attaque par rançongiciel paralysant une mairie au moment d'un scrutin pourrait nuire à la tenue d'un scrutin, même si cela n'était pas l'objectif initial des attaquants.

Face à ces menaces, l'ANSSI a adopté un rôle particulier dans le cadre des élections, notamment pour ce qui concerne le vote électronique. Cela s'inscrit dans une extension naturelle de notre mission classique car le processus électoral, même traditionnel, repose sur des systèmes d'information critiques de l'État, notamment au sein du ministère de l'intérieur pour la gestion des listes électorales et la collecte des résultats. Notre démarche d'accompagnement consiste à assister les choix techniques dans leur conception, à auditer et tester la sécurité des systèmes et à en assurer la supervision pour détecter d'éventuelles attaques. C'est le cas par exemple du système d'information « Élection 2 », utilisé pour les scrutins nationaux et européens, qui fait l'objet d'un suivi étroit en collaboration avec la direction du management de l'administration territoriale et de l'encadrement supérieur (DMATES) du ministère de l'intérieur.

Depuis 2017, nous avons mis en place un mode de fonctionnement particulier lors des scrutins qui consiste à sensibiliser les partis politiques et les équipes de campagne à la menace et à leur proposer une offre de services. Si l'ANSSI, en tant que service du Premier ministre, ne peut imposer des mesures de sécurité aux partis politiques, elle est à leur disposition pour les aider à sécuriser leurs infrastructures, notamment celles mises en place dans le cadre d'une campagne électorale.

Nous disposons d'un dispositif renforcé d'astreinte, de détection et d'analyse de la menace durant les périodes de scrutin et nous nous mettons alors à la disposition, selon les casn du Conseil constitutionnel, du Conseil d'État ou de la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP). Notre rôle est de notifier et de rendre compte immédiatement de tout incident de cybersécurité susceptible d'avoir un impact sur le scrutin, que ce soit en touchant un parti politique, une équipe de campagne, un système lié au vote ou une collectivité dont l'attaque pourrait empêcher le bon déroulement du vote. Nous fournissons toutes ces informations au juge de l'élection et sommes à sa disposition pour analyser tout incident et mesurer son impact éventuel sur la sincérité du scrutin.

Cette démarche s'inscrit dans un contexte international. En lien avec nos partenaires européens, nous participons au réseau CyCLONe, qui regroupe les directeurs des agences nationales de cybersécurité des pays partenaires européens et qui a mis en place un groupe de travail spécifique pour les élections européennes. En 2024, l'ANSSI a par ailleurs participé à une initiative avec nos partenaires européens visant à favoriser les échanges d'informations, les contacts en cas de crise et la synchronisation sur la perception de la menace. Ce modèle, qui a fait ses preuves, n'est pas limité aux crises affectant les scrutins électoraux. Il permet de synchroniser nos réponses à l'échelle européenne sans empiéter sur les compétences propres des États membres, particulièrement dans le cadre des scrutins européens qui nous concernent tous. Nous l'utilisons également pour les scrutins nationaux, partageant des demandes d'information et d'assistance sur l'analyse de menaces particulières. Dans ce cadre, nous avons élaboré des guides communs, notamment un compendium sur la cybersécurité des élections, disponible sur le site de la Commission européenne. Ce document a été préparé par les agences nationales de cybersécurité des États membres en prévision du scrutin européen.

Concernant le vote électronique, il convient de distinguer le vote en mairie sur une machine à voter et le vote par internet sur les terminaux personnels des électeurs, notamment pour les Français de l'étranger. La réalité incontournable qui s'impose est que le vote électronique sera toujours, par nature, moins sécurisé que le vote à l'urne. Plusieurs raisons expliquent cela. Premièrement, l'introduction d'une dépendance numérique implique qu'il ne puisse exister une sécurité de 100 %. Qu'il s'agisse d'une machine électronique pour voter ou, à plus forte raison, des terminaux personnels des électeurs, des vulnérabilités existent et ne peuvent être totalement contrôlées. Deuxièmement, l'intégrité, le secret et la liberté attendus lors d'un scrutin sont difficiles à obtenir simultanément sur le plan informatique. Bien que chacune de ces propriétés puisse être garantie individuellement, leur combinaison représente un défi technologique majeur, nécessitant des solutions de pointe, notamment en matière de cryptographie. Troisièmement, et il s'agit du point de fragilité le plus important, se pose la question de l'intelligibilité. Contrairement au vote traditionnel, dont les mécanismes de sécurité sont facilement compréhensibles par tous, l'évaluation critique des systèmes de vote électronique requiert des connaissances scientifiques pointues, hors de portée du citoyen moyen. Cela soulève une limite fondamentale, celle de la confiance dans le vote, qui repose désormais sur un panel d'experts et non plus sur le citoyen lui-même.

Ces facteurs engendrent plusieurs risques spécifiques au scrutin électronique : le risque de détournement pour modifier les résultats, le risque d'atteinte au secret du vote, le risque de coercition, particulièrement pour le vote sur terminaux personnels et, sans doute le plus préoccupant, le risque de déstabilisation et d'atteinte à la confiance dans le processus démocratique. Ce dernier point est particulièrement sensible face à des attaquants dont l'objectif pourrait être de décrédibiliser le processus démocratique. Une simple revendication d'attaque, même infondée, pourrait porter une atteinte significative à la confiance des citoyens, compte tenu de la complexité technique du système.

Ces risques doivent néanmoins être mis en balance avec les bénéfices attendus. Le vote par internet, par exemple, représente souvent la seule option viable pour les Français résidant loin des bureaux de vote à l'étranger. Il apparaît comme une alternative préférable au vote par correspondance, qui n'offre pas non plus de grandes garanties en termes de confiance et de secret. L'évaluation du risque doit également prendre en compte l'impact potentiel d'un dysfonctionnement, en considérant le nombre d'électeurs participant au scrutin et la nature de celui-ci. L'usage des machines à voter en France se trouve dans une situation particulière. Le moratoire instauré il y a quelques années visait à limiter l'impact potentiel d'un dysfonctionnement en restreignant le nombre d'électeurs utilisant ce mode de scrutin. Le choix des scrutins éligibles au vote par internet pour les Français de l'étranger n'est pas anodin non plus. Réserver cette modalité aux scrutins à plusieurs circonscriptions limite les conséquences d'éventuels problèmes. L'étendre à des circonscriptions uniques, comme pour les élections européennes ou présidentielles, aurait des implications bien plus importantes, compte tenu du nombre d'électeurs.

Face à ces risques, l'ANSSI agit de plusieurs manières. Nous avons élaboré en octobre 2021 des recommandations sur la sécurité des machines à voter, qui ont été publiées par le ministère de l'intérieur. Nous apportons également une assistance technique, particulièrement pour le vote par internet des Français de l'étranger, grâce à une coopération qui dure depuis dix ans. L'ANSSI a accompagné le déploiement de trois solutions successives, dont la plus récente, développée par Voxaly-Docapost, a été utilisée avec succès pour les élections législatives anticipées de 2024. Je tiens à souligner la réussite remarquable de cette mise en œuvre, malgré des délais très courts, notamment grâce aux équipes du Quai d'Orsay et à tous les contributeurs.

Notre rôle dans le vote par internet des Français de l'étranger inclut également la participation au bureau de vote électronique. Cette instance, chargée de superviser le processus, réunit des représentants des ministères concernés, des élus consulaires et des experts indépendants. L'ANSSI participe à la supervision des opérations, notamment le descellement des urnes, et explicite les éventuels risques ou incidents.

Concernant la sécurité, je peux affirmer qu'aucune attaque majeure n'a été constatée lors des scrutins par internet pour les Français de l'étranger. Les vulnérabilités identifiées en amont, principalement par des travaux de recherche et des lanceurs d'alerte, ont permis d'effectuer les corrections nécessaires. Les incidents rencontrés étaient principalement liés à l'acheminement des SMS, qui reste le point faible de la solution en l'absence d'une identité électronique forte, l'envoi massif de SMS à travers le monde posant des défis logistiques.

Je dois enfin évoquer la situation particulière de 2017. La décision difficile d'annuler le vote par internet des Français de l'étranger a été prise en raison d'une refonte tardive de la plateforme, imposée par des évolutions technologiques externes, ne permettant pas de garantir la sécurité nécessaire. Cette expérience a été riche en enseignements et a conduit à des améliorations significatives. Nous disposons aujourd'hui d'une plateforme de vote par internet qui fonctionne

bien, comme l'ont démontré les récentes élections anticipées. Cependant, la prudence reste de mise quant à son extension à d'autres modalités ou scrutins, que ce soit pour les électeurs du territoire national ou pour d'autres types d'élections concernant les Français de l'étranger.

M. Antoine Léaument, rapporteur. Je tiens tout d'abord à souligner la qualité du travail effectué par l'ANSSI au quotidien, qui ne se limite pas au cadre des élections. Je vous prie de transmettre les remerciements de la représentation nationale à vos équipes.

Concernant les élections politiques, au-delà des sujets déjà évoqués sur le scrutin électronique, quelles sont les menaces potentielles qui pèsent sur les scrutins traditionnels, notamment lors de la remontée des résultats ? J'identifie deux points de vulnérabilité. Premièrement, le répertoire électoral unique. Une puissance étrangère ou des acteurs malveillants pourraient tenter de perturber les informations qu'il contient, non pas nécessairement pour empêcher la tenue du vote mais pour compliquer l'organisation des élections et jeter ainsi le doute sur la sincérité du scrutin. Nous savons qu'aux États-Unis, par exemple, la contestation des résultats est allée jusqu'à l'envahissement du Congrès. Deuxièmement, la transmission des résultats. Vous avez évoqué deux risques principaux : la modification effective des résultats et la création d'une fausse impression de modification pour semer le doute et la désinformation. Pourriez-vous développer davantage ces aspects ?

Par ailleurs, sans compromettre la sécurité nationale, pouvez-vous nous donner des exemples de tentatives d'ingérence dans nos processus électoraux ? Vous avez brièvement mentionné des risques concernant les Français de l'étranger en 2017. Pouvez-vous préciser la nature de ces risques ?

Enfin, le sujet de l'utilisation des réseaux sociaux pour manipuler l'information ou discréditer les résultats électoraux relève-t-il de vos missions ou de celles de Viginum ?

M. Vincent Strubel. La supervision des réseaux sociaux n'est pas du ressort de l'ANSSI mais de Viginum. La mission consiste à détecter non pas les fausses informations en tant que telles, mais leur amplification artificielle. Nous travaillons cependant en étroite collaboration avec eux, notamment face à des attaquants qui peuvent mener des intrusions concrètes dans les systèmes d'information ou revendiquer des attaques de manière exagérée ou totalement fantaisiste. Pour illustrer ce point, prenons l'exemple des Jeux olympiques et paralympiques de Paris 2024, dont l'ANSSI était chargée d'assurer la cybersécurité. Nous avons fait face à des attaques d'activistes qui ont prétendu avoir pollué la Seine par une cyberattaque. Bien que la tentative technique ait échoué, ils ont cherché à déstabiliser l'organisation des JO en faisant croire au succès de l'opération. Notre approche préventive a non seulement consisté à s'assurer que de telles attaques n'étaient pas possibles, mais également à travailler avec les médias et toutes les parties prenantes pour partager rapidement les faits démontrant la fausseté de ces allégations.

Concernant le processus électoral en France, il est beaucoup plus facile de mettre en doute la sincérité du scrutin que de le perturber réellement. Notre organisation des scrutins est relativement résiliente et robuste en termes de garanties de sécurité et de détection des problèmes. Cette situation est d'autant plus vraie que nous faisons face à des adversaires qui contestent systématiquement notre modèle démocratique et qui auraient tout intérêt à le discréditer sans nécessairement le perturber concrètement. Truquer une élection par une cyberattaque dans notre modèle est extrêmement complexe. Cependant, le simple fait de laisser planer le doute sur la sincérité d'un scrutin présidentiel en raison d'une cyberattaque supposée pourrait causer une grave atteinte à la confiance que portent les citoyens au processus démocratique, indépendamment de la validation du scrutin par le Conseil constitutionnel.

Le scrutin à l'urne est plutôt robuste, avec des dépendances numériques limitées. Le répertoire électoral unique, que vous avez mentionné, est relativement simple à surveiller et à protéger. Sa centralisation facilite sa protection en permettant de concentrer les efforts. La collecte des résultats par le biais de systèmes numériques simples ne pose pas de défis particuliers en termes de sécurisation et peut être aisément supervisée. De plus, un éventuel trucage de cette remontée électronique des résultats serait détectable *in fine*, puisque nous conservons toujours une trace papier. Nous conservons la capacité de vérifier les résultats de manière traditionnelle, avec un papier et un crayon, en s'assurant que les votes remontés correspondent bien à ceux déposés dans l'urne, grâce à une traçabilité intégrale du scrutin. Si la sécurisation de ce processus n'est donc pas particulièrement complexe, garantir sa sécurité et sa transparence l'est davantage et il est important que nous puissions nous exprimer devant la représentation nationale pour expliquer ces aspects.

Concernant des exemples de tentatives de déstabilisation, nous pouvons citer la campagne électorale américaine de 2016, marquée par un vol de données et leur divulgation progressive. Cette opération très organisée visait à déstabiliser une candidate. En 2017, une tentative similaire a eu lieu en France avec les *MacronLeaks*, mais avec moins de succès en raison d'un périmètre plus restreint et de sa proximité avec le scrutin.

Aujourd'hui, ce sont probablement les partis politiques et les campagnes électorales qui représentent le maillon le plus faible en termes de cybersécurité. Ces structures, souvent comparables d'un point de vue numérique à des PME ou des start-ups, ne disposent pas de systèmes d'information aussi développés que ceux du ministère de l'intérieur, supervisés par l'ANSSI. Bien que nous proposions une offre de services pour aider les partis politiques, nous ne pouvons pas leur imposer ces mesures.

Concernant l'incident de 2017 sur la plateforme de vote par internet des Français de l'étranger, il s'agissait essentiellement d'une surchauffe. La plateforme utilisait une technologie Java, qui a été interdite par les navigateurs peu avant le scrutin. Cela a nécessité un redéveloppement urgent de la plateforme. Dans les dernières semaines, les équipes de développement étaient surchargées et la correction d'un problème en créait souvent de nouveaux. En raison de ces limites internes et circonstancielles, nous n'avons pas pu atteindre un niveau de sécurité satisfaisant dans les délais impartis.

M. le président Thomas Cazenave. Je souhaite revenir sur la question des machines à voter. Si je comprends bien, toute utilisation d'un élément numérique implique un risque. Pouvez-vous préciser les difficultés liées à ces machines ? Il semble que la situation soit problématique puisque certaines communes utilisent des équipements vieillissants. Bien qu'un moratoire ait été instauré, les communes utilisatrices ne souhaitent pas revenir en arrière mais ce *statu quo* ne pourra pas durer indéfiniment. Quelle est votre recommandation pour sortir de cette impasse ? Le fait que ces machines ne soient connectées à rien limiterait prétendument les risques d'intrusion. Est-ce vraiment le cas ? Pourriez-vous détailler les risques liés aux machines à voter dans le cadre actuel et comment envisagez-vous l'évolution de ce moratoire ? Quelles solutions pourrions-nous envisager ?

M. Vincent Strubel. C'est une vaste question !Tout d'abord, il faut comprendre qu'aucun système informatique n'est totalement isolé. Les machines à voter, bien que peu connectées, le sont à certains moments. En amont, lors du processus de développement et d'intégration des composants logiciels, il existe des points de connexion. Ces machines comportent un système d'exploitation, divers logiciels, probablement un navigateur, autant d'éléments qui peuvent potentiellement être compromis. De plus, même si ces machines sont

scellées entre deux scrutins, elles doivent être reconfigurées pour chaque élection. Cela implique souvent l'utilisation d'une clé USB, qui crée un autre point de vulnérabilité. Bien que la France ne soit pas nécessairement concernée, dans d'autres pays, des chercheurs ont démontré qu'il était possible de compromettre certaines machines à voter simplement en branchant une clé USB. Ces systèmes ne fonctionnent donc pas en totale autarcie et il existe des vecteurs potentiels de compromission à différentes étapes : par les électeurs, lors de la configuration du vote ou encore au moment de la collecte des résultats. Bien qu'elles ne soient normalement pas connectées à internet, les machines à voter restent des systèmes d'information complexes et potentiellement attaquables.

Dans ce contexte, le moratoire prononcé il y a quelques années était probablement la moins mauvaise des décisions, puisqu'il visait à freiner un déploiement accéléré de ces machines alors que les risques étaient mal maîtrisés. Cependant, le maintien du *statu quo* montre aujourd'hui ses limites, car les machines vieillissent sans évoluer et sans que la question soit réglée. Ces dernières années, l'ANSSI a élaboré des recommandations concernant ces machines, visant à améliorer leur sécurité, à limiter les risques de cyberattaques et à garantir la transparence du scrutin. Ces recommandations, qui ont été transmises au ministère de l'intérieur et aux parlementaires en 2021, se heurtent toutefois à la réalité car les machines actuellement en service ne sont pas nécessairement conformes à ces nouvelles exigences.

Un point crucial de nos recommandations est l'introduction systématique d'une trace papier du vote. Cela implique la matérialisation du choix de l'électeur sur un bulletin papier, qui serait ensuite réinjecté dans la machine pour le décompte électronique. Cette approche permettrait de conserver les avantages de la tabulation automatique tout en offrant la possibilité d'une vérification manuelle en cas de doute.

D'autres améliorations, bien que plus complexes à mettre en œuvre, sont également nécessaires. Il s'agit notamment de l'audit systématique du code source des machines à voter et de la mise en place de processus d'intégrité renforcés. Ces derniers devraient inclure des vérifications de l'intégrité du logiciel, en particulier lors de la configuration des machines, pour s'assurer qu'aucune modification non autorisée n'a été effectuée. Il est par ailleurs nécessaire d'intégrer un mécanisme de mise à jour sécurisé. Les machines à voter, comme tout système informatique complexe, reposent sur divers composants logiciels susceptibles de présenter des vulnérabilités ou des bugs. L'absence d'un processus de mise à jour pourrait conduire à des situations de vulnérabilité à long terme.

La mise en œuvre de ces recommandations nécessiterait des modifications substantielles des machines à voter actuellement disponibles sur le marché. Je n'ai pas à me prononcer sur le processus décisionnel qui pourrait mener à un changement des règles en matière de machines à voter ou à la levée du moratoire, mais il est clair que des améliorations significatives sont nécessaires et qu'elles ne peuvent être simplement décrétées, car elles impliquent des évolutions technologiques importantes.

M. le président Thomas Cazenave. Si je comprends bien votre raisonnement, il serait envisageable de maintenir en conditions opérationnelles et de continuer à sécuriser le parc existant de machines à voter. Dans cette optique, rien n'empêcherait alors de poursuivre le déploiement de ces machines dans les communes qui en sont dotées, ce qui permettrait de sortir du *statu quo* actuel.

Pour résumer ce que vous avez exposé, il semble qu'en l'état actuel certaines conditions ne soient pas entièrement réunies, notamment en ce qui concerne la maintenance.

Cependant, si ces conditions étaient satisfaites, il serait alors acceptable de poursuivre l'utilisation des machines à voter existantes et potentiellement d'envisager leur déploiement dans de nouvelles communes intéressées. Est-ce bien le point de vue que vous défendez ?

M. Vincent Strubel. Tout en précisant que je ne suis pas nécessairement légitime pour trancher ce débat qui dépasse largement les questions de cybersécurité, je confirme qu'il est effectivement nécessaire de sortir tôt ou tard de la situation actuelle, qui n'est ni satisfaisante ni soutenable sur le long terme.

Deux options raisonnables peuvent être envisagées pour sortir de cette impasse, avec toutes les précautions qui s'imposent : renoncer de manière générale aux machines à voter et conserver uniquement le vote à l'urne traditionnel ou ouvrir la possibilité d'utiliser les machines à voter, mais avec des conditions et des exigences techniques clairement définies, offrant la meilleure protection possible. Nous devons néanmoins garder à l'esprit que, même avec toutes les mesures techniques envisageables, nous n'atteindrons jamais le même niveau de sécurité ni d'intelligibilité qu'avec le vote à l'urne traditionnel.

Le choix doit être fait en considérant les bénéfices attendus. Déployer des machines à voter vise à obtenir un avantage par rapport au vote à l'urne traditionnel mais l'évaluation de ces bénéfices dépasse mon domaine de compétence.

M. le président Thomas Cazenave. Dans le cadre de vos responsabilités, avez-vous eu connaissance de machines à voter ayant posé des difficultés ? Avez-vous été saisi de cas concrets soulevant des doutes légitimes ou avérés sur l'intégrité de ces machines ?

M. Vincent Strubel. À l'étranger, les exemples de dysfonctionnements et de vulnérabilités liés aux machines à voter sont nombreux et ont été illustrés dans des travaux de recherche, sans qu'une cyberattaque soit nécessairement impliquée.

Concernant les machines à voter utilisées en France, je m'exprime avec prudence, d'une part parce que je pense que les défauts constatés ont été corrigés et, d'autre part, pour éviter de susciter de doutes injustifiés sur leur fiabilité actuelle. Il faut rappeler que le moratoire prononcé à l'époque faisait suite à l'identification d'un certain nombre de limites en matière de sécurité des machines à voter telles qu'elles étaient alors mises en œuvre. Cette situation a conduit non seulement à des correctifs mais également à une décision de prudence compte tenu des faiblesses identifiées.

M. le président Thomas Cazenave. Si je comprends bien, dans les années récentes, vous n'avez pas été saisi de cas de doutes concernant les machines actuellement en service, qui présenteraient des risques ou des failles susceptibles de jeter le doute sur l'intégrité du scrutin.

M. Vincent Strubel. Je n'ai effectivement pas connaissance de telles situations.

M. Antoine Léaument, rapporteur. Deux interrogations supplémentaires méritent d'être soulevées. Premièrement, s'agissant de la faille centrale que vous avez évoquée, le facteur humain apparaît comme un risque majeur. Récemment, plusieurs députés et sénateurs ont été victimes d'une campagne d'hameçonnage, révélant ainsi une possible insuffisance de formation, y compris parmi les détenteurs de responsabilités politiques. Dans mes fonctions antérieures, lorsque j'avais la charge de la communication numérique d'un candidat à l'élection présidentielle, nous avions collaboré avec vos services afin de sécuriser l'accès aux réseaux sociaux. Il est apparu qu'une formation, même minimale, permettait de déjouer des attaques qui, bien qu'efficaces, restent relativement simples à contrer.

Pensez-vous qu'il serait pertinent d'instaurer des formations obligatoires en cybersécurité à l'intention de certains responsables publics, notamment les parlementaires ? Une telle mesure pourrait-elle contribuer à renforcer la sûreté de l'État en prévenant des failles exploitables ? Je mesure la complexité d'un tel dispositif, notamment la nécessité de concilier la confiance envers les services étatiques chargés de la sécurité avec la réticence que pourrait susciter l'idée qu'une agence gouvernementale puisse avoir accès aux données sensibles d'un parti politique.

Vous semblez par ailleurs considérer que l'un des principaux risques pesant sur les élections réside dans la vulnérabilité des partis politiques eux-mêmes, certains faisant preuve d'un manque de compétences techniques ou d'intérêt pour la sécurisation de leurs données.

Ma seconde question porte sur le vote électronique à distance. Vous avez mentionné les enjeux liés à la sécurité des appareils. Supposons qu'à l'issue des travaux de cette commission d'enquête, il soit décidé que le vote à distance constitue une solution efficace pour favoriser la participation électorale, en particulier celle des jeunes. Dans cette hypothèse, une cyberattaque menée au moyen d'une application ludique virale, massivement téléchargée sur les téléphones, pourrait-elle représenter une menace sérieuse pour l'intégrité du scrutin ? Une telle application pourrait-elle intégrer un outil permettant d'altérer le vote des citoyens, ou ce scénario relève-t-il de la pure fiction ?

M. Vincent Strubel. Dans le cas d'un scrutin à distance, c'est l'ordinateur ou le téléphone de l'électeur qui vote. Bien que ces appareils votent en principe conformément à la décision de l'électeur, il est difficile de le garantir car cela dépend de la sécurité et de l'intégrité du terminal. Rien ne peut être imposé en la matière et il serait impensable d'exiger que les électeurs votent uniquement avec certains modèles de smartphones réputés plus sécurisés. Cette garantie n'existera jamais, ni pour les téléphones ni pour les ordinateurs.

Le scénario que vous évoquez, qui consisterait à duper les électeurs pour qu'ils installent une application truquée capable de manipuler les téléphones, est probablement le plus crédible. Cependant, une telle attaque à grande échelle, visant les téléphones de tous les électeurs Français à l'étranger, reste complexe à mettre en œuvre. Elle pourrait avoir pour but de copier le vote exprimé, violant ainsi le secret du vote, ou de le modifier. Bien que difficile, cela n'est pas impossible. Bien qu'il soit plus aisé de semer le doute sur la fiabilité du vote que de réellement truquer une élection, cela peut suffire à ébranler la confiance dans le processus électoral.

Concernant la sensibilisation, aucune action n'est de trop. Nous devons toutefois admettre que même les personnes les plus sensibilisées, y compris le directeur général de l'ANSSI, peuvent commettre des erreurs telles que cliquer sur un lien malveillant. La sécurité ne peut donc reposer uniquement sur la sensibilisation, bien que celle-ci reste importante. La sensibilisation des personnes exposées, dont font partie les parlementaires, est effectivement cruciale. Quant à rendre cette formation obligatoire, cela soulève des questions de séparation des pouvoirs et ne relève pas de mon domaine de compétences. L'ANSSI propose déjà des sessions de sensibilisation aux parlementaires des deux chambres, soit directement, soit par le biais des services de l'Assemblée nationale ou du Sénat formés par l'ANSSI.

Le principal enjeu de formation que j'identifie est la faible compréhension générale des enjeux numériques, qu'il s'agisse de manipulation de l'information ou de cyberattaques. Cette méconnaissance constitue un facteur de fragilité de nos sociétés face à des menaces hybrides. Le manque de compréhension du numérique ou de la nature d'une cyberattaque facilite la tâche des attaquants, en particulier lorsqu'ils cherchent à déformer la réalité ou à faire croire à des attaques plus importantes qu'elles ne le sont en réalité.

Pour illustrer ce point, prenons l'exemple des attaques par déni de service subies par les sites web du Sénat et de l'Assemblée nationale. Ces attaques, qui consistent à saturer un site web pour le rendre inaccessible pendant quelques heures, ont parfois été présentées dans la presse comme des cyberattaques russes paralysant l'Assemblée nationale ou le Sénat. Cette description est largement exagérée et inexacte. Ces incidents, bien que gênants, prennent naturellement fin après un certain temps. Pourtant, leur perception et leur traitement médiatique peuvent amplifier considérablement leur impact réel. Dans le cas évoqué, l'intervention d'activistes pro-russes ne signifiait pas nécessairement une implication de l'État russe. En outre, le fonctionnement n'a pas été paralysé, les travaux essentiels se sont poursuivis et le site web du Sénat est resté accessible. À ma connaissance, aucune donnée n'a été volée. La tendance de notre société à dramatiser des événements mineurs constitue un facteur de fragilité.

Consciente que la formation peut jouer un rôle crucial dans la lutte contre ces phénomènes, l'ANSSI travaille depuis un certain temps sur cet axe. Nous développons des formations de spécialistes en cybersécurité pour répondre aux besoins du secteur et collaborons également avec l'éducation nationale, notamment via le programme PICS, pour intégrer ces notions dans le cursus des collégiens et des lycéens. C'est à ce stade que nous formons les futurs citoyens et que nous pouvons leur présenter les métiers de la cybersécurité, un domaine où les opportunités sont nombreuses et qui manque de personnels qualifiés. L'objectif est également de transmettre une compréhension de ces enjeux, afin que les citoyens de demain disposent des outils nécessaires pour faire face à ces défis, ce qui nous aidera collectivement à lutter contre ce type de menaces.

Concernant notre rôle auprès des partis politiques, il est important de rappeler que l'ANSSI n'est pas une autorité indépendante. Nous sommes donc extrêmement prudents dans notre offre de services aux partis politiques, tout en restant disponibles pour apporter l'aide nécessaire. Dans notre offre, nous rappelons également que l'ANSSI n'est pas le seul acteur capable d'apporter une assistance en matière de cybersécurité. La France bénéficie en effet d'un écosystème de prestataires privés qui a été structuré ces dernières années grâce à des certifications délivrées par l'ANSSI. Ces certifications attestent de la confiance qui peut être accordée à ces prestataires et à leurs compétences. Ils peuvent réaliser des audits, fournir des conseils et constituent notre dernier ajout au portefeuille de prestataires qualifiés. Cette recommandation fait partie des premières orientations proposées à un parti politique sollicitant de l'aide, qu'il se considère comme une cible potentielle de cyberattaques ou qu'il cherche simplement à renforcer sa cybersécurité. Dans ce cadre, plusieurs options lui sont présentées : une assistance directe peut être apportée si le parti le souhaite et un catalogue de solutions recommandées est également mis à disposition. D'autres solutions, non spécifiquement recommandées par l'État, restent accessibles en toute liberté de choix. L'objectif est d'accompagner ces acteurs dans leur recherche d'assistance, y compris auprès d'autres organismes, en tenant compte du fait que l'intervention d'un service de l'exécutif auprès d'un parti politique s'accompagne nécessairement de certaines considérations.

L'ANSSI repose sur deux piliers indispensables à la poursuite de ses missions, qui sont son expertise et la confiance des bénéficiaires. Nous sommes extrêmement attentifs à ces aspects dans l'ensemble de nos missions. Lorsque nous traitons une cyberattaque, nous appliquons une forme stricte de secret professionnel et ne divulguons jamais d'informations car cela serait contraire à notre éthique.

M. Antoine Léaument, rapporteur. Ma dernière question se situe à l'intersection de vos missions et de celles de Viginum, tout en touchant également au domaine de la presse. L'un des principaux risques que j'identifie pour les prochaines échéances électorales, en particulier

l'élection présidentielle à venir, réside dans une manipulation de l'information à la fois polymorphe et sophistiquée. Avec l'émergence de logiciels de plus en plus performants, il ne s'agit plus seulement de diffuser de fausses informations mais de générer de faux contenus, tels que les *deepfakes*. Ces technologies permettent de produire des contenus factices, y compris des mises en scène dans lesquelles un candidat ou une candidate pourrait tenir des propos à l'opposé de ses positions habituelles, voire appeler à voter en faveur d'un adversaire. Une telle vidéo relayée massivement sur les réseaux sociaux sèmerait la confusion parmi les électeurs. La meilleure réponse résiderait certes dans la formation du public et dans sa capacité, a priori spontanée, à identifier qu'un candidat ne peut pas, du jour au lendemain, renier l'ensemble de ses déclarations. Toutefois, une manipulation informationnelle d'ampleur, associée par exemple au piratage du site d'un média au moment opportun pour en renforcer l'apparente véracité, pourrait faire peser un risque considérable sur la sincérité du scrutin.

Dans une situation aussi critique, puisque nous sommes ici dans un scénario de crise majeure, les services de l'ANSSI et de Viginum disposent-ils de moyens d'action permettant de faire supprimer, de manière rapide et massive, ces contenus frauduleux sur les réseaux sociaux ? Vous avez évoqué le rôle de « cyberpompiers » : seriez-vous en mesure d'intervenir contre des contenus manifestement fallacieux, potentiellement publiés par des comptes affiliés à des puissances étrangères cherchant à déstabiliser l'élection ?

Par ailleurs, afin d'éviter toute dérive arbitraire, envisagez-vous un dispositif de collaboration avec les équipes des candidats à l'élection présidentielle ? L'objectif serait qu'ils puissent bénéficier d'un canal direct avec vos services afin de signaler des contenus frauduleux, en demandant par exemple la suppression immédiate d'une vidéo qui ne proviendrait pas du candidat et constituerait une menace pour l'intégrité du scrutin. Une telle approche a-t-elle déjà été envisagée ? Lors des deux précédentes élections présidentielles, période durant laquelle je travaillais auprès d'un candidat, j'ai acquis la conviction que la meilleure manière de garantir la sincérité du scrutin sur cet enjeu spécifique serait d'accorder aux candidats une capacité de signalement rapide et efficace des contenus qui leur sont frauduleusement attribués. De plus, une démarche collégiale favoriserait, selon moi, la confiance des acteurs politiques dans l'outil et l'infrastructure mis en place. Une telle solution vous semble-t-elle réaliste ou envisageable ?

M. Vincent Strubel. Il m'est difficile de ne pas réagir à la question des opportunités offertes par l'intelligence artificielle, tant en matière de génération de contenus que dans le domaine des cyberattaques. Je demeure convaincu que l'IA ne permet pas de réaliser l'impossible, mais qu'elle simplifie considérablement des tâches qui, auparavant, requéraient un haut niveau d'expertise. Par exemple, la falsification d'une photographie ou d'une vidéo était déjà envisageable avant l'émergence de l'IA mais nécessitait des compétences techniques avancées. Désormais, ces pratiques sont largement démocratisées, offrant à des acteurs malveillants moins expérimentés des moyens d'action jusque-là hors de leur portée. S'agissant des cyberattaques, l'IA ne constitue pas en soi un facteur de rupture mais agit plutôt comme un levier, facilitant à la fois le travail des attaquants et celui des défenseurs.

S'agissant du retrait de contenus frauduleux, il convient d'aborder cette question avec prudence, car elle ne relève pas des missions de l'ANSSI, ni de celles de Viginum. Notre rôle se limite à la détection, l'analyse et l'explication des manipulations de l'information, sans pouvoir d'intervention directe. Dans le cas que vous évoquez, des procédures légales existent déjà pour demander le retrait de contenus litigieux, celles-ci étant généralement encadrées par un magistrat. Dans le cadre d'une procédure électorale, cette compétence reviendrait, selon toute vraisemblance, au juge de l'élection.

Même en cas d'attaque d'ampleur survenant dans les derniers instants d'un scrutin et susceptible d'en altérer le résultat, l'intégrité ou la sincérité, notre première réponse, conformément à l'organisation mise en place depuis 2017, consisterait à saisir le juge de l'élection. C'est à lui qu'il appartiendrait d'évaluer l'impact d'un tel événement et de déterminer les mesures à adopter, celles-ci pouvant, dans des cas extrêmes, aller jusqu'à l'invalidation du scrutin. Il est essentiel de préserver la séparation des pouvoirs et de veiller à ce que l'exécutif n'outrepasse pas son rôle dans l'organisation du processus électoral.

M. Antoine Léaument, rapporteur. J'ai effectivement évoqué le risque d'arbitraire inhérent à ce type de décision. La difficulté majeure de ces contenus réside dans leur viralité exceptionnelle. Le temps que le juge de l'élection prenne une décision de suppression, l'information aura déjà largement circulé. Cet enjeu crucial, qui reste en suspens, est particulièrement préoccupant dans la perspective de la prochaine élection présidentielle.

J'ai eu l'occasion de rencontrer un candidat à une élection présidentielle en Bolivie qui a été victime d'une fausse vidéo diffusée principalement sur des messageries telles que WhatsApp. Il a perdu l'élection avec seulement deux points d'écart, ce qui soulève des questions sur la sincérité du scrutin. Ma question porte donc sur l'existence de telles capacités techniques pour effectuer un retrait massif de contenus si une décision de justice l'ordonnait.

M. Vincent Strubel. Si les mécanismes de retrait des contenus existent et sont prévus par la loi, la mise en œuvre dans le cadre d'un scrutin soulève une difficulté fondamentale de notre métier : il est toujours plus compliqué de défendre que d'attaquer. Un défenseur agissant dans la légalité et le respect de principes fondamentaux est en effet soumis à des contraintes que l'attaquant ne subit pas.

Or, face à un enjeu aussi capital que celui de l'intégrité électorale, il existe peut-être des aspects à repenser concernant les capacités d'intervention du juge de l'élection. Je peux imaginer un scénario de cyberattaque impliquant des échanges entre un parti politique ciblé, l'ANSSI et le juge de l'élection. Bien que cette intermédiation soit probablement plus complexe à mettre en œuvre, l'impact de l'inaction sur la confiance dans l'élection serait plus néfaste.

M. le président Thomas Cazenave. Je vous remercie pour cet échange passionnant sur ce sujet important qui faisait partie des interrogations de notre commission d'enquête.

La séance s'achève à vingt heures dix.

———

Membres présents ou excusés

Présents. – M. Bruno Bilde, M. Thomas Cazenave, M. Antoine Léaument

Excusé. – M. Xavier Breton