ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mercredi 25 juin 2025
Séance de 16 heures 30

Compte rendu n° 11

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 16 heures 30

La commission spéciale a auditionné M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la cybermalveillance (GIP-ACYMA), M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI) et Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris.

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité par l'audition de M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma) ; de M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI) et de Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre I^{er}, consacré à la résilience des activités d'importance vitale, procède à la transposition de la directive sur la résilience des entités critiques (REC) ; il est rapporté par Mme Hervieu. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité, procède à la transposition de la directive sur la sécurité des réseaux et des systèmes d'information (NIS 2) ; il est rapporté Mme Le Hénanff. Enfin, le titre III, consacré à la résilience opérationnelle numérique du secteur financier, procède à la transposition de la directive, connue sous son nom anglais, Digital Operational Resilience Ac, DORA. Il est rapporté par Mickaël Bouloux, qui s'excuse de ne pas pouvoir être présent aujourd'hui. Enfin, M. Éric Bothorel est le rapporteur général du projet de loi.

Nous avons souhaité vous entendre, car les institutions que vous représentez sont chargées à des titres très divers de lutter contre la cybercriminalité. Pourriez-vous nous dresser un état des lieux de la menace telle que vous la percevez et des moyens mis en place pour lutter contre ce phénomène inquiétant et en pleine croissance ? Je souhaiterais également recueillir votre avis sur le filtre anti-arnaque que nous avions inscrit dans la loi et qui n'est pas encore opérationnel. Quand celui-ci sera-t-il développé et mis en place ? Par ailleurs, quel est votre avis sur l'article introduit par le Sénat interdisant l'affaiblissement du chiffrement ? Dans ce contexte, nous souhaitons aussi vous entendre sur la manière dont vous percevez le projet de loi et les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI). Mon propos introductif a pour objet de vous présenter rapidement la manière dont le ministère de l'intérieur est organisé en matière de lutte contre la cybercriminalité, avant de mettre en lumière l'état de la menace et quelques réflexions dans le cadre de la transposition de NIS 2, en lien avec nos différentes observations sur le terrain, notamment du côté du monde de l'entreprise.

Le Comcyber-MI est un service à compétence nationale créé le 1er décembre dernier, que j'ai l'honneur de commander. J'ai pour adjoints un policier et un magistrat. L'ensemble des autres personnels sont des militaires de la gendarmerie et des personnels civils de la gendarmerie nationale. Ce dispositif, chargé de lutter contre la cybercriminalité est organisé autour de quatre grands piliers. Le premier pilier porte sur la stratégie, puisque nous sommes

en charge de définir la stratégie ministérielle de lutte contre la cybercriminalité, qui a été annoncée par le ministre délégué François-Noël Buffet le 2 avril dernier à l'occasion du Forum InCyber à Lille. Elle a vocation à être déclinée par les services de police et de gendarmerie dans des plans d'action pour chacune des entités.

Nous avons également pour mission de contribuer à porter la parole du ministère de l'intérieur sur les évolutions réglementaires et législatives, de manière à permettre aux gendarmes et aux policiers de pouvoir travailler dans les meilleures conditions possibles. Nous conduisons également une action internationale et nous sommes chargés de différentes actions de prévention et de mise à disposition des contenus au profit des forces de police et de gendarmerie pour mener des actions de prévention dans les territoires.

Le deuxième pilier concerne l'anticipation, autour de deux composantes. La première a trait au renseignement d'intérêt cyber. Nous avons pour mission de publier tous les ans un rapport sur l'état de la menace. Le premier rapport a été publié l'année passée, au mois de juillet, et le rapport 2025 le sera dans les jours à venir. Au-delà, nous réalisons des fiches d'alerte flash sur différents phénomènes, que nous diffusons de manière très large, à la fois au sein du ministère, auprès des autres administrations, et de l'écosystème privé. À titre d'exemple, cette division de l'anticipation est d'ailleurs présente au sein du Campus Cyber, de manière à être connectée à l'écosystème privé, au monde de la recherche et au monde universitaire. Dans l'anticipation, nous menons également des actions en matière de gestion de crises, en particulier sur des sujets qui sont liés à la prévention.

Nous n'intervenons pas directement sur l'accompagnement à la gestion de crises, mais plutôt à la préparation, notamment des entreprises ou des collectivités. À ce titre, nous avons réalisé en collaboration avec cybermalveillance.gouv.fr un module de formation en ligne (Mooc) d'une durée d'à peu près deux heures, qui permet de se poser les bonnes questions sur une crise potentiellement naissante. Ce Mooc est régulièrement utilisé par des entreprises, dans le cadre de l'accompagnement et de la préparation à une gestion de crise cyber.

Le troisième pilier porte sur la formation. Notre centre national de formation continue de haut niveau en matière cyber est situé à Lille. Il forme des policiers et des gendarmes de la France entière, par exemple sur le blanchiment des cryptomonnaies ou encore l'enquête sous pseudonyme. Nous avons aussi élargi les formations au *continuum* de sécurité à différents acteurs en charge de la lutte contre la cybercriminalité tels que des magistrats, mais aussi quelques entités du ministère de l'économie et des finances.

Enfin, le quatrième pilier est d'ordre pilier opérationnel, c'est-à-dire apporter un appui aux services de police et de gendarmerie spécialisés dans le cadre des enquêtes judiciaires sur des compétences dites rares. Je pense en particulier au blanchiment des cryptomonnaies, sujet majeur aujourd'hui et largement utilisé dans le cadre de la criminalité organisée, mais aussi au traitement de la donnée de masse ou l'expertise numérique du haut du spectre sur tous les objets connectés.

Les différentes directions du ministère disposent, à leur niveau, d'un service spécialisé en matière d'enquête judiciaire. Pour la police nationale, il s'agit de l'Office anti-cybercriminalité (Ofac), qui est en charge de la coordination opérationnelle des services ; l'Unité nationale cyber (UNC) pour la gendarmerie et la Brigade de lutte contre la cybercriminalité (BL2C), sans parler de la direction générale de la sécurité intérieure (DGSI) dans un domaine de compétences très particulier.

S’agissant de l’état de la menace, notre prochain rapport sera publié dans quelques jours. Il portera à la fois sur les atteintes fortes aux biens et les atteintes aux personnes. Les atteintes aux biens, qui représentent globalement deux tiers des infractions enregistrées, correspondent, pour 80 % d’entre elles, à des escroqueries sur internet. Les 20 % restants portent sur des atteintes au système de traitement automatisé des données, notamment les attaques par rançongiciel, sans doute les plus dévastatrices sur les systèmes d’information. Ce phénomène important touche typiquement les territoires, en métropole ou en outre-mer, les collectivités territoriales de toute taille, les petites et moyennes entreprises (PME), les entreprises de taille intermédiaire (ETI), les hôpitaux, les professions de santé en général. Il y a quelques années, les grands groupes industriels étaient les principales victimes. L’adversaire s’est largement adapté et aujourd’hui, il part à la chasse sur tous les types de structures ; tout le monde peut être concerné. En conséquence, la mise à niveau de la maturité cyber dans les territoires pour les différentes entités est importante pour la résilience globale de notre système économique.

S’agissant des atteintes aux personnes, nous observons un certain nombre de sujets liés à la pédopornographie, au cyberharcèlement, sur les réseaux sociaux notamment, et internet en général.

Ensuite, je souhaite offrir un éclairage sur la partie prévention. Le Comcyber-MI est notamment en charge de transmettre aux services de police et de gendarmerie des éléments de langage pour mener la prévention dans le territoire. Je tiens à évoquer à ce titre une action historiquement conduite par la gendarmerie nationale, c’est-à-dire une action de diagnostic cyber, notamment au profit des collectivités territoriales, mais qui a ensuite été déclinée au profit des entreprises.

Elle a débuté en 2021 avec un questionnaire d’autodiagnostic de dix questions qui a démontré que les risques étaient plutôt de nature « rouge » que « verte », ce qui était assez problématique. La gendarmerie a souhaité aller plus loin, en développant un pré-diagnostic de 70 à 120 questions en fonction de la taille de la collectivité. Ce questionnaire comporte surtout des questions « de bon sens » posées à l’entité en charge de la collectivité, au-delà des directeurs des systèmes d’information (DSI). Il a permis de révéler que de nombreuses collectivités n’étaient pas au niveau de maturité cyber que l’on aurait pu espérer.

Dans cette action, nous avons souhaité nous rapprocher de l’Agence nationale de la sécurité des systèmes d’information (Anssi), à la suite de la création du Comcyber-MI. L’Anssi a ainsi développé l’outil MonAideCyber, vers lequel le ministère de l’intérieur s’oriente en matière de diagnostic. MonAideCyber figure aujourd’hui dans la stratégie ministérielle de lutte contre la cybercriminalité. Après les collectivités, nous nous sommes tournés vers les entreprises pour pouvoir assurer un certain nombre de diagnostics. Les différents outils disponibles (autodiagnostic, pré-diagnostic et audit) ne disposent pas tous de la même profondeur de champ, ce qui pose la question de savoir lesquels utiliser, selon quels besoins.

Ensuite, que faire ? Dès lors que le constat d’une maturité cyber insuffisante pour une collectivité ou pour une entreprise est posé, les services de police ou de gendarmerie n’orientent pas vers un prestataire de services mais vers cybermalveilliance.gouv.fr qui dispose dans les territoires d’une liste d’entités référencées ou labellisées, ou vers les CSIRT régionaux, qui disposent d’entités référencées. Dans ce cadre, l’enjeu de la coordination est essentiel, les entreprises ou les collectivités évoquant souvent les sujets de visibilité, ce qui soulève la question de la labellisation.

Le Comcyber-MI noue également des liens très étroits avec l'Anssi, incontournable sur NIS 2. Nous avons besoin que nos gendarmes et nos policiers disposent d'une bonne connaissance des éléments essentiels de NIS 2, afin qu'ils puissent communiquer et répondre aux questions. Nous élaborons actuellement avec l'Anssi un document simple à cet effet, mais également un document plus élaboré pour les personnels qui effectueront des diagnostics dans le cadre de MonAideCyber.

Par ailleurs, les forces de sécurité intérieure ont besoin d'être alertées dès lors qu'une attaque cyber est connue. Au-delà de la priorité principale d'une entreprise ou d'une collectivité qui cherchent à rétablir un système d'information, il nous faut récupérer des éléments techniques nous permettant de localiser, voire d'identifier un auteur. Nous avons donc besoin d'une coordination entre la victime, le cas échéant l'Anssi, les entités de remédiation et les services enquêteurs. Il s'agit là du principe du « Dites-le-nous une fois ».

S'agissant du filtre anti-arnaque, je préfère laisser Jérôme Notin évoquer le sujet, le Comcyber-MI n'étant pas directement impacté. Vous avez également mentionné l'affaiblissement du chiffrement. Plutôt que de répondre sur l'affaiblissement du chiffrement en tant que tel, je préfère évoquer la question du besoin des enquêteurs. La plupart des enquêtes judiciaires concernent une multitude de données, raison pour laquelle le Comcyber-MI dispose d'une compétence rare, le traitement de la donnée de masse.

Dès lors que la donnée est chiffrée, nous ne pouvons pas y accéder, ce qui affecte la recherche d'éléments permettant d'établir la manifestation de la vérité. Les messageries chiffrées EncroChat, Sky ECC ou plus récemment Ghost ou Matrix sont des dispositifs mis en place par des réseaux criminels, mais nous avons pu accéder aux données, ce qui nous a permis de démanteler un certain nombre de réseaux de criminalité organisée et conduire des interpellations à travers le monde. En résumé, les enquêteurs ont besoin de pouvoir accéder à la donnée.

Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris. La section J3 dédiée à la lutte contre la cybercriminalité du parquet de Paris dispose d'une compétence nationale concurrente, c'est-à-dire qu'elle a vocation à se saisir des affaires du haut du spectre, les dossiers qui ont un intérêt pour la sécurité de la nation et qui impliquent de disposer d'une centralisation de l'information et de l'enquête. Le reste des dossiers sera quant à lui laissé aux parquets locaux. Naturellement, il existe un magistrat référent cyber dans chaque parquet de France, avec lequel il est possible de dialoguer, d'échanger.

La section J3 est une petite section composée de cinq magistrats ; de deux assistants spécialisés, c'est-à-dire du personnel spécialement formé techniquement pour nous aider ; une attachée de justice dédiée à la lutte contre la cybercriminalité qui apporte un soutien du point de vue de la coopération internationale ; et d'une équipe de greffiers. Cette section a crû au fil des années, à mesure que la menace s'est développée.

Le rôle de la justice consiste à traduire les cybercriminels devant des juridictions, afin qu'ils soient jugés et condamnés pour les infractions qu'ils ont commises. Lorsque ces auteurs sont situés dans des pays qui ne coopèrent pas, qui n'exécutent pas les demandes d'extradition, l'intérêt de l'enquête consiste à pouvoir émettre des mandats d'arrêt, ce qui signifie que les cybercriminels ne pourront plus quitter le pays. Même s'il n'y a pas de condamnation, cette menace du mandat d'arrêt est extrêmement forte et puissante.

Au-delà des questions d'arrestation et de jugement, qui constituent véritablement le cœur de notre métier, nous luttons ces dernières années contre les infrastructures criminelles. Ce faisant, en démantelant des réseaux de *botnets* derrière les attaques, nous empêchons les criminels de pouvoir attaquer nos institutions, nos entreprises. De même, nous saisissons des avoirs criminels, comme des *wallets* de cryptomonnaies riches de plusieurs dizaines de millions d'euros, affaiblissant ainsi les réseaux. Cet argent saisi permet d'indemniser les victimes, et lorsque celles-ci ne peuvent être identifiées, il est reversé à l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (Agrasc), l'agence chargée de gérer les avoirs criminels pour la justice. Elle pourra ensuite l'utiliser pour mener d'autres actions, permettre aux magistrats et aux enquêteurs d'être plus efficaces.

Une autre action, plus novatrice, consiste à utiliser le canal judiciaire comme un canal diplomatique. Dans certains cas, notamment pendant les Jeux olympiques, nous avons pu identifier que des pays nous avaient attaqués, probablement à travers leurs services. Nous leur avons donc envoyé une demande d'entraide, par exemple pour identifier le titulaire de l'adresse IP utilisée. Nous savions parfaitement que nous n'obtiendrions pas de réponse, mais à travers le canal judiciaire, nous leur avons fait savoir que nous avions connaissance du fait qu'ils étaient responsables de l'attaque.

Les différents moyens mis en œuvre par la section cyber contribuent à la lutte contre la cybercriminalité de façon générale. De façon indirecte, nous parvenons aussi à capter des renseignements. Grâce à l'article 706-105-1 du code de procédure pénale, nous avons la possibilité de communiquer l'information judiciaire de nos dossiers cyber aux différents services de l'État : l'Anssi, la DGSI, la direction générale de la sécurité extérieure (DGSE), le Comcyber des armées. Ces éléments leur permettent d'avoir une meilleure compréhension de la menace, d'assembler les pièces du puzzle, et de pouvoir mener une riposte. De fait, la justice et l'action du parquet contribuent, avec celles des autres services de l'État, à une riposte globale de la France.

À présent, je souhaite vous dresser un rapide panorama de la menace. Comme le général Husson l'a signalé, la première menace concerne les rançongiciels, car ils frappent le tissu économique, déstabilisent nos hôpitaux, nos collectivités locales. Ces rançongiciels se sont perfectionnés et nous sommes aujourd'hui confrontés à des groupes extrêmement structurés, dotés d'une véritable organisation criminelle. Pour autant, nous parvenons à obtenir des résultats. Je pense par exemple au dossier LockBit ou à l'auteur du rançongiciel Ako que nous avons jugé le mois dernier au tribunal judiciaire de Paris.

Néanmoins, je dois vous faire part d'un constat plus préoccupant, qui concerne la transformation numérique de la délinquance. Lorsque j'ai commencé à la section de lutte contre la cybercriminalité en 2017, nous nous concentrions surtout sur les piratages en tant que tels. Aujourd'hui, nous nous apercevons que les groupes criminels, qui n'étaient pas présents dans le cyber initialement, se sont « numérisés ». Dans la mesure où la société est complètement digitalisée, les surfaces d'attaque ont augmenté.

À titre d'exemple, auparavant, les narcotrafiquants ne pratiquaient pas le piratage informatique. Aujourd'hui, ils piratent les logiciels dans les ports pour faire passer des conteneurs de cocaïne, s'adjoignent les services de hackers pour pouvoir être plus discrets dans la communication. Nous assistons à une transformation générale de cette délinquance. Dans certains de nos dossiers, des groupes de délinquance habituels ont recruté des ingénieurs informatiques pour des sommes extravagantes, parfois 1 million d'euros.

Il faut retenir que maintenant, tous les groupes criminels ont un intérêt à attaquer un système de traitement automatisé de données, qu'ils ne travaillent pas en silos, mais que les narcotrafiquants et les hackers voient leur intérêt à unir leurs forces. À ce titre, il convient de mentionner le dossier « Dark Bank », une banque occulte mise à jour grâce au dossier Sky ECC. Cette banque a blanchi l'argent des narcotrafiquants, c'est-à-dire du cash, soit 1 milliard de dollars en dix-huit mois. Les hackers avaient beaucoup de cryptomonnaies et voulaient du cash, quand les narcotrafiquants avaient la problématique inverse. En conséquence, cette banque a fait chambre de compensation entre ces deux univers.

Ces deux éléments doivent être gardés à l'esprit aujourd'hui lorsque l'on parle de résilience. Nous serons de plus en plus attaqués parce que nous sommes de plus en plus digitalisés, parce que les groupes criminels traditionnels auront besoin de s'attaquer à ces vecteurs pour commettre des infractions, par exemple de narcotrafic. Le constat n'est guère réjouissant : les organisations criminelles ont intégré la digitalisation et le vecteur numérique comme une composante à part entière de leur activité. Face à cette menace grandissante, nous devons être plus efficaces dans notre réponse, encore progresser d'un cran.

S'agissant des questions plus spécifiques de M. le Président, je laisserai Jérôme Notin évoquer le filtre anti-arnaque, sujet sur lequel il est très engagé. Ensuite, lors des débats sur l'affaiblissement du chiffrement dans le cadre de la loi de lutte contre le narcotrafic, le parquet de Paris a été sollicité pour prendre position. Nous ne l'avons pas fait, pour différentes raisons, notamment parce que nous estimions que cette question ne relevait pas de notre compétence.

Néanmoins, à mon niveau, je peux vous fournir quelques éléments d'analyse. Nous avons évidemment besoin de pouvoir déchiffrer de la donnée pour nos enquêtes. À ce titre, le véritable enjeu consiste à savoir si l'on peut déchiffrer cette donnée sans affaiblir le chiffrement. Le service technique national de captation judiciaire (STNCJ), qui dépend de la DGSI, est censé effectuer des captations, c'est-à-dire hacker les téléphones, les serveurs et les ordinateurs, pour récupérer la donnée au profit de la police, de la gendarmerie et, *in fine*, de la justice. Ce service, qui a mis du temps à éclore, a obtenu des résultats assez prometteurs ces dernières années. Il doit continuer à pouvoir disposer de capacités pour pouvoir progresser.

Mais, au-delà, j'ai déjà proposé la création d'une véritable direction technique, qui serait co-dirigée par les deux ministères de la justice et de l'intérieur. À ce titre, le SNCJ pourrait intégrer cette agence, au même titre que l'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ), qui est chargée des interceptions téléphoniques pour la justice, pour venir au soutien de nos enquêtes.

La question ne consiste pas à savoir s'il faut affaiblir le chiffrement, mais quels moyens techniques la justice, la police et la gendarmerie ont à leur disposition pour mener des enquêtes. En créant cette véritable direction technique, qui existe à la DGSI et à la DGSE, vous armeriez la justice pour répondre à ces enjeux. À titre d'exemple, notre section cyber est souvent sollicitée par des collègues magistrats, qui souhaitent notre éclairage sur les possibilités techniques dans des dossiers de droit commun. Si cette agence était créée et dotée de véritables moyens humains, techniques et financiers, elle pourrait accomplir ce travail au profit de toutes les juridictions.

M. Jérôme Notin, directeur général du groupement d'intérêt public Acyma. Je commencerai mes propos par une présentation succincte de notre dispositif, la manière dont nous percevons le projet de loi et dont nous pensons que nous pourrions être impliqués, avant

d'aborder filtre anti-arnaque ainsi qu'un petit point d'actualité sur le chiffrement. Je précise également que la proposition de Mme Johanna Brousse concernant la création d'une direction technique co-dirigée par la justice et l'intérieur me paraît tout à fait opportune.

S'agissant de l'état de la menace, nous publions un rapport d'activité tous les ans, puisqu'en tant que dispositif national d'assistance aux victimes d'actes de cyberviolence, nous sommes au contact direct des victimes, particuliers, entreprises et collectivités. L'année dernière, la plateforme cyber-malveillance.gouv.fr a accueilli 5,4 millions d'utilisateurs, contre 3,7 millions en 2023. Sur cette plateforme, nous offrons des parcours de qualification de la menace, en fonction des différents profils, pour proposer aux victimes des conseils adaptés, une mise en relation avec des prestataires. Nous avons ainsi cartographié sur l'ensemble du territoire des prestataires référencés et des prestataires labellisés.

Depuis le 17 décembre dernier, il existe une mise en relation avec un policier, un gendarme, vingt-quatre heures sur vingt-quatre, sept jours sur sept, à travers le 17Cyber. Nous sommes passés de 280 000 parcours d'assistance toutes victimes confondues en 2023 à 420 000 parcours, soit une multiplication par deux depuis la mise en place du 17Cyber.

Les assujettis à NIS 2 sont du ressort de l'Anssi. En revanche, compte tenu du travail que nous avons effectué depuis de nombreuses années, nous pensons pouvoir intervenir à deux niveaux. Le premier niveau concerne la prévention et la sensibilisation. La directive fait à de nombreuses reprises référence à la nécessité d'actions de prévention. L'article 5 *bis* ajouté par le Sénat évoque la stratégie nationale et dans un de ses alinéas, il précise que des campagnes massives doivent être réalisées pour les différents assujettis. L'année dernière, le texte de la Commission supérieure du numérique et des postes (CSNP) sur NIS 2 recommandait aussi des actions de prévention.

Je propose ainsi qu'à l'article 5, nous puissions être identifiés comme le dispositif qui porte ces actions de prévention, en lien avec la stratégie nationale pour les années 2025-2030. Lors de vos auditions a souvent été évoqué le fait que la sensibilisation ne fonctionnait pas toujours ; mais ceci est dû à l'insuffisance de moyens dont nous disposons pour conduire des campagnes de sensibilisation sur le modèle de la sécurité routière, qui dispose d'un budget de 20 millions d'euros pour effectuer ses campagnes, depuis des dizaines d'années.

Ensuite, les prestataires labellisés constituent un début de réponse à une partie des problèmes sur la partie relative à la sécurisation et l'accompagnement des collectivités, des très petites, petites et moyennes entreprises (TPE-PME) dans les territoires qui seront assujettis à NIS 2. L'Anssi, qui est membre de notre comité de pilotage du label, a compris le rôle de nos prestataires experts cyber. Dans le cadre de groupes de travail avec l'Anssi, nous avons évalué le niveau de notre référentiel de labellisation et des référentiels techniques.

Le GIP est convaincu que grâce à une petite formation et avec l'aide complémentaire d'une structure qui pourrait être l'autorité nationale, nous serons en mesure d'identifier les prestataires. Pour le dire très simplement, il nous manque aujourd'hui des leviers pour fidéliser ces prestataires et nous sommes convaincus que NIS 2 constituerait une bonne opportunité pour leur permettre d'accompagner la sécurisation des structures qui en ont besoin, mais ne savent pas vers qui se tourner quand elles identifient cette problématique.

La directive précise par ailleurs que « *Les États membres peuvent mettre en place au niveau national un mécanisme de financement destiné à couvrir les dépenses nécessaires à l'exécution des tâches des entités publiques chargées de la cybersécurité dans l'État membre*

en vertu de la présente directive ». La CSNP recommandait déjà en octobre dernier d'allouer des crédits supplémentaires au secrétariat général de la défense et de la sécurité nationale (SGDSN) dans le cadre du programme 129 pour le projet de loi de finances (PLF) pour 2025, fléchés vers le GIP Acyma.

De fait, il y a urgence ; le budget 2025 du GIP a baissé de 120 000 euros par rapport à 2024 et il continuera à diminuer l'année prochaine puisque l'un de nos nouveaux membres nous quitte. Or chaque année, je ne dispose que 200 000 à 300 000 euros pour engager des actions de prévention et de communication. De plus, deux personnes qui étaient mises à disposition par nos membres sont reprises par leur structure d'origine. En outre, le dernier rapport de la Cour des comptes sur NIS 2 souligne la problématique de lisibilité, mais le 17Cyber, en tant que guichet unique, devrait précisément apporter une réponse à cette problématique. J'estime que nous ne coûtons pas beaucoup d'argent à l'État français, mais que les impacts que nous pouvons engendrer sont quand même assez importants.

Ces contraintes budgétaires nous ont de fait conduits à stopper la campagne de prévention que nous menions avec l'Institut national de la consommation (INC) sous le format des Conso Mag, qui nous permettaient de toucher des millions de téléspectateurs. De la même manière, nous avons été contraints de refuser de travailler avec le Comcyber-MI sur la version 2 de SenCy-Crise, alors que nous étions très heureux de contribuer à la première mouture. Je n'étais pas en mesure d'allouer une somme qui vous paraîtra dérisoire, 20 000 à 30 000 euros, nécessaire à l'évolution de notre plateforme pour l'hébergement de la nouvelle version.

S'agissant du filtre anti-arnaque, j'ai eu l'occasion de dresser un historique puisque nous avions rendez-vous la semaine dernière avec le cabinet de Clara Chappaz. En septembre 2022 s'est déroulée une première réunion de lancement, portée par le ministère du numérique, qui a confié à notre GIP le soin d'étudier la mise en place du filtre anti-arnaque. En trois mois, nous avons produit un rapport, qui s'inspirait notamment du modèle belge, extrêmement pragmatique et qui fonctionne. Ce rapport a été remis au ministre Jean-Noël Barrot en janvier 2023. Nous indiquions à cette occasion que le délai de développement serait d'une dizaine de mois à partir du moment où nous recevrions les financements.

Le ministre a pris l'engagement d'un démonstrateur pour la Coupe du monde de rugby à l'automne 2023, puis d'un filtre opérationnel pour les Jeux olympiques. Mais plusieurs mois se sont passés sans nouvelle du ministère. Ensuite, pendant une longue période, nous avons été confrontés à un problème avec la direction générale des entreprises (DGE) à Bercy sur la qualification juridique de la convention nous concernant, ces services nous orientant vers une convention de mandat, laquelle ne nous permet pas de sous-traiter. Or nous devions construire et héberger un *data center* dans un SecNumCloud. Finalement, la DGE a décidé de passer un marché de gré à gré de 10,8 millions d'euros en février 2024, auquel nous avons répondu initialement par une offre à 7,2 millions d'euros, en l'assortissant de réserves par rapport à certaines exigences de sécurité.

La DGE nous a ensuite indiqué qu'elle ne disposait que de 5,9 millions d'euros. Nous avons aligné notre offre sur ce montant, mais en réduisant nécessairement le périmètre du maintien en condition opérationnelle et de sécurité, de 36 mois à 30 mois. En juillet 2024, la DGE nous a notifié que la procédure était déclarée sans suite pour un « motif d'intérêt général » tenant à l'insuffisance des ressources financières de la direction bénéficiaire, c'est-à-dire elle-même.

En janvier 2025, la direction interministérielle du numérique (Dinum) a été mandatée pour établir une contre-proposition à notre proposition et nous a contactés. Nous nous sommes rencontrés, avant de tenir une réunion en mars avec la dizaine d'autorités administratives impliquées dans la mise en place ou l'exploitation du filtre. Finalement, vendredi dernier, au cabinet de Clara Chappaz, nous avons échangé d'une manière très constructive avec la Dinum.

De son côté, la DGE nous a annoncé qu'elle ne voulait pas mettre en place le filtre, mais nous nous en doutions déjà, puisque cette administration remet en cause les choix de son ministre, voire du président de la République, dès lors que le filtre anti-arnaque était un engagement du président pour sa réélection. Cela ne peut que poser question. Finalement, la ministre arbitrera entre, *a priori*, la Dinum et Acyma pour décider de la structure qui développera et opérera le filtre anti-arnaque.

M. Éric Bothorel, rapporteur général. Vous êtes les grands témoins de la nécessité de ce projet de loi. À ce stade, je tiens, à travers vous, à remercier les équipes qui œuvrent chaque jour, au quotidien et dans vos domaines respectifs, à la lutte contre la cybercriminalité. Vous êtes au cœur de la stratégie nationale de cybersécurité qui vient d'être validée. Je centrerai mon intervention et mes questions sur les propositions et préconisations qui vous concernent dans cette stratégie et qui pourraient être intégrées à ce projet de loi.

Madame Brousse, face à l'escalade des cybermenaces et à cette sophistication croissante des cybercrimes, le renforcement des capacités judiciaires françaises en matière de lutte contre la cybercriminalité constitue une nécessité impérieuse. L'enjeu crucial pour la France est double : améliorer l'efficacité des investigations judiciaires pour identifier et traduire en justice les cybercriminels et renforcer ces capacités à décourager toute forme de cybercriminalité en envoyant le message que la cybercriminalité ne sera pas impunie.

Les capacités d'investigation spécialisée des services compétents seront renforcées. Cela implique d'une part de doter le parquet spécialisé de Paris, compétent au niveau national, de ressources nécessaires pour mener des enquêtes complexes et aboutir à des condamnations. Je n'évoquerai pas la compétition qui pourrait exister entre le parquet national anticriminalité organisée (Pnaco) récemment créé et le J3, dont l'excellence et l'expertise sont reconnues de tous. Vous avez clairement souligné que les criminels ne s'exonèrent pas de mettre en œuvre des moyens cyber. Disposez-vous des moyens à la hauteur des ambitions en matière de cybercriminalité ? En outre, vous avez évoqué l'existence de magistrats référents cyber dans chaque parquet. Ce dispositif fonctionne-t-il ? Faut-il poursuivre son développement ?

Par ailleurs, le cadre légal judiciaire, en particulier le code de procédure pénale, devra également évoluer pour tenir compte des spécificités de la cybercriminalité. Parmi les adaptations nécessaires, différents éléments sont cités. Il s'agirait d'abord de la création d'un cadre pour conduire les opérations de démantèlement et de désinfection à distance des supports informatiques utilisés par des systèmes criminels à l'insu de leurs propriétaires légitimes, afin de faire cesser l'infraction. Il s'agirait ensuite de la création d'une infraction spécifique de fraude informatique. Cette infraction permettrait de sanctionner plus efficacement les actes de piratage informatique, d'intrusion dans les systèmes informatiques et de vol de données.

Il est également question de la modification de l'infraction de plateformes en ligne. Cette infraction actuellement limitée à la diffusion de contenus illicites, devrait être élargie

pour couvrir d'autres types d'infractions commises sur les plateformes en ligne, comme la cybercriminalité. Quel est votre point de vue sur ces évolutions du code de procédure pénale ?

Enfin, un débat a lieu concernant la fragilité du cadre juridique actuel sur la pratique du renseignement d'origine sources ouvertes (Osint), notamment pour des institutionnels comme vous. Est-il nécessaire de renforcer notre cadre légal pour la pratique de l'Osint, en établissant par exemple que certains acteurs soient plus légitimes que d'autres à le pratiquer ?

Mme Johanna Brousse. S'agissant des moyens alloués à la justice, nous espérons effectivement un renforcement des capacités de J3, à la fois en termes d'assistants spécialisés, d'attachés de justice, et de magistrats. Un sixième magistrat doit nous rejoindre en septembre ; nous espérons que cela sera effectif. Il est certain qu'il faut continuer à monter en puissance si nous voulons pouvoir nous donner les moyens de répondre à cette menace.

Il convient d'être extrêmement vigilant concernant le périmètre de la section de lutte contre la cybercriminalité. Nous défendons l'idée qu'une section cyber ait la primauté sur le Pnaco ou sur d'autres juridictions sur ce qui doit être centralisé ou non au niveau national. En effet, il ne faut pas que la centralisation de l'information s'effrite. La section cyber doit pouvoir continuer à disposer en priorité de ce droit de se saisir des dossiers cyber. La centralisation de l'information nous permet de créer des liens, de collecter des éléments et d'être efficaces.

S'agissant des nouvelles infractions suggérées, il est évident que notre arsenal législatif devra se renforcer pour pouvoir s'adapter aux nouvelles techniques émergentes. Aujourd'hui, plusieurs dossiers ont été classés ou ont même fait l'objet de relaxe, en raison d'un vide juridique.

Laissez-moi l'illustrer par un exemple très concret. Certains individus ont profité d'une vulnérabilité sur un site et ont rempli leur compte de cryptomonnaies simplement en cliquant. Ils sont devenus millionnaires. Ils ne pouvaient pas être poursuivis pour vol parce qu'il ne s'agissait pas d'une soustraction frauduleuse. Le ministère de la justice nous a incités à les poursuivre pour escroquerie, mais il n'y a pas eu de manœuvre frauduleuse. Ils ont donc obtenu une relaxe en première instance, puis en appel.

Face à ce vide juridique, il serait sans doute opportun de réfléchir à la création d'une nouvelle infraction, la fraude informatique. Elle existe déjà dans d'autres pays et permettrait d'étoffer utilement l'arsenal législatif français. Le délit d'administration de plateforme a été créé en 2023 dans la loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) et nous a par exemple permis de faire fermer la plateforme Coco.gg. Le potentiel de cette infraction pourrait effectivement être renforcé si le texte était écrit de manière plus englobante, ce qui nous permettrait également de lutter plus efficacement contre les ingérences numériques étrangères.

De très grands efforts ont déjà été accomplis sur ce sujet, notamment avec la proposition de loi de Sacha Houlié sur la création d'une circonstance aggravante d'ingérence étrangère, mais il est possible d'aller encore plus loin. Plus globalement, il faudra réfléchir à certaines techniques spéciales d'enquête. Nous nous appuyons un texte générique, sur la perquisition et la captation pour les mettre en œuvre, mais nous ne sommes pas certains que les techniques utilisées rentrent dans ce cadre.

S’agissant de l’Osint, concrètement, nous utilisons ce que nous trouvons en sources ouvertes sur internet pour documenter nos procédures. Des propositions émergent en la matière, dans la mesure où des acteurs privés, mais aussi des enquêteurs peuvent se sentir en insécurité dans l’utilisation des *leaks*. Pour notre part, nous considérons que nous pouvons les employer en procédure. Peut-être faut-il en passer par un texte de loi pour clarifier la situation et rassurer l’ensemble de l’écosystème cyber. Mais la question se pose également en termes de compétitivité française. Certaines grandes entreprises m’indiquent ainsi qu’elles préfèrent acheter des solutions étrangères, qui ne se posent pas la question de savoir si les données ont été piratées ou non. Les entreprises françaises essayent de jouer le jeu, mais elles ne savent pas si elles ont le droit de récupérer les *leaks*. En conséquence, elles hésitent à agir de la sorte et me posent la question. Je leur réponds que je pratique de cette manière dans mes enquêtes, mais que je n’ai pas aujourd’hui l’autorisation de leur dire si elles ont la capacité de le faire, car cela peut correspondre à du recel de délit.

M. Christophe Husson. Ce point fait l’objet de nombreuses réflexions du ministère de l’intérieur, dans le cadre de l’entité CIRSO-MI, le centre des investigations et des recherches en source ouverte du ministère de l’intérieur. Elle rassemble l’ensemble des services de police et de gendarmerie, mais également les services de renseignement. Ces entités s’interrogent en effet sur les *leaks* qui seraient utilisés dans le cadre de l’enquête judiciaire ou du renseignement. Le ministère de l’intérieur a réfléchi à un texte qui pourrait être proposé dans ce cadre, mais uniquement sur son propre périmètre du ministère de l’intérieur.

Mme Anne Le Hénanff, rapporteure. Je vous ai écouté attentivement. Je rappelle en préambule qu’il ne s’agit pas non plus de surtransposer la directive. Ensuite, à la lumière des constats que vous dressez, j’observe que les moyens qui seront accordés seront essentiels dans la transposition de NIS 2, qu’il s’agisse des moyens financiers ou des moyens humains. Je déplore par ailleurs que 80 % des décrets d’application de la loi visant à sécuriser et à réguler l’espace numérique (Sren) que nous avons voté il y a peu, n’aient toujours pas été publiés.

Monsieur Notin, comment envisagez-vous l’impact direct, opérationnel sur vos sollicitations lorsque la loi de transposition de NIS 2 sera promulguée ? En avez-vous estimé le nombre ? Disposez-vous de suffisamment de moyens pour y répondre ? Visiblement, cela ne semble pas être le cas.

Je souhaite également évoquer les collectivités territoriales. L’Anssi a proposé un seuil de 30 000 habitants dans le cadre de NIS 2. Quel est votre avis à ce sujet ? Dans certains cas de figure, il apparaît pertinent, parce qu’il faut bien établir une limite, mais dans d’autres, il semble que cela n’ait pas de sens. Certaines communes n’ont pas de DSI, et encore moins de responsable de la sécurité des systèmes d’information (RSSI). Les systèmes d’information sont interconnectés avec ceux de l’intercommunalité. Certaines communes détiennent des compétences en matière d’eau, essentielles pour NIS 2, mais comportent moins de 10 000 habitants. J’aimerais connaître votre point de vue à ce sujet, ainsi que sur la chaîne des sous-traitants, dans la mesure où NIS 2 sera diffusée bien au-delà des 15 000 entités ciblées.

Madame Brousse, je vous remercie pour votre présentation. J’aimerais que vous puissiez également nous donner votre avis sur le hacker « éthique » qui, s’il n’est pas évoqué noir sur blanc dans le texte, figure en toile de fond. Cette notion a-t-elle un sens ? Je rappelle ainsi que le considérant 60 de la directive NIS 2 indique que les États membres doivent

protéger les hackers éthiques sans les citer nommément. Que pensez-vous du cadre juridique existant en la matière ? Devrons-nous l'approfondir ?

Enfin, vous avez souligné que la voie judiciaire devient parfois une voie diplomatique, lorsque vous transmettez une adresse IP à un État étranger. En quoi est-ce efficace, concrètement ? Cela contribue-t-il à faire cesser les attaques ?

Mme Sabine Thillaye (Dem). La Cour des comptes a évoqué la confusion des écosystèmes cyber, la multiplicité des acteurs étatiques impliqués sans qu'il n'existe pour autant de véritable gouvernance unifiée. Pensez-vous qu'une telle gouvernance est souhaitable ?

Ensuite, nous comprenons bien que les financements sont le nerf de la guerre. Que se passera-t-il si ceux-ci ne peuvent être obtenus ? Par ailleurs, en tant que parlementaires, comment pouvons-nous mieux sensibiliser dans nos circonscriptions, dont certaines sont très rurales ?

Mme Laetitia Saint-Paul (HOR). Général, je m'interroge sur les enjeux de vidéosurveillance et de reconnaissance faciale. Dans quelles mesures les freins juridiques existant actuellement sur l'utilisation de ces moyens affectent notre efficacité pour arrêter les criminels ? Vous avez parlé du blanchiment des cryptomonnaies. Pourriez-vous détailler de quelle manière ce blanchiment rejaillit dans l'économie réelle ? J'ajoute qu'un rapport sénatorial traite de la place de l'or dans le blanchiment d'argent. Par ailleurs, pourriez-vous nous faire parvenir votre rapport sur l'état de la menace quand il sera publié ? S'agissant du partage de l'information, vous étiez plutôt rassurants, mais n'existe-t-il pas un émiettement des acteurs ? Ce partage fonctionne-t-il bien avec les armées, la DGSI, le SGDSN ?

Madame la procureure, je m'intéresse aux liens entre criminalité étatique et non étatique. Avez-vous des exemples à nous soumettre à ce titre ? Je souhaiterais également en savoir plus sur les liens entre les différentes criminalités, les enjeux de radicalisation en matière de terrorisme. Les mêmes outils sont-ils utilisés par les différents types de criminalité ? Ensuite, j'observe que l'époque n'est sans doute pas à la création de nouvelles agences, mais pourriez-vous revenir sur votre proposition d'agence technique ou nous faire parvenir une note à son propos ? Enfin, quelles sont vos suggestions pour nous, législateurs ?

M. Jérôme Notin. Les différents rapports existants en matière de cybersécurité, qu'ils soient parlementaires ou émanant de la Cour des comptes, font état d'un émiettement des dispositifs, préjudiciable à leur bonne compréhension sur le terrain. Les victimes ne perçoivent pas les différences entre la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos), le service Perceval et le traitement harmonisé des enquêtes et signalements pour les e-escroqueries (Thesee). À la demande du président de la République, nous avons travaillé collectivement à la mise en place du 17cyber.gouv.fr, qui a vocation à orienter la victime vers tous les dispositifs étatiques, les prestataires historiques référencés et labellisés cybermalveillance.gouv.fr. L'activité de cybercriminalité ne va cesser de croître et nous militons pour faire du 17Cyber la solution visible.

Madame la rapporteure, l'impact de NIS 2 sur le GIP dépendra en grande partie des métiers que nous exerçons. D'après ce que j'en comprends, 0,5 % des entreprises et des collectivités seront concernées par NIS 2, soit une masse assez faible par rapport à la masse que nous traitons quotidiennement sur la partie assistance. S'agissant de la prévention, même

si l'Anssi sera leur point de contact, nous serons ravis de fournir aux opérateurs d'importance vitale nos supports de sensibilisation.

Ensuite, comme je l'ai indiqué un peu plus tôt, nous éprouvons des difficultés à fidéliser les prestataires labellisés. Ils doivent consacrer du temps aux procédures que nous leur demandons, à nous transmettre les rapports d'incidents, les rapports de sécurisation. Les candidats doivent également verser 800 euros à l'Association française de normalisation (Afnor). À cet égard, France Cybersecurity labellise un éditeur de solutions cyber, mais il ne garantit pas que son détenteur soit en capacité d'évaluer la maturité cyber d'une structure, publique ou privée, et d'émettre des recommandations.

La plupart des RSSI travaillant dans les structures privées consacrent beaucoup de temps à remplir des tableurs pour démontrer leur conformité à des règles que chaque donneur d'ordre, public ou privé, établit lui-même. NIS 2 sera à ce titre extrêmement positif, puisque grâce à l'Anssi, il existera un référentiel technique commun sur lequel chacun pourra s'appuyer et des structures conformes à NIS 2 seront en mesure d'accompagner les acteurs.

Mme Johanna Brousse. Madame la rapporteure, vous m'avez interrogée sur l'intérêt d'utiliser le canal judiciaire comme une voie diplomatique. Quand nous signifions à un pays que nous avons mis en lumière son attaque et notamment l'utilisation de telle ou telle adresse IP, telle ou telle infrastructure, il s'aperçoit qu'il n'est plus du tout furtif et anonyme. Cela impliquera pour lui de devoir redéployer de nouvelles infrastructures pour pouvoir mener d'autres attaques. Il devra donc se réorganiser, ce qui lui fera perdre du temps et des moyens.

Ensuite, il existe au niveau de l'Anssi un dispositif très utile qui permet à des hackers éthiques de réaliser des signalements, ce qui dispense l'Agence de procéder à un article 40 ou à un signalement au parquet. Néanmoins, si nous sommes saisis par une entité qui a été hackée par un hackeur éthique, même agissant pour de bonnes raisons, à l'instar d'un lanceur d'alerte, nous serons malgré tout obligés d'ouvrir une enquête et il n'est pas exclu que la victime se constitue partie civile auprès d'un juge d'instruction ou effectue une citation directe. Dès lors, il n'existe pas de véritable protection en tant que telle. Si l'on voulait pousser plus loin la protection des lanceurs d'alerte, il faudrait stipuler que ce hacking « éthique » constitue une cause d'exonération de la responsabilité pénale, ce qui n'est pas le cas à l'heure actuelle, même si le parquet reste maître de l'opportunité des poursuites.

Néanmoins, pour en avoir discuté récemment à Anssi, je sais que les acteurs de l'écosystème sont parfois réticents à signaler un événement, car ils redoutent d'encourir une responsabilité. Dès lors, il conviendrait peut-être de clarifier le dispositif, ce que je laisse à votre appréciation. Les personnes qui effectueraient des signalements légitimes devraient peut-être pouvoir disposer d'un cadre extrêmement protecteur et être incités à le faire.

Ensuite, nous constatons effectivement une réelle porosité. Les cybercriminels sont avant tout des mercenaires qui peuvent se mettre au service de certains États afin de mener à bien leurs actions. Régulièrement, des acteurs du rançongiciel travaillent directement pour des États, dans la mesure où le but du *ransomware* consiste certes à gagner de l'argent et à financer certaines opérations, mais aussi à entraver l'économie d'un pays.

Par ailleurs, le parquet national antiterroriste dispose d'un référent cyber avec lequel nous dialoguons. Des questions demeurent en suspens, néanmoins. Par exemple, si demain une cyberattaque de nature terroriste occasionne des morts, quelle sera la section chargée du

dossier ? Il existe certes un plan de gestion de crise qui nous permet dans une certaine mesure de répondre à cette question. Mais peut-être conviendrait-il d'aller plus loin et de prévoir une possibilité de co-saisine de juridictions spécialisées, ce qui n'est pas le cas aujourd'hui.

Enfin, vous m'avez questionnée sur la proposition de création d'une agence technique pour le ministère de la justice et le ministère de l'intérieur. Différentes branches, ANTENJ et le SNCJ, existent aujourd'hui et effectuent un travail remarquable. Leur regroupement au sein d'une même agence dotée d'une mission globale et plus étendue permettrait de gagner en efficacité. Je pourrais vous transmettre un certain nombre d'éléments à ce sujet.

M. Christophe Husson. Depuis 2022, nous avons effectué 2 029 diagnostics sur les collectivités territoriales, dont trente étaient ultramarines et une sur onze avait été victime de rançongiciel. La plus petite était la mairie d'une commune de 200 habitants. Le dispositif a été étendu au PME ou aux ETI, qui s'est traduit par 338 diagnostics (dont neuf sur des entreprises ultramarines), dont une sur six avait été victime d'attaque par rançongiciel. Enfin, soixante-quatorze diagnostics ont été réalisés sur des hôpitaux en zone gendarmerie, dont un sur six a été victime d'un rançongiciel. Ces chiffres montrent bien qu'aujourd'hui, tout le monde est vulnérable, quelles que soient la structure et sa taille.

S'agissant de la gouvernance, notre entité est jeune au sein du ministère de l'intérieur et l'objectif consiste bien à assurer une meilleure coordination avec les services enquêteurs de la police et de la gendarmerie. Je partage avec Jérôme Notin l'idée que le 17Cyber doit constituer le point d'entrée, lisible pour tous.

Le dispositif MonAideCyber de l'Anssi a été conçu comme une communauté d'aidants dans les territoires, qui pourra mener des diagnostics. Il convient de promouvoir cette communauté : plus nous disposerons de personnes en mesure de mener un diagnostic MonAideCyber dans les territoires, plus les modalités de prévention seront efficaces.

S'agissant du blanchiment des cryptomonnaies, le Comcyber de la gendarmerie a démantelé il y a quelque temps la plateforme Bitzlato et a saisi près de 20 millions d'euros en cryptomonnaies. Cette expérience est utile pour le travail de formation que nous menons, notamment au sein de notre centre de formation cyber de Lille. En effet, nous ne formons pas uniquement des spécialistes au niveau central à l'Office anti-cybercriminalité, à l'Unité nationale cyber ou la Brigade de lutte contre la cybercriminalité ; nous formons également des militaires de la gendarmerie et des fonctionnaires de la police nationale dans les territoires. En effet, nous avons besoin de personnes qui maîtrisent les sujets de la traçabilité des cryptoactifs, au plus proche des territoires en métropole et en outre-mer. De fait, ayant échangé à de nombreuses reprises avec des procureurs dans les territoires, je confirme qu'il existe aujourd'hui un véritable besoin de proximité.

Le rapport sur l'état de la menace est public. Il sera publié et disponible sur le site du ministère de l'intérieur, mais je vous le transmettrai dès sa publication. S'agissant du partage de l'information et en particulier le renseignement d'intérêt cyber avec les autres acteurs, le Comcyber-MI est connecté à l'InterCERT. Ici, le partage de l'information intervient en matière de captation de données et, potentiellement, de leur transmission.

J'ajoute que nos relations avec le Comcyber des armées sont très régulières. Le Comcyber-MI dispose ainsi d'un officier de liaison au sein du Comcyber des armées. Des rencontres bilatérales interviennent par ailleurs tous les six mois avec mon homologue au sein

du ministère des armées. Nos équipes échangent très régulièrement sur le renseignement d'intérêt cyber. Nous disposons au Comcyber-MI d'une plateforme de Cyber Threat Intelligence (CTI) et nous éclairons le Comcyber des armées, qui conduit un projet sur le sujet. Nous travaillons évidemment de manière commune sur les difficultés et les pratiques et l'échange de l'information *stricto sensu*.

Enfin, une question a porté sur la reconnaissance faciale. À ce titre, je rejoins les propos initiaux qui ont concerné l'accès à la donnée. Aujourd'hui, la société est particulièrement numérisée ; nous disposons d'images vidéo statiques ou dynamiques. Dans le cadre d'une enquête judiciaire, une reconnaissance faciale pourra toujours constituer un élément utile pour les enquêteurs, notamment par son exploitation à l'aide de l'intelligence artificielle. Naturellement, ceci doit toujours intervenir dans un cadre légal adapté et garant de nos principes démocratiques.

M. le président Philippe Latombe. Je vous remercie de votre présence et d'avoir répondu aux questions.

La commission se réunira début septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer à notre réflexion et produire un texte le plus lisible et efficace possible. L'objectif consiste en effet à éviter des effets de bord.

La séance est levée à dix-huit heures dix.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du mercredi 25 juin 2025 à 16 h 30

Présents. - M. Éric Bothorel, Mme Amélia Lakrafi, M. Philippe Latombe, Mme Anne Le Hénanff, Mme Laetitia Saint-Paul, Mme Sabine Thillaye

Excusé. - Mme Marietta Karamanli