ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Jeudi
16 février 2023
Séance de 15 heures 30

Compte rendu n° 13

SESSION ORDINAIRE DE 2022-2023

Compte rendu

Commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français

Présidence de
M. Jean-Philippe Tanguy,
Président de la commission

ASSEMBLÉE NATIONALE

Jeudi 16 février 2023

La séance est ouverte à quinze heures trente-cinq.

(Présidence de M. Jean-Philippe Tanguy, président de la commission)

———

M. le président Jean-Philippe Tanguy (RN). Nous avons le plaisir d'auditionner cet après-midi M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), M. Vincent Strubel, directeur de l'Agence nationale de sécurité des services d'information (ANSSI), et M. Gabriel Ferriol, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Avec cette audition, nous achevons nos travaux consacrés aux services de renseignement, qui nous ont amenés à interroger les responsables de la direction générale de la sécurité intérieure (DGSI), de la direction générale de la sécurité extérieure (DGSE), de Tracfin et de la direction nationale du renseignement et des enquêtes douanières (DRNED).

Du fait de la position centrale du SGDSN dans la mise en œuvre de la politique française de défense et de sécurité, nous attendons de cette audition qu'elle nous éclaire sur le degré d'intensité des tentatives d'ingérence et des ingérences avérées auxquelles la France est confrontée, que ce soit dans la vie politique – nationale et locale –, dans la vie économique, dans les médias ou dans les relais d'opinion.

Nous serons également heureux de vous entendre plus spécifiquement sur un aspect essentiel de la politique de défense et de sécurité : les ingérences par voie électronique, qui emportent des enjeux de souveraineté nationale et de survie de la démocratie.

Avant de vous laisser la parole pour un propos liminaire, je vous rappelle qu'en vertu de l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, les personnes auditionnées par une commission d'enquête doivent prêter serment de dire la vérité, toute la vérité, rien que la vérité. Aussi, je vous invite à lever la main droite et à dire : « Je le jure. »

(MM. Stéphane Bouillon, Vincent Strubel et Gabriel Ferriol prêtent serment.)

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Le SGDSN contribue, au sein de l'État, à la protection du pays non seulement contre les menaces ouvertes et affirmées, sur lesquelles vous êtes amenés à travailler également, mais aussi contre celles, plus discrètes, sournoises, qui visent à nous affaiblir sans que le seuil de conflictualité ne soit franchi, et parfois même sans que leurs auteurs ne puissent être identifiés.

Le champ de ces menaces s'est étendu et complexifié au cours des dernières années, compte tenu de la situation internationale, et leur impact est de plus en plus perceptible sur notre sol. Parmi ces menaces, figurent celles qui sont qualifiées d'« hybrides ». Nous les avons classées en plusieurs catégories.

Il y a d'abord les attaques dans le cyberespace, dont l'ampleur devient considérable. Si elles sont souvent de nature criminelle, visant à extorquer une rançon ou à vendre des

données préalablement pillées – c'est ce qui s'est passé avec nos hôpitaux –, elles peuvent aussi répondre à des objectifs d'espionnage et se traduire par la prise de contrôle ou le sabotage de systèmes informatiques. Dans ce domaine, ce sont très souvent des États qui sont à la manœuvre, ou les opérations utilisent des proxys situés de manière privilégiée dans certains États.

C'est ce qui s'est passé lors de l'affaire Sandworm : des attaques informatiques organisées en Russie ont visé des administrations françaises. J'ai alors rencontré mon homologue, M. Patrouchev, dans le cadre d'un canal de déconfliction, et je lui ai indiqué que nous avions constaté qu'un service russe nous attaquait. Dans ce genre de situation, en général, l'adversaire répond : « Très bien. Prouvez-le moi. » Or si nous lui fournissons les preuves, il a ainsi le moyen de corriger son système et de ne plus être détecté la fois suivante. L'efficacité de telles démarches est donc limitée.

L'attribution d'une attaque à un pays est complexe, voire risquée : nous annonçons qu'une attaque a eu lieu, dont le mode d'action est imputable, de source ouverte, à tel ou tel pays – en l'occurrence, la Russie, mais la Chine est l'autre acteur principal dans ce domaine. Nous le faisons assez régulièrement, soit de manière autonome, soit en partenariat avec l'Union européenne lorsque plusieurs États membres ont été attaqués, soit en coordination avec les Américains. Il arrive aussi qu'un attaquant utilise par exemple les outils d'APT31, autrement dit un système chinois de cyberattaque bien connu sur le *dark web*. Pour autant, attribuer formellement une attaque à un État est difficile car les faux-semblants sont permanents : un État peut utiliser APT31 pour faire porter le chapeau à Chine, par exemple. Les pièges sont nombreux.

Il y a également les ingérences numériques étrangères que l'on pourrait qualifier de manipulations de l'information. Il s'agit d'« *opérations impliquant […] un État étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, par le biais d'un service de communication au public en ligne, d'allégations ou imputations de faits manifestement inexactes ou trompeuses de nature à nuire aux intérêts fondamentaux de la Nation* », selon les termes du décret pris en Conseil d'État portant création de Viginum. Le Conseil d'État et la Commission nationale de l'informatique et des libertés (CNIL) ont veillé à ce que le dispositif soit précis et n'attente pas aux libertés individuelles. Nous avons bénéficié d'un précieux éclairage du Conseil d'État : celui-ci a considéré qu'au regard de l'objectif constitutionnel de sincérité de l'information délivrée à nos concitoyens, Viginum avait la possibilité d'accéder à certaines données, de manière à vérifier que les internautes français dialoguaient sur les réseaux sociaux avec de vrais internautes et non avec une ferme à trolls située dans une banlieue de Saint-Pétersbourg ou avec des robots se contentant de relayer des informations produites ici ou là.

Dans ce domaine, l'attribution est souvent facile, grâce au travail effectué par Viginum. Elle est également nécessaire, non pas pour dénoncer le fait que tel pays ou telle entité s'est livré à de la désinformation, mais pour expliquer à nos concitoyens qu'ils se sont fait manipuler, qu'on leur a mis dans la tête des idées conformes à ce qu'un dirigeant ou une organisation étrangers souhaitaient qu'ils pensent alors même qu'ils croyaient participer à un débat serein et authentique. Il est très important pour nous de donner à nos concitoyens, sous une forme pédagogique, les éléments d'information leur permettant de juger. À cet égard, les aveux de M. Prigojine concernant sa fameuse ferme à trolls de Saint-Pétersbourg, ou des articles comme ceux que *Le Monde* a publiés aujourd'hui sur une entreprise israélienne spécialisée dans les manipulations des réseaux sociaux sont très utiles : ils permettent de

démontrer qu'une machinerie est à l'œuvre, à l'étranger, dont l'objectif est de nuire à nos intérêts, à la sincérité des débats et, potentiellement, à celle des scrutins.

Le troisième type de menace hybride concerne les atteintes à notre patrimoine scientifique et technique, les tentatives de capter nos savoir-faire dans les entreprises les plus sensibles pour notre souveraineté économique. Cela passe par l'espionnage, le sabotage, la prise de contrôle capitalistique, ou encore le débauchage de talents. Ces manœuvres peuvent être précédées par le démontage réputationnel de l'entreprise à travers des attaques informationnelles. C'est un enjeu auquel nous sommes très sensibles. Chaque année, avec la direction générale des entreprises (DGE) du ministère de l'économie et des finances, nous examinons plusieurs centaines de dossiers concernant ce que l'on appelle des « pépites industrielles », nécessaires à notre économie, faisant l'objet d'attaques ou de tentatives de prédation. Des interdictions d'exportation ou de vente d'une entreprise à un État étranger sont parfois décidées. Il arrive également que Bpifrance et des fonds amis en prennent le contrôle.

Le *lawfare* est une quatrième forme de menace hybride et d'ingérence étrangère. Il s'agit de l'utilisation du droit international ou de l'application extraterritoriale du droit d'un État. Cela passe aussi par l'imposition de normes internationales telles que des taxonomies, par du lobbying ou par la judiciarisation de certaines activités économiques et sociales à l'international. Le fait pour un État étranger d'engager des poursuites contre le dirigeant d'une entreprise au motif qu'il a vendu du matériel à tel ou tel pays, qui vise ainsi à neutraliser ce dirigeant ou à limiter l'activité de son entreprise, constitue une ingérence étrangère et une manière de porter atteinte à nos intérêts fondamentaux.

Quand une réglementation comme l'*International Traffic in Arms Regulations* (ITAR) permet aux autorités d'un État, dès lors qu'un produit vendu dans un autre pays contient un composant fabriqué sur son sol, de vérifier si la vente est conforme aux règles qu'il a édictées, il peut s'agir d'une forme d'ingérence, selon la façon dont c'est appliqué. C'est ce que font les Américains depuis plusieurs années, mais aussi les Chinois : ceux-ci ont copié, dans l'esprit, le *Patriot act* américain et, profitant de leur puissance économique, essaient de s'ingérer dans les économies étrangères. Dans ce contexte également, nous sommes amenés à travailler avec la DGE. Des discussions sont engagées avec l'État concerné. Lorsque les Américains ont des questions à poser aux entreprises, ils passent dorénavant par le SGDSN, avec l'appui de la DGE. Nous vérifions que ces questions sont en rapport avec l'activité de l'entreprise et évaluons l'intérêt de cette dernière. Si nous considérons que certaines de ces questions sont intrusives, qu'elles visent à connaître des secrets de fabrication, nous expliquons à nos amis américains que nous ne jugeons pas la démarche nécessaire à la manifestation de la vérité et nous la bloquons. C'est beaucoup plus compliqué avec les Chinois. Quoi qu'il en soit, nous essayons de progresser dans ce domaine pour contrer les attaques.

Il faut également protéger nos normes face à la *common law*. Cela suppose d'agir à l'échelon européen, sous peine de nous trouver isolés. Nous nous battons aussi, à travers les normes de l'Organisation internationale pour la normalisation (ISO), pour que soient fixées des règles qui ne soient pas uniquement favorables à des intérêts étrangers. Plus encore peut-être que les entraves aux autres formes d'ingérence, celles opposées au *lawfare* sont fondamentales : à terme, l'utilisation du droit pour prendre insidieusement le contrôle dans un autre pays, imposer ses propres normes et ses procédures judiciaires, apparaît comme la menace la plus sérieuse.

Au sein du SGDSN, la protection du patrimoine scientifique et technique et la lutte contre le *lawfare* sont traitées dans des directions qui existent depuis longtemps. Nous disposons de plusieurs autres services, dont certains de création plus récente, qui nous permettent de travailler sur l'ensemble des enjeux liés à la protection. Par exemple, dans le cadre de la procédure d'habilitation au secret de la défense nationale, nous menons des enquêtes pour nous assurer que les personnes concernées ne risquent pas d'être soumises à des pressions. Nous veillons à ce que certains dossiers soient classifiés, afin qu'ils ne soient pas dévoilés à d'autres États. Nous veillons aussi à provoquer, dans les collectivités locales et dans les entreprises, une nécessaire prise de conscience : les uns et les autres doivent comprendre que nous ne vivons pas dans un monde sympathique, où chacun respecte les règles du jeu. Certains essaient d'abuser de leur absence de méfiance et de précautions…

Même si nous avons deux services opérationnels, l'ANSSI et Viginum, nous ne sommes pas un service de renseignement. Comme toute administration, nous devons rendre des comptes au Parlement, en toute transparence, sur l'ensemble des éléments que nous traitons, même si certains sont classifiés.

Je n'entrerai pas dans le détail des textes législatifs et réglementaires, mais répondrai à vos questions éventuelles sur cet aspect. Nous œuvrons, chaque fois que c'est nécessaire, à l'élaboration de législations protectrices, notamment à destination des fonctionnaires. La loi Sapin 2, la circulaire du Premier ministre du 11 octobre 2021 et le code pénal permettent de contrer les attaques et de poursuivre les personnes coupables de tentatives d'ingérence. Nous essayons également d'encadrer les activités de lobbying. La loi Sapin 2 vise celles qui revêtent une nature professionnelle. Les autres posent problème : certaines personnes sont instrumentalisées dans le but de se livrer à ces activités. Peut-être faudrait-il faire évoluer le droit pour les prendre en compte et parvenir à plus de transparence, par exemple en confiant cette mission à la Haute Autorité pour la transparence de la vie publique (HATVP). Sur ce point également nous pourrons répondre à vos questions.

Les dispositions inscrites dans le code pénal sont assez peu utilisées en pratique par les magistrats, peut-être parce qu'elles sont très inspirées du temps de guerre et semblent moins pertinentes depuis la fin de la Guerre froide. Il n'en demeure pas moins que des sanctions sont prévues ; elles sont même sévères. S'agissant de la trahison ou de l'intelligence avec une puissance étrangère, dans la mesure où leur répression est devenue assez théorique, peut-être faudra-t-il réfléchir au quantum de peine, à la nature de l'incrimination ou encore aux conditions dans lesquelles les personnes concernées peuvent être mises en cause.

M. Vincent Strubel, directeur de l'Agence nationale de la sécurité des services d'information. L'ANSSI, placée sous l'autorité du SGDSN, joue le rôle de chef de file dans le dispositif national de cybersécurité – car nous ne sommes pas les seuls à nous occuper de ces questions : il existe des services dédiés au sein du ministère de l'intérieur et du ministère des armées, et chaque ministère assure sa propre protection. L'ANSSI collabore avec ces services et nous nous efforçons tous de mener des politiques cohérentes.

L'agence compte environ 600 agents. Son action se décline selon trois grands axes.

Le premier consiste à répondre aux cyberattaques. Il s'agit de les détecter, de les analyser, de chasser l'attaquant lorsqu'il est toujours présent et, le cas échéant, de passer la main à la justice, à qui il revient de réprimer les crimes. Nous exerçons cette mission en liaison étroite avec l'ensemble des acteurs concernés et pertinents pour le sujet, à savoir les services de renseignements, qui ont des éléments complémentaires à apporter, et la justice.

Nous collaborons dans un cadre clair et qui fonctionne bien : le centre de coordination des crises cyber (C4).

Le deuxième axe consiste à sécuriser l'État. Nous veillons à ce qu'il ne soit pas une victime facile. Certes, la sécurité absolue n'est qu'une chimère, mais nous nous efforçons de relever globalement le niveau de sécurité de l'État, de ses opérateurs et de ses établissements, en coordination étroite avec l'ensemble des ministères : chacun d'entre eux est responsable de son système informatique, donc de sa sécurité, mais nous partageons des exigences, ainsi que des indicateurs permettant de mesurer les menaces, et nous rendons compte des progrès réalisés à nos autorités politiques respectives.

Le troisième axe est plus difficile à définir. Pour simplifier, il s'agit de protéger nos concitoyens – non seulement les individus, mais également les entreprises et les associations, car l'ensemble du tissu économique et social fait l'objet de cyberattaques. Nous déployons un éventail de mesures très large, commençant par la formation. Dès le collège, il est important de sensibiliser les futurs citoyens à ces enjeux. C'est d'ailleurs l'occasion de leur parler des carrières dans le domaine de la cybersécurité, car nous cherchons toujours des personnels qualifiés. Nous participons également à l'organisation de la réponse aux attaques dans les services de proximité, y compris la gendarmerie et la police, et au déploiement de mesures de sécurité parmi les opérateurs économiques et dans le tissu associatif.

On ne cesse de répéter que la menace va crescendo ; c'est une réalité. Elle se matérialise dans trois principaux types d'attaque auxquelles nous faisons face.

La première catégorie, la plus visible et la plus importante – en quantité, mais peut-être pas pour ce qui est de son impact –, est celle que l'on désigne par le vocable de « cybercriminalité ». Il s'agit des activités criminelles ayant, pour l'essentiel, une visée lucrative. Il est beaucoup question de rançongiciels, qui paralysent des systèmes et proposent de les débloquer en échange d'une rançon, mais d'autres pratiques entrent dans cette catégorie, telles que l'extorsion de données, l'exigence de rançons en échange de la non-publication de données, ou encore les activités visant à détourner des systèmes pour produire de la crypto-monnaie. En amont et en aval de ces activités criminelles, un écosystème s'est constitué. L'objectif de ces activités est de produire de l'argent, au profit de groupes appartenant au monde du crime organisé même si la frontière avec d'autres types d'acteurs est parfois floue.

Les auteurs de ces attaques ne ciblent personne en particulier : ils pratiquent une sorte de pêche au chalut. C'est ce qui vaut à nos hôpitaux d'en être régulièrement victimes, avec des conséquences parfois graves et particulièrement abjectes, quand bien même les règles de la comptabilité publique interdisent de verser la moindre rançon – ce que les criminels commencent à comprendre, me semble-t-il. Les PME et les collectivités sont également des cibles récurrentes. En général, ce sont les entités les plus vulnérables qui se font prendre au piège. De grandes entreprises ont été victimes de ces pratiques il y a quelques années, mais elles ont relevé leur niveau de sécurité pour s'en prémunir.

Dans la deuxième catégorie de menaces, nous plaçons celles qui relèvent de l'espionnage. On en parle peu, puisque, par construction, l'attaquant cherche à rester discret, et nous le sommes également quand nous traitons ce type d'affaire, mais ce sont elles qui mobilisent l'essentiel de notre activité de réponse à des incidents, car il s'agit d'opérations longues, très complexes, touchant l'ensemble des entreprises stratégiques ainsi que l'État.

Nous découvrons des attaquants qui, graduellement, récupèrent des secrets ou des informations sensibles, parfois depuis des mois, voire des années.

La troisième catégorie rassemble les actes de « sabotage » – mais, là encore, c'est un raccourci de langage – ou de « déstabilisation stratégique ». Comme l'espionnage, ces menaces sont en général le fait d'États. Elles visent à perturber le fonctionnement d'infrastructures stratégiques, ou bien, ce qui est encore plus pernicieux, à se mettre en position de le faire le moment venu. Nous en avons eu un exemple très récemment, au début de l'affrontement russo-ukrainien, avec la paralysie du service KA-SAT, une infrastructure de communications par satellite opérée par Viasat. Cette opération de sabotage a eu des conséquences sur le territoire ukrainien, mais aussi bien au-delà : elle a largement débordé sur le territoire français. Nous observons également un autre cas de figure : certaines personnes prennent la main sur des systèmes d'information et s'y installent très discrètement, sans récupérer d'informations à la différence des espions. Nous supposons qu'elles attendent l'ordre de tout détruire – perspective qui nous inquiète tout particulièrement.

L'ANSSI ne nomme ni les victimes ni les attaquants. S'agissant des victimes, si elles choisissent de communiquer ou y sont contraintes par certaines règles juridiques, c'est à elles qu'il appartient de le faire ; en général, le nom d'une victime est pour l'ANSSI une information classifiée. En ce qui concerne l'attaquant, nous identifions un mode opératoire le désignant, mais nous ne spéculons pas sur son identité. Il revient à la justice de dire de qui il s'agit – lorsque l'affaire est judiciarisée –, avec le niveau d'exigence qui lui est propre en matière de preuves. Cela peut également relever d'une décision des autorités politiques, lesquelles choisissent parfois, notamment quand l'auteur des faits est un autre État, d'actionner des leviers, diplomatiques ou autres, pour lui signifier notre courroux justifié.

L'ANSSI se borne à désigner des modes opératoires, parfois au moyen de phrases alambiquées qui reflètent cette réalité fondamentale : nos connaissances techniques ne nous permettent pas de savoir de qui émane l'attaque, et nous ne cherchons pas à identifier des individus, ni même des États.

M. Gabriel Ferriol, chef du service de vigilance et de protection contre les ingérences numériques étrangères. Viginum travaille sur une autre catégorie de menaces : les manipulations de l'information. Il s'agit d'un ensemble de techniques et de modes opératoires visant à altérer les perceptions collectives et l'accès à l'information, dans le but, *in fine*, d'orienter le comportement. Les objectifs visés par les personnes se livrant à ces activités sont, pour l'essentiel, d'éroder la confiance du public dans les institutions, de polariser des débats d'intérêt général, de créer ou d'amplifier des tensions au sein de la société. C'est une catégorie de menaces particulièrement sensible pour une démocratie, dont le bon fonctionnement repose sur le débat public.

Parmi les phénomènes divers relevant de la manipulation de l'information, Viginum est chargé d'identifier et de caractériser les ingérences numériques étrangères. Nous nous fondons sur quatre critères juridiques précis : l'atteinte potentielle à nos intérêts fondamentaux ; l'implication d'un acteur étranger – ce qui ne veut pas dire que l'on attribue une origine à l'attaque –; un contenu manifestement inexact ou trompeur, c'est-à-dire « *dont il est possible de démontrer la fausseté de façon objective* », selon les termes de la jurisprudence du Conseil constitutionnel ; une « *diffusion artificielle ou automatisée, massive et délibérée* », ou la volonté d'une telle diffusion.

Pour exercer cette mission, nous observons les réseaux sociaux et essayons de détecter des situations potentiellement inauthentiques. Nous examinons les comptes impliqués dans le débat public numérique en nous demandant s'ils appartiennent vraiment à des personnes physiques. Nous visons les contenus touchant à nos intérêts fondamentaux qui peuvent apparaître comme inexacts ou trompeurs et, par là même, traduire une manipulation de l'information. Enfin, nous essayons d'identifier les comportements anormaux, c'est-à-dire coordonnés ou aberrants. Nous visons par exemple des comptes qui ne dorment jamais, qui réagissent de façon systématique à d'autres comptes, qui s'organisent pour faire des signalements en essaim ou mettre en avant le même narratif au même moment sous diverses formes.

Nous nommons ces phénomènes « manœuvres informationnelles ». Quand nous identifions une situation de ce type, nous produisons un « relevé de détection ». Pour celles qui présentent des risques, nous entrons dans une phase d'investigation approfondie qui s'appelle la « caractérisation », pendant laquelle nous confrontons ce phénomène potentiellement anormal aux quatre critères que j'ai énoncés. C'est un travail à la fois technique et juridique.

Viginum assiste par ailleurs le SGDSN dans l'animation de la politique publique de lutte contre les manipulations de l'information, dans laquelle de nombreux ministères sont impliqués.

Dans le contexte d'élections nationales, nous avons également un rôle d'assistance des autorités garantes du bon déroulement des scrutins, notamment le Conseil constitutionnel et l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom).

Enfin, nous animons la coopération avec nos homologues étrangers.

Viginum est un service d'investigation, pas de police ou de renseignement. Notre objectif est l'observation et la description des phénomènes, mais nous ne menons pas d'actions répressives. Nous ne prononçons pas de sanctions ; nous ne déférons personne devant les tribunaux. Nous travaillons uniquement avec des contenus ou des données publiquement accessibles, c'est-à-dire que tout un chacun peut observer dans le débat public numérique, sans interagir avec les participants. Les agents de Viginum ne manipulent pas d'avatars, ne rejoignent pas de groupes fermés, ne postent jamais de messages : nous restons dans une posture d'observation. Nous n'accédons pas non plus aux conversations privées.

En tant que service technique et opérationnel, Viginum a pour rôle de produire des analyses qui guident les pouvoirs publics dans les mesures de contre-influence ou de contre-ingérence qui doivent être prises. Si nous apportons notre appui à la mise en place de ces actions, à aucun moment nous n'y participons nous-mêmes : ce sont d'autres administrations qui les mènent.

L'action de Viginum est suivie par un comité éthique et scientifique, placé auprès du secrétaire général, qui a accès à l'ensemble de notre production, notamment les fiches de traçabilité et les documents relatifs aux collectes automatisées que nous réalisons. Le comité peut formuler des recommandations et il rend chaque année un rapport – celui concernant l'année 2022 ne devrait pas tarder à sortir.

M. le président Jean-Philippe Tanguy. Pourriez-vous préciser les quatre critères définissant l'ingérence ?

M. Gabriel Ferriol. Le premier critère caractérisant une ingérence numérique étrangère est le suivant : le phénomène est susceptible de porter atteinte aux intérêts fondamentaux de la nation, notion juridique particulièrement importante, notamment dans le domaine régalien. Elle est définie à l'article 410-1 du code pénal et sous-tend le dispositif d'autorisation des techniques de renseignement prévu par l'article 811-3 du code de la sécurité intérieure.

Deuxièmement, nous devons démontrer qu'un acteur étranger au moins est impliqué dans le phénomène – étant entendu, une fois encore, qu'implication n'est pas synonyme d'origine.

Troisièmement, il s'agit de contenus « *dont le caractère inexact ou trompeur est manifeste* » et « *dont il est possible de démontrer la fausseté de manière objective* », selon les termes de la décision du Conseil constitutionnel du 20 décembre 2018 sur la loi relative à la lutte contre les manipulations de l'information.

Enfin, le contenu est caractérisé par une diffusion artificielle ou automatisée, massive et délibérée – ou l'intention de procéder à une telle diffusion : le décret fondant Viginum vise à la fois la tentative et la réalisation. Ce critère est important, car l'intérêt d'un outil comme Viginum est précisément de se placer autant que possible en anticipation de ces phénomènes : il ne s'agit pas seulement de réagir.

M. Stéphane Bouillon. Pour prendre l'image des feux de forêt, que chacun connaît, et comparer une attaque en manipulation de l'information à de tels incendies, notre travail est de repérer les mises à feu avant qu'elles ne se propagent hors de contrôle.

M. le président Jean-Philippe Tanguy. Pouvez-vous nous faire un état des lieux des menaces, des tentatives et des cas avérés d'ingérence au cours des élections présidentielle et législatives de 2022 et de l'élection présidentielle de 2017 ? D'où venaient ces attaques ? Qui ciblaient-elles ? Quelle a été leur ampleur ?

M. Stéphane Bouillon. Le fait essentiel, en 2017, a été ce que l'on a appelé les « *Macron Leaks* » : une pénétration sur les réseaux du candidat Macron qui a donné lieu à la perception, à la déformation, au triturage, puis au lâcher d'informations à un moment où il aurait été très difficile, pour le candidat, de réagir. Viginum n'existait pas à l'époque et c'est l'ANSSI qui a géré ce dossier. Le prédécesseur de Vincent Strubel, Guillaume Poupard, qui suivait les aspects de cybersécurité de la campagne, ayant constaté que le candidat Macron avait fait l'objet d'attaques, a prévenu le Conseil constitutionnel. Celui-ci a décidé de faire interdire la diffusion de ces informations et de bloquer les réseaux sociaux sur ce sujet, de façon à garantir la sincérité du scrutin.

Nous avons fait en sorte que Viginum soit opérationnel avant la campagne présidentielle de 2022 et nous nous sommes mis à la disposition du juge constitutionnel, de la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP) et de l'Arcom. Au cours de la campagne, nous leur avons rendu compte quotidiennement de toutes nos productions. Tous les soirs, un motard allait leur porter les productions de Viginum ou les informations que l'ANSSI avait obtenues. Le principe, c'était que nous étions aux ordres de ces autorités et que nous ne faisions rien de ces informations sans leur autorisation.

Au début de la campagne, en octobre 2021 et en janvier 2022, nous avons organisé deux réunions au SGDSN, auxquelles nous avons convié tous les candidats déclarés ou susceptibles de se déclarer. Il s'agissait de présenter notre travail aux représentants des équipes de campagne et de les mettre en garde contre les menaces qui pouvaient exister en matière de cyber, de manipulation de l'information et d'espionnage. Nous leur avons expliqué que des États étrangers pouvaient voir en eux un « investissement pour le futur » et faire sortir, lorsqu'ils seraient aux affaires, des informations compromettantes. Nous nous sommes mis à la disposition de l'ensemble des candidats et leur avons également donné le nom de sociétés privées susceptibles de faire le même travail que nous, s'ils préféraient ne pas dépendre de la puissance publique.

M. Vincent Strubel. Dans le cadre de la campagne, l'ANSSI a surtout veillé à sécuriser les systèmes de l'État, en particulier les systèmes d'information liés de près ou de loin à l'organisation du scrutin : gestion des listes d'émargement, remontée des résultats, gestion des procurations, etc. Comme l'a expliqué le secrétaire général, elle a œuvré à la sensibilisation des candidats mais aussi à celle des communes, qui étaient en première ligne, et à celle des médias, qui peuvent également être des cibles en période électorale.

En 2017, la gestion des MacronLeaks a été d'autant plus facile que cela s'est produit dans les deux jours précédant le scrutin. Le Conseil constitutionnel a rappelé qu'il n'était plus temps de discuter de tout cela et les médias ont joué le jeu ; ils ont pris leurs responsabilités. En 2022, nous n'avons rien noté de significatif, seulement des épiphénomènes, des tentatives d'attaque contre certains sites internet dont il est difficile de savoir si elles étaient ciblées. Certains médias, notamment de presse écrite, nous ont informés de tentatives d'attaque dites « en déni de service » : c'est l'attaque la plus basique, puisqu'il s'agit de saturer un site internet en lui envoyant un très grand nombre de requêtes pour qu'il ne soit plus accessible. Ces attaques ont été d'une importance mineure : les protections de ces médias en ligne devaient être suffisantes et aucune coupure d'accès ne s'est produite. Ces faits ont été remontés au Conseil constitutionnel, qui a estimé qu'ils n'avaient pas eu un impact significatif sur la campagne électorale, ni sur le scrutin.

M. Gabriel Ferriol. En période électorale, les ingérences numériques étrangères peuvent avoir quatre types de cible. Les premières sont évidemment les candidatures elles-mêmes : des acteurs souhaitant s'ingérer dans le processus électoral mènent des campagnes de dénigrement ou de promotion de certains candidats. Ces deux types d'attaque ne sont pas exclusifs l'un de l'autre : une candidature peut faire l'objet à la fois du soutien d'un acteur malveillant et du dénigrement d'un autre. Il arrive ensuite que les attaques visent les thèmes de campagne : les résultats du vote ne seront pas les mêmes selon que la campagne porte sur des sujets sociaux ou économiques. Les thèmes de campagne peuvent eux-mêmes faire l'objet d'une manipulation de l'information. Les médias traditionnels constituent le troisième type de cible. Enfin, ces attaques peuvent viser les institutions et le processus électoral lui-même : on a observé des cas de manipulation de l'information visant à décourager certaines parties de la population de voter au prétexte que la procédure électorale serait biaisée ou inopérante, ou que l'élection serait volée. Il fallait sécuriser la procédure de vote elle-même.

Tous les modes opératoires classiques peuvent s'observer : contrefaçon de contenus concernant les informations électorales ou les institutions ; usurpation d'identité pour prêter à une personnalité publique des propos qu'elle n'aurait pas tenus et essayer de la discréditer ; amplification de narratifs pour accroître ou modifier la visibilité de certaines idées dans le débat public numérique. Certains modes opératoires combinent une dimension cyber et une dimension informationnelle : ce fut le cas des *Macron Leaks* en 2017.

Viginum s'était organisé pour assurer le bon déroulement de l'élection de 2022. C'était un moment important pour la vie de ce jeune service ; sept équipes spécialisées étaient chargées de protéger les candidatures et les thèmes de campagne, avec le soutien de nos statisticiens, de nos mathématiciens et de notre laboratoire de données. Nous avions également noué des contacts avec d'autres administrations au sein de la gouvernance interministérielle de la politique publique de lutte contre les manipulations de l'information. Nous avions des liens avec l'Arcom et la CNCCEP. Nous avions aussi des contacts plus informels avec la sphère académique et celle des *fact checkers*.

Au total, au cours des campagnes présidentielle et législative de 2022, nous avons détecté soixante phénomènes potentiellement inauthentiques ; douze ont donné lieu à une investigation approfondie et fait l'objet d'une note de caractérisation, pour voir s'ils répondaient aux quatre critères de définition de l'ingérence numérique étrangère ; ce fut le cas pour cinq d'entre eux. On a appelé « Beth » celui qui nous a paru le plus préoccupant. Nous avons communiqué dessus après avoir reçu mandat du Comité opérationnel de lutte contre les manipulations de l'information (COLMI) pour ce faire.

Qu'est-ce que le phénomène Beth ? Un candidat a fait l'objet d'une promotion très emphatique pendant plusieurs mois de la campagne. Quelques jours avant le vote, des médias alternatifs ont révélé qu'il aurait bénéficié du soutien de fermes à trolls. Telle qu'on l'a interprétée, la manœuvre visait à jeter le discrédit sur ce candidat, et plus largement sur la procédure de vote en France. C'est un phénomène que l'on a analysé, dont on a informé les plateformes, et sur lequel on a communiqué.

M. Stéphane Bouillon. Un certain nombre d'entreprises installées en Afrique, notamment au Mali et au Sénégal, ont commencé, par l'intermédiaire de fermes à trolls, à faire la promotion du candidat Macron en reprenant une partie de sa propagande, en changeant les photos et en aménageant les textes. Leur but était double : pouvoir dire, juste avant le scrutin, que le président sortant utilisait des manœuvres de manipulation de l'information pour se faire réélire ; et, deuxièmement, prétendre qu'il utilisait les Africains dans une posture néocolonialiste. Il est apparu que les entreprises qui avaient fait ce travail avaient été stipendiées par la galaxie Wagner, qui faisait ainsi un coup double : mettre en cause la légitimité de la campagne menée par le candidat et délégitimer l'action de la France en Afrique.

Nous avons rendu compte de ce phénomène au Conseil constitutionnel, qui a considéré qu'il n'avait pas eu d'impact sur la sincérité du scrutin. Depuis, nous continuons de noter des attaques venues d'Afrique, de la part de certaines de ces entreprises, qui ont changé de nom. C'est l'un des modes d'action de la société Wagner, qui est très active dans la guerre en Ukraine. Son fondateur, M. Prigojine, a créé une ferme à trolls dans la banlieue de Saint-Pétersbourg, l'*Internet Research Agency* (IRA). Il est également très actif dans bon nombre de pays africains où il essaie de nuire à ce que nous sommes et à notre présence.

Durant la campagne de 2022, une attaque est aussi venue des États-Unis. On a commencé à lire que la société canadienne Dominion, qui fournit les machines à voter aux États-Unis, avait aussi fourni à la France son système de vote électronique. L'argumentation était la suivante : en faisant appel à Dominion, nous truquions les élections, puisque l'élection avait été truquée aux États-Unis. Le ministre de l'intérieur a dû rappeler qu'aucune machine Dominion n'était utilisée en France et qu'il y avait, en outre, une étanchéité entre les systèmes électoraux fonctionnant dans les communes et le système qui permettait de transmettre les résultats depuis les préfectures vers le réseau central. Un problème constaté dans une

commune ne risquait donc pas de remettre en cause l'ensemble du système. Nous avions prévu, en cas de dysfonctionnement électronique, d'utiliser des méthodes qui ont fait leur preuve par le passé : papier, téléphone et calculatrices.

M. Gabriel Ferriol. J'ajoute que tout cela s'est fait sous le contrôle du comité éthique et scientifique.

M. le président Jean-Philippe Tanguy. Les cinq phénomènes que vous avez relevés ont-ils tous touché d'autres partis politiques ? Ou bien seuls le candidat Macron et nos institutions, à travers le système de vote, ont-ils été visés ?

M. Stéphane Bouillon. Des attaques ont touché d'autres candidats, mais elles ont eu un moindre impact et une moindre efficacité que le phénomène Beth. Nous les avons recensées et les avons également signalées au Conseil constitutionnel.

M. le président Jean-Philippe Tanguy. Peut-être ma perception n'est-elle pas la bonne – et je ne voudrais pas que ma question vous semble provocatrice –, mais soixante phénomènes identifiés et cinq attaques avérées, n'est-ce pas finalement assez peu pour une élection présidentielle ? Est-ce parce qu'il y a eu peu de tentatives, ou bien parce que le système français nous protège correctement ?

M. Stéphane Bouillon. Je serai humble : je pense qu'il y a eu beaucoup de tentatives, qu'on en a vu un nombre considérable, mais que beaucoup aussi nous ont échappé, tout simplement parce qu'elles n'ont pas été efficaces et n'ont pas prospéré. J'ai utilisé tout à l'heure l'image du feu de forêt : on voit la forêt qui commence à brûler, mais pas forcément tous les incendiaires avec leur boîte d'allumettes. Peut-être aussi la dissuasion a-t-elle fonctionné : nous avions publiquement indiqué que Viginum et l'ANSSI seraient sur le pont.

Au moment des élections fédérales allemandes, à l'automne 2021, nous avons travaillé avec nos voisins et observé les manipulations d'information qu'ils ont eu à subir. Ils ont fait face à quelques attaques, notamment certaines, assez dures, qui ciblaient la candidate écologiste. Mais, globalement, il y a eu moins d'attaques que ce que l'on pouvait craindre, compte tenu de la présence de fortes communautés étrangères en Allemagne, potentiellement soumises à l'influence de leur pays d'origine.

M. le président Jean-Philippe Tanguy. En 2022, j'étais directeur de campagne adjoint de Marine Le Pen. Les comptes Twitter de plusieurs dirigeants de la campagne du Rassemblement national ont connu un dysfonctionnement. Il ne s'est peut-être agi que d'un bug informatique et pas d'une attaque, mais Christophe Bay, à l'époque, en a informé vos services. Nos comptes ont été rétablis, mais nous n'avons jamais su ce qui était arrivé. Savez-vous ce qu'il en est ? Est-il possible qu'il se soit agi d'une attaque étrangère ?

M. Stéphane Bouillon. M. Bay m'avait effectivement alerté. J'ai prévenu l'Arcom, qui s'est saisie de cette question. Je n'ai pas eu de précision à l'issue.

M. le président Jean-Philippe Tanguy. D'une manière générale, est-ce que les réseaux sociaux, notamment les réseaux américains, qui sont très utilisés en France, coopèrent avec vous dans la lutte contre ces attaques ? Je sais que Twitter communique très mal avec la police et la justice ; c'est en tout cas ce que j'ai constaté par le passé et je ne sais pas ce que son rachat par Elon Musk va changer. Les réseaux sociaux coopèrent-ils ? Pour vous, sont-ils un problème ou, au contraire, une partie de la solution ?

M. Gabriel Ferriol. Les plateformes sont un acteur essentiel de la lutte contre les manipulations de l'information, d'abord parce qu'elles ont accès à beaucoup d'informations utiles que, pour notre part, nous ne pouvons pas forcément observer. Ensuite parce qu'elles disposent en outre d'un certain nombre de leviers pour lutter contre les manipulations de l'information : elles peuvent bannir des comptes ou suspendre des contenus ; elles peuvent aussi faire ce que l'on appelle du *shadow banning*, c'est-à-dire rendre un utilisateur moins visible dans les résultats de recherche ; elles peuvent enfin décider de la démonétisation d'un compte.

Les plateformes sont-elles un problème ou une solution ? Il est difficile de les prendre en bloc : il y en a de différentes sortes et toutes ne sont pas aussi enclines à travailler avec nous. Certaines y sont réticentes pour des raisons de moyens, mais il y en a aussi qui, par principe, ne souhaitent pas participer à la lutte contre la manipulation de l'information et qui utilisent même cet argument pour fédérer leur communauté. Certaines font valoir qu'accorder quelque chose à un pays, c'est prendre le risque qu'un autre pays demande la même chose.

Pendant la campagne présidentielle, nous avons eu des contacts avec la plupart des grandes plateformes et leur avons adressé deux demandes. La première était de nature opérationnelle : nous leur avons demandé de nous signaler ce qui pouvait ressembler à des ingérences numériques étrangères et de lever les doutes que nous pouvions avoir au sujet de certains comptes ou de certaines activités qui nous paraissaient inauthentiques. Les plateformes ont des équipes d'investigation en interne dont l'avis peut parfois nous être utile – ce fut le cas pour le phénomène Beth. Notre deuxième demande était plus technique et pratico-pratique : nous voulions nous assurer que les comptes d'accès que nous utilisions pour observer les plateformes ne feraient pas eux-mêmes l'objet de mesures de bannissement. Dans l'ensemble, ces échanges ont été fructueux, même si les plateformes ne nous ont pas spontanément signalé de phénomènes. Nous avons des contacts réguliers avec elles sur les phénomènes qu'elles signalent dans leur rapport. Nous dialoguons avec elles ; ce dialogue repose sur la bonne volonté des uns et des autres.

M. le président Jean-Philippe Tanguy. Pour des raisons organisationnelles que l'on peut comprendre, et du fait de la massification des données et des phénomènes, l'État français, comme d'autres États occidentaux, délègue la modération des contenus aux plateformes. Cela pose plusieurs questions, à commencer par celle des moyens que ces plateformes consacrent effectivement à la modération : qu'est-ce qui relève de l'être humain et qu'est-ce qui relève de l'algorithme ? D'autre part, compte tenu de l'importance des comptes Facebook et Twitter des candidats en période électorale et de la communication que les partis politiques font sur ces plateformes, n'est-il pas problématique que ce soient les plateformes elles-mêmes qui soient chargées d'analyser ces contenus ? N'est-ce pas déjà une forme d'ingérence ? Je pense notamment aux contenus relatifs à la valeur de la laïcité, qui n'a pas tout à fait le même sens dans le monde anglo-saxon.

Je ne mets évidemment pas sur le même plan l'ingérence culturelle anglo-saxonne et celle d'un pays hostile. Je constate seulement que lorsque nous publions des contenus relatifs à la laïcité – et cela vaut pour tous le partis politiques –, il arrive qu'ils soient censurés, particulièrement ceux qui concernent le voile ou l'islamisme, au nom d'une interprétation culturelle anglo-saxonne. La question se pose aussi pour d'autres phénomènes culturels comme le wokisme. Imaginons que celui-ci prenne de l'ampleur d'ici à la prochaine élection ; imaginons que des revendications islamistes modérées prennent de l'ampleur et que l'on voie fleurir les contenus expliquant que refuser l'accès à une salle de sport à une personne voilée ou barbue est une discrimination. Ces questions ne sont pas considérées de la même façon des

deux côtés de l'Atlantique. Est-ce que ce sont des situations auxquelles vous réfléchissez ? Comment les gérerait-on, sachant qu'on a tout à fait le droit, en République française, de considérer sans attenter à nos valeurs constitutionnelles que le voile islamique est un problème pour le droit des femmes ?

M. Stéphane Bouillon. Il me semble que ce n'est pas à l'État, que ce n'est pas au pouvoir exécutif, surtout en période de campagne électorale, d'agir ou de réagir sur ce sujet. C'est avant tout le rôle de la presse, puisque le fondement même de notre démocratie, c'est la possibilité, pour les journaux, de s'exprimer et d'émettre des opinions. Il me paraît essentiel, dans une démocratie, qu'une diversité d'opinions puisse s'exprimer. Cela peut aussi valoir sur les réseaux sociaux à partir du moment où les gens savent à qui ils ont affaire et où les choses sont transparentes : on peut être *woke* ou anti-*woke*, mais il faut savoir de quoi on parle. Quand on lit *Libération* ou *Le Figaro*, on sait à quoi s'en tenir.

Les journaux doivent favoriser l'éducation du public. C'est leur rôle de mener un travail d'investigation et d'explication. La justice, qui est indépendante, doit quant à elle faire appliquer la loi, notamment celle de 1881 sur la presse et celle de 2018 sur la manipulation de l'information. Désormais, l'Arcom a de vrais moyens d'action et elle peut faire pression sur les réseaux sociaux. La loi l'autorise, après une mise en demeure, à saisir le juge des référés et à couper le robinet, à partir du moment où un réseau social dépasse les bornes et contribue à une manipulation d'information manifeste et désordonnée.

Nous avons déjà un certain nombre de remparts et un arsenal juridique ; à vous de voir si les évolutions actuelles imposent de les renforcer. En tout cas, il me semble qu'en période électorale, l'autorité administrative que je représente doit rester en retrait. C'est au personnel politique, sous le contrôle du juge de l'élection, et aux médias, sous le contrôle du juge judiciaire, de veiller à ce que tout se passe bien. Je considère, comme lorsque j'étais préfet et que j'organisais les élections dans mon département, que ma plus-value est de faire en sorte que tout se passe correctement.

Mme Constance Le Grip, rapporteure. Au sujet des ingérences numériques étrangères, il a beaucoup été question de la Russie. D'autres puissances étrangères se sont-elles livrées à des tentatives d'ingérence numérique en France ? Si tel est le cas, ont-elles le même mode opératoire ? Ou bien la Russie est-elle le seul pays à agir de manière aussi massive et organisée ? Après l'assassinat de Samuel Paty, on a vu se développer une campagne antifrançaise très virulente, qui semble être née en Turquie. Pouvez-vous nous en dire plus ?

M. Stéphane Bouillon. Après l'assassinat de Samuel Paty, nous avons effectivement fait l'objet de nombreuses attaques. Pour y faire face, nous avons créé la *task force* Honfleur – du nom d'une salle de réunion du SGDSN –, qui a permis d'identifier un certain nombre de sites et d'adresses IP, de remonter jusqu'à l'agence de presse Anadolu et de conclure à l'origine turque de cette campagne. Elle a pris fin quelques mois après l'attentat, mais nous sommes toujours à l'écoute de ce qui peut venir de Turquie, notamment des critiques sur la politique française au Moyen-Orient, en Afrique ou ailleurs.

Nous sommes également attentifs à ce que fait l'Iran, ainsi que la Chine, même si celle-ci cherche davantage à promouvoir sa propre politique qu'à se mêler de nos affaires. Une partie de l'ultra-droite américaine a également été active à plusieurs reprises pendant la campagne. Le Canada avait connu plusieurs manifestations de camionneurs. Une tentative a eu lieu en France, qui avait été téléguidée depuis les États-Unis et le Canada : cela n'a pas

prospéré. Ceux que l'on appelle les MAGA – pour *Make America Great Again* – ne s'intéressent pas qu'à la politique américaine : ils regardent ce qui se passe ailleurs et sont actifs. Nous avons suivi le site américain Gettr pendant la campagne électorale : il a contribué à lancer l'affaire des machines à voter.

M. Gabriel Ferriol. Certains acteurs ont, de longue date, investi le champ informationnel et même développé une doctrine à ce sujet, qu'ils ont simplement adaptée au numérique. Ils réussissent à produire des effets politiques très puissants – on le voit en Afrique – à des coûts limités. D'autres procèdent à un rattrapage en investissant rapidement ce champ pour rejoindre leurs prédécesseurs. Les premiers venus renoncent à des opérations à large spectre pour cibler des thématiques ou des communautés très étroites afin d'être plus discrets, alors que les nouveaux arrivants lancent plutôt de vastes opérations assez faciles à observer.

La Chine est un cas particulier. Elle a des capacités informationnelles énormes mais qui doivent être comprises avant tout comme la prolongation à l'extérieur des frontières du dispositif instauré à l'intérieur pour contrôler la population. Comme l'a dit le secrétaire général, la doctrine chinoise est d'abord une doctrine de réaction en cas de franchissement de certaines lignes rouges bien définies ; c'est pourquoi, nous avons besoin d'être prépositionnés pour tenir compte de la menace car si la Chine décidait d'agir, les effets seraient massifs.

Mme Constance Le Grip, rapporteure. Les premiers arrivés dont vous parlez, c'est l'État russe ?

M. Gabriel Ferriol. Oui, mais certaines structures para-étatiques russes. Aujourd'hui, la zone de confrontation avec nos compétiteurs stratégiques est principalement l'Afrique.

Mme Constance Le Grip, rapporteure. Depuis l'invasion de l'Ukraine par l'armée russe, on a enregistré, semble-t-il, un nombre record de cyberattaques – on parle de 2 000 – contre l'Ukraine ou contre des intérêts ukrainiens. Observe-t-on depuis la même date un phénomène d'ampleur comparable, ou simplement une hausse du nombre de cyberattaques, visant les intérêts français ou ceux d'autres pays européens soutenant les forces ukrainiennes, et qui soit imputable à la Russie ? J'ai bien entendu que l'ANSSI ne nomme ni les victimes ni les attaquants, mais vous pouvez peut-être apporter une réponse globale.

M. Vincent Strubel. Je ne me risquerai pas à donner des chiffres très précis car les cyberattaques sont encore plus compliquées à compter que les manifestants… Les versions sont nombreuses, selon la définition que l'on retient d'une cyberattaque, la manière de compter, l'origine et le destinataire du signalement.

Voici ce que nous avons très concrètement observé.

Le territoire ukrainien a subi massivement – c'est de l'information de seconde main – des attaques visant à accompagner des manœuvres que les militaires appellent cinétiques : en plus de se taper dessus dans le monde réel, les adversaires l'ont fait dans le monde virtuel. Les Ukrainiens ont fait face, dans une large mesure.

Étonnamment, au premier semestre, le nombre d'attaques de cybercriminalité sur le territoire français – tout au moins de celles dont l'ANSSI a été informée – a baissé. Parmi les facteurs qui, selon notre analyse, y ont contribué figure le fait que plusieurs groupes actifs

dans le domaine de la cybercriminalité ont choisi un camp dans l'affrontement russo-ukrainien et orienté leur action en conséquence, pas nécessairement en Europe occidentale, mais – c'est du moins ce que certains ont annoncé, et nous pensons qu'ils l'ont fait – sur le territoire de l'Ukraine et des pays limitrophes, ou bien sur le territoire russe.

Un groupe de cyber-attaquants appelé Conti qui pratiquait le rançongiciel à très grande échelle a même explosé en vol : la plupart de ses membres ayant annoncé prendre fait et cause pour la Russie, un Ukrainien qui en faisait également partie ne s'est pas aligné sur cette position et en a profité pour laver le linge sale du groupe sur les réseaux publics. Du coup, ce groupe a disparu – il s'est sans doute recomposé ailleurs.

Quoi qu'il en soit, cette petite baisse circonstancielle du nombre de cyberattaques relevant de la cybercriminalité a été suivie d'une reprise au second semestre : l'activité s'est restructurée.

Ainsi, il y a eu énormément d'attaques en sabotage sur le territoire ukrainien. Je mets à part l'attaque contre le système de communications satellitaires Viasat, qui a eu des effets sur tout le territoire européen en détruisant non le satellite, heureusement, mais les moyens de communication avec lui, y compris, dans une large mesure, sur le territoire français. Elle a été attribuée à la Russie par l'ensemble des membres de l'Union européenne. Du reste, son déclenchement dans la nuit du 23 au 24 février 2022 ne laissait guère de doute quant à son origine et sa finalité.

Nos partenaires européens nous ont également signalé des attaques s'apparentant plutôt à de la reconnaissance, destinées à évaluer les faiblesses potentielles de systèmes d'information, notamment dans le domaine de la distribution du gaz. Là encore – sans me risquer à une attribution formelle, d'autant plus que ce sont nos partenaires qui ont observé le phénomène –, le contexte laisse peu de doute.

Enfin, l'espionnage n'a évidemment pas reflué pendant cette période. Cette fois, je me risquerai à un chiffre : en 2022, l'ANSSI a mené dix-neuf opérations – un terme qui correspond à notre niveau d'intervention le plus élevé, engageant nos agents de manière massive pendant des semaines, voire des mois, face à une attaque majeure afin de bien comprendre ce qu'a fait l'attaquant, par où il est entré, comment le faire sortir et comment s'assurer qu'il ne reviendra pas – qui correspondaient quasi exclusivement à de l'espionnage. Et, puisque nous l'avons dit publiquement, je me permets de préciser, sans que cela ait la portée d'une attribution, que neuf de ces attaques relevaient de modes opératoires attribués en source ouverte à la Chine. Autrement dit, d'autres que nous attribuent à l'État chinois ces modes opératoires que nous avons nous-même observés. Cette réalité n'est pas nouvelle et n'a pas changé pendant la crise ukrainienne.

Si les effets du sabotage se sont concentrés sur le théâtre d'opérations, nous n'excluons pas qu'ils en débordent à l'avenir, surtout dès lors que des actions de reconnaissance ont été constatées. Nous sommes donc très vigilants, en particulier pour le secteur de l'énergie.

Mme Constance Le Grip, rapporteure. Quand vous parlez d'espionnage cyber, comment caractérisez-vous l'espionnage ? Par la captation de données, le vol de savoir-faire ?

M. Vincent Strubel. Ce que l'on voit dans ces affaires, c'est le ciblage bien précis d'entreprises stratégiques et de l'État afin de voler des secrets industriels, commerciaux ou

des informations sensibles détenues par l'État, par exemple au sujet de sa posture diplomatique.

On parle en anglais d'*Advanced Persistent Threats* (APT) : des attaquants prennent très discrètement le contrôle du réseau informatique d'une entreprise, s'y installent durablement, s'y étendent largement, puis, de manière très progressive et toujours discrète, font sortir de l'information, et pas n'importe laquelle. Dans une entreprise, ce sont les secrets industriels s'il y en a, les listes de prospects commerciaux, les offres commerciales, bref tout ce qui peut être intéressant dans un contexte stratégique de concurrence économique. La même approche se transpose aisément au niveau de l'État. Il s'agit clairement d'espionnage.

On voit parfois faire cela sans qu'aucune information ne soit exfiltrée. On se dit alors que ceux qui sont venus là ont l'intention d'y rester jusqu'à ce que l'on ait besoin d'eux.

M. Stéphane Bouillon. C'est le principe des chevaux de Troie : on ne sait pas où ils sont, mais un jour, alors que l'on a besoin de tel service public, il ne fonctionne pas. On peut citer l'exemple célèbre d'une ville sur les bords de Loire où l'eau coulait au robinet, mais où ce n'était plus la régie municipale qui contrôlait l'écoulement.

Mme Constance Le Grip, rapporteure. Nous découvrons l'affaire *Story Killers* grâce au consortium Forbidden Stories et au journal *Le Monde*. Quels commentaires appelle-t-elle de votre part ? Y avez-vous appris quelque chose ?

M. Stéphane Bouillon. Je ne connaissais pas la Team Jorge. Mais qu'il y ait, dans un certain nombre de pays, dont Israël, des spécialistes capables de travailler sur tout et n'importe quoi au profit de quiconque les paiera, on s'en doutait. Ils avaient du reste été remarqués – non par nous directement, puisque nous ne nous occupons pas d'actions qui ne sont pas des ingérences numériques étrangères contre la France. Le fait de peser sur l'élection d'un chef d'État en Afrique intéresse en revanche les services de renseignement, que vous pourrez interroger.

Malheureusement, tout cela n'est donc pas une surprise. Comme nous sommes dans le Far West, de plus en plus de gens peuvent gagner beaucoup d'argent dans une relative impunité – jusqu'à un certain point seulement, car les donneurs d'ordre n'aiment pas la publicité lorsque les choses sont découvertes et les autorités réagissent vite. À la suite de l'affaire Pegasus, la société NSO a été interdite aux États-Unis et est en train de couler. Certes, je ne doute pas que le fonds de commerce soit repris, si ce n'est déjà fait. Toujours est-il que certains sont devenus indésirables dans le métier.

M. Gabriel Ferriol. À première lecture, l'enquête du *Monde* paraît très sérieuse et complète. Nous sommes en train de l'analyser en détail car elle est très intéressante pour approfondir notre connaissance des modes opératoires et éclairer notre travail de veille et d'anticipation.

L'affaire m'inspire trois observations.

Premièrement, le secrétaire général pourra en témoigner, à la création de Viginum, il y avait des manifestations de scepticisme quant à la menace informationnelle. Existait-elle vraiment ? Nécessitait-elle de mobiliser des moyens au niveau étatique ? Était-il justifié de lutter contre les ingérences numériques étrangères ? Les enquêtes démontrant l'existence de cette menace sont donc utiles, notamment quand les démocraties sont visées.

Deuxièmement, l'enquête montre la diversité des acteurs impliqués, qui ne sont pas seulement étatiques : il existe une offre d'acteurs privés à but lucratif qui manipulent l'information contre rémunération. Elle a aussi l'intérêt de montrer la conjonction de l'approche cyber et de la manipulation de l'information – très intégrées dans le modèle de l'équipe en question –, qui justifie que l'ANSSI et Viginum collaborent étroitement.

Enfin, on voit que la lutte contre les manipulations de l'information ne concerne pas seulement l'administration : elle nécessite de bâtir un véritable écosystème avec des chercheurs et la presse. De notre point de vue, il est positif qu'un consortium d'une centaine de journalistes travaillant pour une bonne douzaine de médias s'implique dans cette lutte. Et si cela peut produire une prise de conscience, c'est salutaire.

M. Charles Sitzenstuhl (RE). L'ANSSI a mené, je crois, une enquête sur les *Macron Leaks*. Pouvez-vous nous faire part de ses résultats ? Sait-on qui a organisé la diffusion des documents ?

M. Vincent Strubel. Ma réponse ne va pas vous satisfaire, mais l'affaire ayant fait l'objet d'une judiciarisation, il ne nous appartient pas de donner les résultats de l'enquête. L'ANSSI a contribué conformément à son rôle à l'analyse de ce qui s'est passé, mais n'a pas participé plus que d'habitude à l'identification des responsables.

M. Charles Sitzenstuhl (RE). Le jugement est-il rendu ?

M. Vincent Strubel. Dans ce contexte comme dans d'autres, la justice a été saisie, mais je serais bien incapable de vous dire si l'affaire a été jugée.

M. Stéphane Bouillon. Visiblement, l'origine est russe. Je crois d'ailleurs que le président Macron l'a fait remarquer lors de ses premiers entretiens avec le président Poutine. Sans les attribuer directement à quiconque, il a vivement déploré en sa présence que les *Macron Leaks* aient pu se produire, ce qu'il n'a pas fait devant d'autres.

M. Charles Sitzenstuhl (RE). J'aimerais revenir sur l'ingérence physique. Le SGDSN est rattaché à Matignon, ce qui lui donne une vision interministérielle. Je souhaiterais vous entendre au sujet des influences ou ingérences russes touchant les hauts fonctionnaires, particulièrement des officiers de nos forces armées. Je suis parfois étonné d'entendre à la télévision les prises de position de certains officiers retraités ou officiers généraux de la deuxième section ; d'autres s'en sont émus récemment dans la presse. Elles semblent montrer la pénétration, depuis plusieurs années, d'une idéologie pro-russe dans notre appareil d'État, notamment auprès des plus hauts dirigeants de nos armées. Cette menace a-t-elle été suffisamment identifiée ? Des travaux de sensibilisation ont-ils été menés ou vont-ils l'être pour que les personnes visées abordent avec beaucoup plus de précaution la mythologie dont la « nouvelle Russie » fait l'objet ?

M. Stéphane Bouillon. Les généraux et officiers concernés sont tous de deuxième section, c'est-à-dire qu'ils ne sont plus en activité. La question peut effectivement se poser de savoir si, à ce stade, on est totalement libre de sa parole. Peut-être sera-t-elle soulevée lors de l'examen du projet de la loi de programmation militaire ; ce serait intéressant. Elle relève vraiment de la loi. S'agissant de personnels non actifs, la Grande Muette peut-elle commencer à parler ? Jusqu'à quel point, jusqu'à quel niveau ?

On peut également se demander s'il est bien normal que des officiers pilotes puissent, après leur temps de service, louer leurs services pour apprendre à une autre armée à voler sur tel ou tel type d'appareil ou à faire face à tel autre. J'ai tendance à penser que la réponse est non : normalement, le code pénal et le code de justice militaire devraient pouvoir s'appliquer à ce genre de situation. En tout cas, les armées y sont très sensibles et il faut y travailler.

Quant au personnel des armées en activité, des enquêtes de sécurité sont menées par la DRSD (direction du renseignement et de la sécurité de la défense) : l'histoire de chacun, les pays où il s'est rendu et les personnes qu'il fréquente sont très précisément examinés. Pour voir moi-même passer les éléments qui concernent les agents d'autres ministères, je peux vous dire que la DGSI est elle aussi très scrupuleuse, trop au goût de certains : une personne ayant fait un séjour d'études de plusieurs mois dans une université à l'étranger est au moins mise en garde et, en tout état de cause, écartée de certains dossiers. Les mesures prises sont donc très rigoureuses pour les civils comme pour les militaires. Si l'on est simplement soupçonné d'avoir été compromis, par exemple si on a eu une liaison sentimentale avec une personne d'origine étrangère pas très éloignée d'un consulat ou d'une ambassade, on est écarté sans pitié. J'en ai des exemples parmi d'anciens collaborateurs.

Cela étant dit, on peut trouver dans ce milieu, comme dans toute partie de la société, des pro-russes et des anti-russes, et cela fait partie du débat.

La question de la liberté de parole se pose aussi pour les anciens ambassadeurs. Et qu'en est-il des personnes qui ont travaillé très longtemps pour l'État et qui partent dans le privé ou au service d'autres pays ? Il faut être sévère, mais sans nuire à l'attractivité de l'État en interdisant à ceux qui l'auront servi d'avoir ensuite une autre carrière. En outre, tout dépend de la période historique : la Russie étant actuellement en conflit avec l'Ukraine, que nous soutenons, cela nous choque d'entendre tel ou tel contester ce que nous considérons comme la vérité, mais il faut aussi se poser la question à froid. Il y a quelques années, avant l'invasion de l'Ukraine, était-il normal que des responsables diplomatiques, militaires ou de services qui étaient de farouches partisans de Poutine interviennent à ce sujet ? Le législateur aura à mener un travail complexe pour déterminer la juste proportionnalité et l'équilibre adéquat entre liberté d'opinion, liberté individuelle, capacité à expliquer ce qu'on est et défense des intérêts fondamentaux de la nation. Je vous souhaite bon courage !

Mme Constance Le Grip, rapporteure. Peut-être pourrions-nous nous inspirer d'exemples étrangers, de grandes démocraties qui auraient résolu la question.

M. Stéphane Bouillon. Il existe aux États-Unis le dispositif FARA – *Foreign Agents Registration Act*. Nous, nous avons la loi Sapin, suivie d'une circulaire primo-ministérielle d'octobre 2021 rappelant aux fonctionnaires sollicités de façon un peu appuyée par un représentant étranger qu'ils doivent en rendre compte à leur autorité et, le cas échéant, saisir la Haute Autorité pour la transparence de la vie publique. La loi Sapin prévoit également que les lobbyistes professionnels se fassent recenser auprès de la HATVP. La vérité est que cela ne fonctionne pas très bien et que la HATVP n'est pas submergée par les déclarations.

Ce qui pourrait être intéressant, et à quoi nous réfléchissons, en envisageant de nous inspirer des États-Unis, ce serait que les lobbyistes « amateurs » – qui ont une autre profession, mais siègent dans un conseil d'administration et font la tournée des administrations pour promouvoir une entreprise ou une position – se fassent connaître de la HATVP. Ainsi, tout le monde serait au courant et un fonctionnaire contacté par telle ou telle

personnalité pourrait vérifier auprès de la HATVP si elle est sincère et, le cas échéant, rémunérée ou soutenue par un État ou une entreprise afin d'en défendre la politique. Nous pensons, en interministériel, à un texte de loi en ce sens ; nous en avons déjà discuté avec la HATVP et, selon le calendrier parlementaire, nous parviendrons peut-être à vous faire des propositions.

M. le président Jean-Philippe Tanguy. Puisque l'on parle des possibilités de revoir la loi, le concept d'intelligence avec l'ennemi, qui me semblait, ainsi qu'à d'autres membres de ma famille politique, tout à fait utilisable, paraît daté et peu opérationnel à plusieurs des personnes que nous avons auditionnées.

En ce qui concerne le cas des anciens pilotes qui vont former d'autres armées, je le découvre et j'en suis stupéfait.

En France, depuis l'invasion de l'Ukraine par la Russie, on entend encore s'exprimer des gens comme Alexander Makogonov, porte-parole de l'ambassade de Russie dans notre pays, régulièrement interviewé sur LCI. Ce qu'il dit – pour le peu que j'ai le temps de suivre – me paraît complètement surréaliste : il raconte n'importe quoi, fait des provocations… Au-delà même des informations qu'il donne, et qu'il appartient aux journalistes de contredire, on le laisse provoquer l'Ukraine, relativiser des violences, la notion même de crime de guerre, les atrocités commises.

Nous nous interrogeons, la rapporteure et moi-même, sur la capacité de la France à s'opposer à la possibilité d'émettre offerte à certains médias. Évidemment, nous sommes en démocratie et nous en sommes tous très heureux, mais il y a tout de même des limites. On a l'impression de subir tout cela, du fait d'un vide juridique : d'un côté, il y a la liberté d'expression et le droit de la presse, que vous avez invoqués ; de l'autre, des dispositions existant dans notre droit, comme la notion d'intelligence avec l'ennemi, semblent hors d'usage, voire taboues. Cet individu, par exemple, je ne comprends pas pourquoi il n'a pas été expulsé.

M. Stéphane Bouillon. Ici, je sors de ma sphère de compétence. Des agents de l'ambassade de Russie, nous en avons expulsé. Du point de vue opérationnel, je préfère que l'on expulse un attaché beaucoup moins visible, mais beaucoup plus actif en sous-main, que le porte-parole officiel, bien connu, intervenant sur une chaîne de télévision, censé y recevoir la contradiction de la part d'autres personnes – cela fait partie du débat. Si ce monsieur était expulsé, il serait remplacé par un autre. C'est sans doute parce que l'ambassadeur ne parle pas très bien français qu'il n'intervient pas lui-même à la télévision comme le faisait son prédécesseur, M. Orlov, lequel était très présent dans les médias.

Parmi les premières sanctions décidées après le début de l'invasion figurait l'interdiction faite à des médias comme *Sputnik* ou *Russia Today* d'émettre à partir de la France et de l'Europe. Nous avions considéré qu'ils devaient être interdits car ils faisaient de la propagande pour la Russie. Progressivement, nous avons fait en sorte que tous les proxys et autres moyens qu'ils pouvaient utiliser pour rebondir soient suspendus. Nous l'avons fait dans un cadre juridique établi ; ils ont eu le droit de contester cette décision devant la justice, nationale comme européenne, qui leur a donné tort. De ce point de vue, la démocratie a bien fonctionné et je ne peux que m'en réjouir.

L'article 414 du code pénal est très clair en ce qui concerne l'intelligence avec l'ennemi, « *le fait de livrer ou de rendre accessibles à une puissance étrangère* […] *des*

renseignements, procédés, objets, documents, données informatisées », etc., l'espionnage, la relation d'entente, pouvant entraîner une peine allant jusqu'à trente ans de détention criminelle et 450 000 euros d'amende, et le sabotage. Les peines sont lourdes. Tout cela date du XX^{e} siècle ! Une réflexion existe sur une meilleure proportion des sanctions. En effet, peut-être la dureté de la sanction encourue dissuade-t-elle le parquet de poursuivre et le juge d'instruction de procéder à des mises en examen. Trente ans de détention criminelle, cela tient au fait qu'il s'agit d'un crime, donc passible des assises ; or aucun juge d'instruction ne renvoie quiconque devant les assises pour intelligence avec l'ennemi actuellement. Pour autant, la correctionnalisation et un quantum de peine moindre pourraient donner le sentiment d'une moindre gravité. L'équilibre demeure à trouver.

Il faut aussi intégrer aux textes les évolutions que nous avons évoquées en parlant des réseaux sociaux et de l'utilisation des médias ou de proxys.

M. Kévin Pfeffer (RN). À propos des ingérences pendant les campagnes, vous avez cité, monsieur Ferriol, le cas précis d'une manœuvre de promotion du candidat Macron suivie d'un dénigrement par des groupes en Afrique, en lien avec Wagner. Vous avez indiqué avoir donné des éléments pour un reportage à ce sujet, que je pense avoir vu sur France 2. Les informations sur ce phénomène ont donc été communiquées au grand public après l'élection.

Or vous avez dit avoir identifié soixante phénomènes, dont cinq correspondant aux quatre critères d'une ingérence numérique étrangère. À qui précisément transmettez-vous les informations relatives à ces cinq cas, et qui décide de la communication de ces éléments au grand public ? Qu'en est-il des quatre cas dont celui-ci n'a pas eu connaissance ? Qui concernaient-ils ?

M. Stéphane Bouillon. Une journaliste a demandé à être insérée chez Viginum pendant quelque temps. Nous avons accepté. Nous en avons prévenu les trois juges de l'élection. Lorsqu'elle a souhaité faire un reportage et sortir l'affaire Beth, nous avons demandé aux juges de l'élection s'ils y voyaient un inconvénient. Ils nous ont répondu que non. Cette journaliste a donc pu travailler, sans que nous n'intervenions sur son travail d'ailleurs. Elle a également eu connaissance des autres sujets qui ont été évoqués ; si elle avait voulu en faire le sujet de son reportage, il en serait allé exactement de même.

M. Kévin Pfeffer (RN). Si elle a eu accès aux cinq dossiers en question, peut-être pourrions-nous y accéder nous aussi. Je ne crois pas que vous les ayez énumérés.

En ce qui concerne les relations avec les plateformes numériques et les suites à donner en cas de détection d'une ingérence avérée, avons-nous vraiment les moyens de stopper la diffusion et de le faire suffisamment rapidement, d'après votre expérience de la réactivité des plateformes ?

M. Gabriel Ferriol. Je précise que la demande de la journaliste, qui avait déjà travaillé sur Wagner, concernait l'influence russe. Nous lui avons communiqué les éléments relatifs à ce phénomène car nous avions, comme l'a dit le secrétaire général, des motifs de soupçonner l'implication de la galaxie Prigojine. Nous ne lui avons pas parlé des autres phénomènes, notamment de ceux émanant de l'extrême droite américaine, car ce n'était pas le sujet de son reportage.

S'agissant du lien avec les plateformes, l'année 2022 a été pour nous une année de test, une année où nous nous sommes demandé comment répondre à ces phénomènes.

Dans le cas du phénomène Beth, nous avons d'abord voulu faire preuve de transparence : la médiatisation de cette histoire permet de démontrer aux gens que ces manipulations existent.

Nous avons aussi contacté les différentes plateformes impliquées pour leur signaler le phénomène. Nous leur avons décrit ce que nous avions observé, en leur fournissant des critères techniques pour qu'elles puissent conduire leurs propres investigations de façon indépendante et décider d'éventuelles actions de modération. La difficulté que nous avons rencontrée, c'est que, parmi nos critères, figurent le « *contenu manifestement inexact ou trompeur* » et la « *diffusion artificielle ou automatisée, massive et délibérée* ». Or les plateformes ont, elles, une lecture très anglo-saxonne : à leurs yeux, le fait qu'un contenu soit manifestement inexact ou trompeur n'est pas une raison suffisante pour le faire disparaître. Elles sont beaucoup plus intéressées par les manœuvres inauthentiques ou coordonnées. En l'occurrence, elles sont tombées d'accord avec nous pour considérer que l'activité en cause était inauthentique ; mais elles ont estimé que nous n'apportions pas suffisamment de preuves d'une coordination des différentes « fermes à trolls » impliquées. Tous ces groupes disaient à peu près la même chose ; mais, parce que nous n'utilisons que des sources ouvertes, nous ne pouvions pas démontrer qu'ils étaient coordonnés, qu'ils avaient un même plan d'action, qu'ils obéissaient à un même commanditaire. Les plateformes ont considéré que les éléments que nous leur apportions ne justifiaient pas une mesure de modération.

Nous restons très humbles : il est tout à fait possible que ce que nous leur apportions n'ait pas été suffisant pour statuer. Mais nous observons aussi que les efforts de modération déployés par les plateformes en Afrique sont bien moins intenses qu'aux États-Unis ou en Europe. Des logiques économiques sont à l'œuvre… C'est pour cette raison que l'Afrique devient, pour reprendre les mots du secrétaire général, une sorte de Far West informationnel ; les États n'interviennent pas pour réguler, les plateformes ne sont pas incitées à le faire. Le champ de l'information y est donc particulièrement sauvage.

M. Kévin Pfeffer (RN). Je vois plutôt d'un bon œil le fait que ces phénomènes soient expliqués au grand public, dès lors qu'ils le sont de manière équitable, pour tous les phénomènes et pour tous les candidats.

Avez-vous seulement détecté des attaques visant à dénigrer les candidats ou bien certains phénomènes visent-ils plutôt à en favoriser certains ?

M. Gabriel Ferriol. Les phénomènes que nous avons classés comme ingérences numériques étrangères visent en effet surtout à dénigrer soit un candidat, soit la procédure électorale elle-même. Le cas Beth est particulier, vous l'avez compris, puisque c'est en apparence une opération de promotion qui se déroule selon un calendrier en deux phases : une première opération d'installation de ces fermes à trolls, de promotion des narratifs ; dans un second temps, on fait apparaître dans des blogs, dans des médias locaux, l'idée que des fermes à trolls seraient actives, dans l'espoir que des journalistes indépendants s'en saisissent, trouvent les premiers comptes implantés et confirment qu'une opération de promotion avait bien été téléguidée. C'est une manœuvre sophistiquée, qui implique une grande maîtrise de l'enjeu informationnel par certains de nos compétiteurs stratégiques.

Parmi les soixante phénomènes que nous avons détectés, il y avait de tout : certaines choses nous paraissaient inauthentiques mais nos vérifications n'ont rien donné ; certains phénomènes cachaient peut-être des ingérences mais nous n'avons pas pu démontrer l'implication d'un acteur étranger. Encore une fois, je parle avec beaucoup de modestie : la

campagne présidentielle de 2022 était le premier engagement intense du service Viginum, créé quelques mois auparavant seulement. Je n'affirmerai pas que nous avons tout vu, tout compris. Mais nous avons pu démontrer qu'il était possible de mettre au jour des phénomènes et de tester notre chaîne de réponses et de ripostes.

Sur ce dernier aspect, j'ajoute à ce que disait le secrétaire général que c'est là une action interministérielle par nature, puisque ces phénomènes de manipulation de l'information touchent plusieurs champs ministériels : les élections relèvent du ministère de l'intérieur, l'influence et la contre-ingérence relèvent plutôt des services de renseignement et du ministère des affaires étrangères. Cela explique le rattachement de Viginum au SGDSN : la manœuvre d'ensemble doit être coordonnée, sous l'autorité de la Première ministre, pour définir une ligne d'action commune.

Mme Constance Le Grip, rapporteure. J'aimerais aborder la question de la sensibilisation à la réalité de la menace et du risque d'ingérence étrangère. Tous les services que nous avons rencontrés ont, comme vous-même, monsieur le secrétaire général, insisté sur l'importance de faire comprendre à tous combien cette menace est élevée, protéiforme et incessante. Il y a toutefois des maillons faibles. Nous nous inquiétons par exemple des ingérences étrangères dans nos universités et nos institutions de recherche, mais aussi, au-delà du milieu strictement académique, dans les *think tanks* et autres fondations – dont nous voyons bien que certains sont sous influence, voire financièrement accompagnés. Le rapport du sénateur André Gattolin *Mieux protéger notre patrimoine scientifique et nos libertés académiques* avait déjà démontré la réalité de ces phénomènes. Des actions sont menées, même s'il n'est bien sûr pas question de mettre en cause les libertés académiques, mais comment pensez-vous qu'il soit possible de sensibiliser tout un chacun à la nécessité d'être sur ses gardes ? Que peut faire l'État, notamment le ministère de l'enseignement supérieur et de la recherche ?

En ce qui concerne les médias, l'Arcom joue son rôle. Mais il est vrai que l'on voit régulièrement sur LCI le porte-parole de l'ambassade de Russie, à qui n'est apportée aucune véritable contradiction. Bien sûr, vous avez raison, si ce n'était pas lui, ce serait quelqu'un d'autre… Sur BFM TV non plus, les plateaux ne sont pas toujours équilibrés.

J'aimerais également vous entendre sur les innovations technologiques. C'est depuis toujours un défi pour ceux qui sont chargés de la protection de la nation. Les cryptomonnaies en est un pour Tracfin, par exemple. Dans votre cas, je pense aux *deep fakes* : comment envisagez-vous d'y répondre ?

M. Stéphane Bouillon. Les universités n'ont certes pas autant de crédits publics qu'elles le souhaiteraient, mais l'argent du contribuable doit servir à financer la recherche française et pas celle d'un État étranger. Ceux qui reçoivent de l'argent de l'État ont des devoirs vis-à-vis de lui : ils doivent s'assurer que cet argent employé au profit de notre pays, et pas d'autres. Nous essayons de faire passer le message !

Ainsi, dans le cadre du plan d'investissement France relance ou d'autres actions de soutien à des entreprises ou à des laboratoires, nous essayons d'introduire des clauses qui obligent les bénéficiaires à assurer une certaine sécurité. Nous envoyons souvent la DGSI – ou la gendarmerie pour les petites structures – dans les entreprises que nous avons classées comme « opérateurs d'importance vitale » ou « opérateurs de service essentiel » ou dans les laboratoires dont le travail peut intéresser les intérêts fondamentaux de la nation, pour vérifier

si tout se passe bien, notamment si les zones à régime restrictif (ZRR), c'est-à-dire les zones de protection rapprochée autour des locaux, sont bien respectées.

Nous nous demandons si, afin d'inciter les gens à accomplir des efforts, il ne faudra pas un jour demander au législateur de définir des règles et d'imposer des conditions de sécurité plus sévères que celles prévues aujourd'hui par décret – à moins que nous n'agissions sous forme contractuelle. Nous essayons de dialoguer mais, avec certains chercheurs, cela demeure compliqué…

Le ministère de l'enseignement supérieur et de la recherche est tout à fait sensible à ce sujet, très actif, et nous discutons très régulièrement pour que toutes les instances de recherche s'assurent auprès de différentes universités qu'elles prennent en considération tel ou tel élément.

Nous veillons aussi à refuser des visas à certains étudiants étrangers, ou à les retirer lorsque nous nous rendons compte par exemple que l'étudiant est resté dans le laboratoire à une heure où il était censé être rentré chez lui. Nous sommes très attentifs, y compris pour des demandes de formation pour des étudiants en licence de lettres, d'histoire ou de sciences humaines qui, une fois inscrits dans une université, souhaitent basculer vers la physique ou la chimie. La plus grande prudence est de mise.

Certains présidents d'université comprennent la situation et sont attentifs ; d'autres sont hermétiques, et ce n'est pas forcément ceux dont on attendrait une grande vigilance qui se révèlent attentifs – nous avons quelques déceptions ! Nous devons donc poursuivre nos efforts.

Votre rapport nous sera certainement utile pour ouvrir des discussions, évoquer les sujets, expliquer. Les articles du *Monde* sur la Team Jorge le sont aussi, car ils permettront de se rendre compte qu'internet est une jungle. Plus on en parle, plus les gens se méfieront – et s'il faut peut-être renforcer les sanctions pour ceux qui sont vraiment de mauvaise volonté, c'est bien l'aspect pédagogique qui m'apparaît primordial.

S'agissant des innovations technologiques et en particulier des *deep fakes*, c'est pour nous une grande source d'inquiétude. Nous travaillons au sein des services secrets – mais Bernard Émié, directeur général de la sécurité extérieure, vous en parlerait mieux que nous – et avec d'autres interlocuteurs pour recenser ce qui permet, dans une vidéo, de repérer les *deep fakes*. Les Américains ont progressé sur ce sujet, nous échangeons avec eux pour identifier les problèmes. La menace est incontestablement forte. Le nouveau logiciel ChatGPT en est une également : l'intelligence artificielle en est à ses balbutiements et ses erreurs sont très visibles, mais la vitesse du progrès étant ce qu'elle est, les prochaines machines seront, je n'en doute pas, beaucoup plus talentueuses. Nous pouvons nous retrouver dans une situation où nous serons bêtes face à une intelligence artificielle – et c'est un véritable danger.

L'intelligence artificielle doit être un outil pour l'intelligence humaine, mais elle ne peut pas la remplacer… Vaste programme, comme on dit ! Et, contrairement à la machine, l'esprit humain est paresseux. Notre faiblesse est donc bien réelle, et le législateur devra nécessairement, un jour, se pencher sur ces problèmes.

M. Laurent Esquenet-Goxes (Dem). Certains lieux connaissent une forte concentration de laboratoires de recherche, d'écoles d'ingénieurs et d'autres structures

stratégiques. Je pense à la Bretagne, mais aussi à Toulouse. Avez-vous connaissance d'une montée des attaques contre ces lieux ? Des mesures spécifiques ont-elles été prises ?

M. Vincent Strubel. Dans le domaine de la cybersécurité comme dans d'autres, la concentration peut être une excellente chose ; le Campus cyber, à La Défense, en est un bon exemple puisqu'il regroupe des utilisateurs de solutions de cybersécurité, des entreprises qui les conçoivent, des chercheurs, des écoles et des services de l'État. Cela permet un essaimage croisé. Tout le monde mange à la même cantine, ce qui permet de faire circuler les idées et d'en faire naître de nouvelles. Il en va de même en Bretagne, ou à Toulouse pour le secteur aérospatial.

La concentration physique ne change pas grand-chose à la menace. Le secteur aérospatial, concentré à Toulouse, fait régulièrement l'objet de tentatives d'espionnage ; les acteurs de la cybersécurité sont aussi des cibles. Ce que l'on constate aujourd'hui, c'est plutôt un déplacement de la menace vers la *supply chain*, la chaîne d'approvisionnement : les sous-traitants, notamment les prestataires informatiques des cibles, sont parfois des cibles plus faciles que les entités stratégiques elles-mêmes, qui ont acquis les bonnes habitudes nécessaires. Nous sommes très vigilants. Je reprends l'exemple du secteur aérospatial : l'ANSSI travaille de longue date avec ces entreprises, avec les entités stratégiques qui font partie de la base industrielle et technologique de défense (BITD), qui sont pour la plupart des opérateurs d'importance vitale. Elles sont très sensibles à ces sujets car elles ont connu des attaques. Mais nous travaillons aussi de plus en plus avec les entités qui se trouvent en amont dans la chaîne d'approvisionnement et avec tous les acteurs de la cybersécurité.

L'ANSSI exerce de nombreux métiers : audit, conseil, utilisation de solutions de détection, réponse à incident – c'est-à-dire cyber-pompier… L'un de ces métiers est la labellisation de prestataires de sécurité informatique : nous nous prononçons sur leur compétence mais aussi sur la façon dont ils sécurisent leurs propres infrastructures. C'est une démarche qui n'est pas nouvelle, puisque les premiers labels remontent à 2014. Nous étions dès ce moment-là bien conscients du fait que les acteurs de la cybersécurité étaient des cibles, d'abord parce qu'ils détiennent des technologies et un savoir-faire rare, mais aussi parce qu'ils peuvent donner accès à d'autres cibles de haute valeur, des entités qu'ils auditent, qu'ils supervisent ou pour le compte desquelles ils vont s'occuper d'infrastructures de cyberdéfense.

Je reviens à votre question après ce détour : la menace cyber est peu sensible à la localisation géographique ; la concentration d'entités spécialisées a d'énormes avantages et ne les expose pas davantage. On peut penser qu'il est alors plus facile de les espionner de façon plus traditionnelle, mais on sort là de mon champ de compétence.

M. le président Jean-Philippe Tanguy. La perte de contrôle capitalistique et l'affaiblissement industriel d'Alcatel posent-ils un problème pour la sécurité nationale et, au-delà, pour celle du continent européen ? C'était un acteur franco-américain de la sécurité. Voyez-vous d'autres possibilités de relancer cette filière ? Thierry Breton a lancé des alertes à propos de différentes filières. Certes, Nokia opère encore en Europe, mais est-ce suffisant ? Je pense par exemple à la sécurité de nos installations en Bretagne.

Une question candide : avez-vous identifié sur le territoire français des complices qui tentent de faciliter l'efficacité des attaques d'acteurs étrangers ?

Vous avez utilisé l'image des filets dérivants. Il est vrai que dans les dernières campagnes, ma famille politique a pu être accusée d'entretenir certains liens. Mais, en tant

que responsable politique et chef d'un petit parti, je suis victime de trolls à la moindre publication. Or ces trolls qui attaquent mes tweets ou mes posts Facebook, ceux de mes camarades, ou le site de notre parti – l'Avenir français est un tout petit parti qui n'a pas de moyens de protection – ne me semblent pas bien différents de ceux qui visent la majorité présidentielle, le parti Les Républicains ou la gauche. Ne sommes-nous finalement pas tous victimes de ces fermes à trolls ? Les acteurs français ne sont-ils pas tous attaqués de façon assez semblable ?

Dernière question : depuis quelques mois, on voit apparaître des publicités numériques qui lient des personnalités politiques à des offres de rénovation thermique ou de crédit d'impôt. Au lieu de voir une photo d'artisan, on voit celle d'un ministre… Est-ce un phénomène sur lequel vous vous penchez ? Cela prend des proportions importantes, notamment en période électorale.

M. Gabriel Ferriol. Le cadre réglementaire nous impose de démontrer l'implication d'un acteur étranger. Ce sont donc eux que nous recherchons en priorité, plutôt que des complices en France. On observe, de manière générale, que les opérations à large spectre, visant à toucher l'ensemble de la population, tendent à disparaître au profit d'opérations beaucoup plus ciblées. Il s'agit de promouvoir un narratif vers certains groupes – on parle de microciblage – en profitant des possibilités offertes par les plateformes numériques de s'adresser à des audiences spécifiques. Le marketing numérique permet de cibler un homme, de telle tranche d'âge, qui habite dans telle région, qui a telle gamme de revenus… Cela permet à nos adversaires d'être plus discrets, et ils choisissent souvent des « communautés à fort engagement », c'est-à-dire des groupes où il y a de bonnes chances que leur message fasse réagir, qu'il devienne viral. Ce sont souvent des communautés assez fermées, centrées sur certaines thématiques, parfois complotistes mais pas toujours, et qui parfois se trouvent seulement sur de petites plateformes.

Nous observons ces comptes, mais encore une fois, ce que nous devons démontrer, c'est l'implication d'un acteur étranger.

S'agissant des publicités sponsorisées, elles nous intéressent, car c'est l'un des modes opératoires qui permet à des acteurs malveillants d'accroître la visibilité de leur message, notamment au moyen du microciblage. Nous disposons d'outils qui nous permettent de savoir qui achète des publicités sponsorisées, et pour quel montant. Nous nous penchons particulièrement sur des publicités à caractère politique en période électorale, et nous nous sommes intéressés à plusieurs phénomènes de cette nature. Toutefois, celles que vous citez me semblent plutôt relever d'arnaques classiques, utilisant l'image de l'État pour ferrer de futures victimes et détourner des aides publiques – ce que l'on a beaucoup vu autour de la rénovation thermique ou du compte personnel de formation.

M. Vincent Strubel. En matière de cyberattaques autant que de trolls, les parlementaires sont des cibles comme tout le monde, et sans doute bien davantage ! Les réponses ne sont pas forcément complexes, et relèvent plutôt de l'hygiène informatique, de quelques précautions simples que l'ANSSI martèle depuis des années, en matière de mots de passe notamment. Je vous citerai une phrase qui est, selon les sources, soit un proverbe africain soit la publicité d'une grande marque de chaussures américaines : quand on est poursuivi par un lion, le plus important n'est pas de courir plus vite que lui mais de courir plus vite que quelqu'un d'autre… Il en va de même en matière numérique : c'est le maillon faible qui est attaqué en premier, et c'est lui qu'il ne faut pas être.

En ce qui concerne les publicités que vous citiez, une partie sont en effet des arnaques, voire des tentatives d'attaque informatique, la façon la plus simple de lancer une telle attaque étant de vous amener à cliquer sur un lien aboutissant à un site piégé qui essayera d'utiliser une vulnérabilité de votre navigateur. Il faut évidemment se méfier. Cela ne relève pas spécifiquement de la compétence de l'ANSSI, mais mobilise beaucoup le groupement d'intérêt public Action contre la cyber-malveillance, le GIP Acyma, créé par l'ANSSI, le ministère de l'intérieur et différents acteurs privés précisément pour sensibiliser à ce type de menaces, de façon permanente mais aussi en réaction à certaines menaces précises. Certaines campagnes du type que vous citez ont même utilisé l'image de l'ANSSI : des mails qui semblaient provenir de l'ANSSI et prévenir d'une menace étaient en réalité des pièges… La première précaution est toujours de ne pas cliquer sur quelque chose qui semble louche !

Vous nous demandez si nous avons identifié des complices. Ce que nous voyons, dans les cyberattaques, ce sont souvent des rebonds : il est très courant que des serveurs personnels, des box internet ou autres soient attaqués par un groupe criminel, ou pire, qui s'en sert ensuite pour attaquer d'autres systèmes. Il y a alors des complices sur le territoire national, mais ils le sont « à l'insu de leur plein gré ». C'est ce qui rend particulièrement complexe d'attribuer une attaque : on ne peut jamais se fonder sur l'adresse IP ou sur le chemin parcouru. C'est toute la subtilité de notre métier !

S'il y a des complices par choix, c'est à la justice de se prononcer.

S'agissant enfin d'Alcatel, je sors de mon domaine de compétence mais des dispositions légales permettent de contrôler certains investissements étrangers en France, sinon pour les bloquer tout à fait, au moins pour imposer des conditions. Dans le cas d'Alcatel, cela a notamment conduit à traiter certaines activités, notamment dans le domaine des câbles sous-marins, différemment des autres – les activités grand public ont été, elles, vendues au plus offrant.

Cela rejoint un enjeu de souveraineté, particulièrement dans les réseaux de télécommunication. Je ne peux que citer la loi du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles. Elle permet à l'État, plus précisément au Premier ministre et au SGDSN qui instruit les dossiers, d'accepter ou de refuser le déploiement de telle ou telle solution dans nos réseaux radioélectriques et dans le réseau de télécommunications mobiles en particulier, sur la base de critères techniques mais pas uniquement. La loi cite, parmi les motifs de refus, *« le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État non membre de l'Union européenne »*. Cela nous permet de protéger l'essentiel dans un domaine où, à défaut d'acteurs français, deux acteurs parmi les trois très présents sur le marché mondial sont encore européens – Nokia et Ericsson –, le troisième étant chinois.

Mme Constance Le Grip, rapporteure. L'entreprise TikTok s'est récemment attaché les services d'un cabinet de lobbying et de relations publiques qui invite les parlementaires à découvrir à quel point TikTok est un média utile à la diffusion de la culture, notamment auprès des jeunes. Le considérez-vous comme un outil d'ingérence chinois ?

M. Stéphane Bouillon. J'aurais tendance à répondre que oui… C'est un réseau social dont le mode de fonctionnement est particulier, et qui est rattaché à la Chine. On ne peut pas le regarder comme neutre, à supposer d'ailleurs qu'il existe un réseau social que l'on

puisse considérer comme neutre. Il faut toujours être prudent, vis-à-vis de TikTok en particulier.

M. Gabriel Ferriol. J'irai dans le même sens. Nous sommes très attentifs au développement de TikTok en France et en Europe. La presse s'est fait l'écho du fait que certains contenus diffusés sur ce réseau en Europe sont très différents de ceux qui sont diffusés en Chine, ce qui pose la question de la finalité de l'outil et de ses usages. TikTok cherche à conquérir des tranches d'âge bien plus jeunes que d'autres réseaux, dans une optique de temps long qui doit appeler notre attention. Du point de vue technique, c'est un outil plus difficile à appréhender pour mes équipes que d'autres plateformes, à la fois parce qu'il est plus récent et parce qu'il est moins ouvert. Nous faisons bien sûr les efforts nécessaires.

On observe aussi sa diffusion très rapide en Afrique, accompagnée d'un énorme effort financier de promotion. C'est un sujet sur lequel nous devons être très vigilants.

M. Vincent Strubel. Pour faire le lien entre ces sujets et celui du *lawfare* et de l'applicabilité du droit, je souligne que l'ANSSI est toujours sensible au droit applicable aux différents fournisseurs de services numériques. La question se pose de manière éminente dans le domaine du *cloud*, c'est-à-dire de l'informatique en nuage, mais pas uniquement. Nous nous préoccupons des modalités d'accès à l'information et des modalités de coopération des acteurs économiques étrangers avec les pouvoirs publics des pays dans lesquels ils sont enregistrés. L'exemple le plus connu est celui du *Cloud Act – Clarifying Lawful Overseas Use of Data Act* – qui permet au juge américain d'accéder très largement aux contenus hébergés et traités aux États-Unis ; cette loi ne concerne pas le seul cloud mais s'étend aux outils de télécommunication, comme WhatsApp par exemple, auxquels la justice américaine peut donc avoir accès sans s'engager dans une démarche de coopération judiciaire internationale. La Chine n'est pas en reste : une loi sur le renseignement de 2017 y fait obligation à tout citoyen, à toute entreprise, à toute association, bref à toute entité chinoise de coopérer avec les services de renseignement dans la collecte du renseignement. Chez nous, un tel texte, à supposer qu'il soit voté par le législateur, serait assorti de conditions d'application précises ; la loi chinoise est autoporteuse, elle n'offre pas plus de précisions, ou alors elles ne sont pas publiques.

M. le président Jean-Philippe Tanguy. Merci à tous les trois de vos réponses passionnantes et précises, comme de votre engagement au service de notre pays et de nos valeurs.

La séance s'achève à dix-huit heures dix.

———

Membres présents ou excusés

Présents. – M. Laurent Esquenet-Goxes, Mme Constance Le Grip, M. Kévin Pfeffer, M. Charles Sitzenstuhl, M. Jean-Philippe Tanguy.

Excusés. – Mme Anne Genetet, Mme Hélène Laporte.