N° 2415

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 14 novembre 2019.

RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA COMMISSION DES AFFAIRES EUROPÉENNES [1]

*sur l'***avenir** *de la* **cybersécurité européenne**

ET PRÉSENTÉ

PAR M. ÉRIC BOTHOREL,
Député

(1) La composition de la commission figure au verso de la présente page.

La Commission des affaires européennes est composée de : Mme Sabine THILLAYE, *présidente* ; MM. Pieyre-Alexandre ANGLADE, Jean-Louis BOURLANGES, Bernard DEFLESSELLES, Mme Liliana TANGUY, *vice-présidents* ; M. André CHASSAIGNE, Mme Marietta KARAMANLI, M. Christophe NAEGELEN, Mme Danièle OBONO, *secrétaires ;* MM. Damien ABAD, Patrice ANATO, Mme Aude BONO-VANDORME, MM. Éric BOTHOREL, Vincent BRU, Mmes Fannette CHARVIER, Yolaine de COURSON, Typhanie DEGOIS, Marguerite DEPREZ-AUDEBERT, M. Benjamin DIRX, Mmes Coralie DUBOST, Françoise DUMAS, Frédérique DUMAS, MM. Pierre-Henri DUMONT, Alexandre FRESCHI, Bruno FUCHS, Mmes Valérie GOMEZ-BASSAC, Carole GRANDJEAN, Christine HENNION, MM. Michel HERBILLON, Alexandre HOLROYD, Mme Caroline JANVIER, MM. Christophe JERRETIE, Jérôme LAMBERT, Mmes Constance Le GRIP, Nicole Le PEIH, MM. Jean-Claude LECLABART, David LORION, Ludovic MENDES, Thierry MICHELS, Xavier PALUSZKIEWICZ, Damien PICHEREAU, Jean-Pierre PONT, Joaquim PUEYO, Didier QUENTIN, Mme Maina SAGE, MM. Benoit SIMIAN, Éric STRAUMANN, Mme Michèle TABAROT.

SOMMAIRE

Pages

INTRODUCTION 7

I. LA LENTE MONTÉE EN PUISSANCE DES ENJEUX EUROPÉENS DE LA CYBERSÉCURITÉ 9

A. LES ENJEUX SOUS-ÉVALUÉS DE LA CYBERSÉCURITÉ 9

1. Des menaces diffuses et peu visibles pour le grand public 9

a. La cybersécurité : une notion aux contours souvent imprécis 9

b. Une typologie de menaces pour la cybersécurité qui ne cesse de s'enrichir 10

c. Le cyberespace : particularités 12

2. Les atteintes à la cybersécurité ont pourtant des conséquences sécuritaires et économiques de plus en plus préoccupantes 13

a. L'évaluation incertaine du nombre d'attaques 13

b. La difficile constitution d'un indice de cybersécurité 14

c. Un paysage de menaces amené à se densifier 15

d. Des menaces en mutation et qui brouillent encore un peu plus les limites entre guerre et paix : la montée des menaces hybrides 17

B. UN FOISONNEMENT D'INSTITUTIONS INTERNATIONALES SAISIES DES ENJEUX DE CYBERSÉCURITÉ 18

1. L'ONU 18

2. L'OTAN 19

3. Interpol 20

4. Le Conseil de l'Europe 20

II. L'ENISA, UNE AGENCE EUROPÉENNE RENFORCÉE AU SERVICE D'UNE CYBERSÉCURITÉ PLUS INTÉGRÉE 22

A. LE PAYSAGE TRÈS ÉCLATÉ DE LA CYBERSÉCURITÉ EUROPÉENNE 22

1. Premières esquisses stratégiques de l'Union européenne 22

2. Une action de cybersécurité dispersée 23

a. Sécurité des réseaux et de l'information 23

i. La création de l'ENISA 23

ii. La création d'un centre d'intervention d'urgence....23
b. Sécurité intérieure : Centre européen de lutte contre la cybercriminalité.... 24
c. Recherche et diplomatie 24
i. Le Service européen pour l'action extérieure 24
ii. L'Institut européen pour les études de sécurité....25
B. UNE STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ QUI TEND À SE CRISTALLISER 26
1. Le cadre stratégique de 2013 et l'adoption de la directive SRI : concilier volet sécuritaire et volet industriel 26
2. La directive SRI : amorcer une architecture européenne de la cybersécurité plus intégrée pour les États membres....28
a. Une volonté de clarification des acteurs et de leurs missions.... 28
b. Des modèles nationaux qui restent très divers 30
c. Les conclusions mitigées de la Commission sur l'application de la directive SRI33
C. L'ENISA PÉRENNISÉE DEVRA CONTRIBUER À RENFORCER L'ARCHITECTURE EUROPÉENNE DE LA CYBERSÉCURITÉ..... 34
1. L'ENISA : une agence pour diffuser la culture de la cybersécurité et assister les États membres....34
2. Certaines faiblesses justifiaient une révision du rôle de l'agence....35
3. La réforme de l'ENISA s'inscrit dans une relance plus globale de la stratégie de cybersécurité de l'Union 36
4. L'ENISA doit devenir un organe de coordination et de soutien aux missions corrélées à ses moyens 37
5. L'ENISA doit être une agence facilitatrice, mais ne peut ni ne doit devenir l'organe supranational de cybersécurité de l'Union....39
6. Il sera nécessaire de clarifier les liens entre l'ENISA et le futur Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité....40
III. LA CERTIFICATION EUROPÉENNE DOIT DÉFINIR UN STANDARD PERMETTANT DE CONCILIER SÉCURITÉ ET PROSPÉRITÉ 41
A. LA CERTIFICATION EUROPÉENNE DOIT COMPOSER AVEC DES CERTIFICATIONS QUI EXISTENT DÉJÀ AUX NIVEAUX NATIONAL ET INTERNATIONAL..... 41
1. La certification existe déjà dans des versions nationales....41
2. Des standards internationaux préexistent également 43
B. SUR LA BASE DE CES ACQUIS, LA CERTIFICATION DOIT DEVENIR UN AVANTAGE COMPARATIF POUR LA CYBERSÉCURITÉ EUROPÉENNE 44
1. Le système prévu par le règlement 44
a. Le règlement européen prévoit une certification facultative et sur trois niveaux :44
b. Certains aspects du rôle de la Commission européenne et de l'ENISA dans la certification seront à préciser dans la pratique.... 44

2. Les points d'attention dans la mise en œuvre prochaine du règlement 46
a. La multiplication des enceintes..... 46
b. La prise en compte des schémas existants 47
c. La question du périmètre des schémas de certification de sécurité 49
d. La difficile conciliation entre réactivité et stabilité des schémas de certification49

TRAVAUX DE LA COMMISSION..... 51

I. TABLE RONDE SUR LA CYBERSÉCURITÉ EN PRÉSENCE DE M. JUHAN LEPASSAAR, DIRECTEUR EXÉCUTIF DE L'ENISA, M. STEVE PURSER, DIRECTEUR DES OPÉRATIONS DE L'ENISA, M. JEAN-BAPTISTE DEMAISON, PRÉSIDENT DU CONSEIL D'ADMINISTRATION DE L'ENISA, ET M. CYRIL CUVILLIER, SOUS-DIRECTEUR ADJOINT DE LA STRATÉGIE DE L'ANSSI..... 51

II. PRÉSENTATION DU RAPPORT D'INFORMATION 63

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR69

INTRODUCTION

Mesdames, Messieurs,

Selon la Commission européenne, 80 % des entreprises européennes connaissent au moins un « incident de cybersécurité » par an. Dans certains États membres de l'Union, jusqu'à 50 % des crimes perpétrés interviendraient dans le champ de la cybercriminalité. Les cybermenaces peuvent prendre des formes multiples, comme en rend compte le rapport sur l'état de la menace liée au numérique en 2019 du Ministère de l'intérieur français : *typosquatting*, rançongiciels, chevaux de Troie d'administration à distance, *cryptojacking* et autres *botnets*. La liste est longue et ne cesse de s'allonger.

De plus, la multiplication des objets connectés et des services en ligne sera renforcée par de futurs réseaux, techniquement plus performants, mais aussi plus vulnérables en termes de sécurité La cybersécurité est donc non seulement un enjeu actuel et souvent sous-estimé, mais devrait également devenir un sujet majeur pour les prochaines années dans une société toujours plus numérisée.

La France occupe une place tout à fait spécifique sur le terrain de la cybersécurité en Europe, car elle dispose d'une expertise ancienne et reconnue, incarnée par son agence nationale, l'ANSSI. Mais la force d'une chaîne se mesurant à l'aune de son maillon le plus faible, une coopération de qualité entre les autorités nationales de l'Union européenne responsables apparaît déterminante. Jusqu'à récemment, l'existence même de telles autorités n'était pas acquise dans tous les États membres, et lorsqu'elles existaient, toutes n'avaient pas la puissance de frappe de l'agence française.

La législation européenne récente (la directive SRI et l'Acte de cybersécurité) s'est donc employé à remédier à cela, en cherchant à concilier le respect de la souveraineté des États membres et une collaboration européenne efficace sous la houlette d'une agence dédiée, l'ENISA.

L'enjeu majeur de la cybersécurité doit évidemment être considéré sous l'angle de la sécurité et de la défense des intérêts à la fois nationaux et européens. Mais sa dimension économique ne doit pas être négligée : la cybersécurité peut aussi être source de prospérité, et l'Union européenne a tout à gagner à présenter un front uni pour affronter la concurrence mondiale et établir des standards de référence.

C’est pourquoi le rapport porte sur les deux volets de l’Acte de cybersécurité : sécuritaire et opérationnel avec le renforcement de l’ENISA, et plus économique avec l’introduction d’un système européen de certification pour la cybersécurité.

À partir des observations recueillies lors des auditions et de l’étude des textes adoptés dans le cadre de l’Acte de cybersécurité européen, le rapport d’information se propose d’abord, de présenter l’émergence des grands enjeux de la cybersécurité en Europe ces dernières années. L’élaboration de réponses institutionnelles européennes coordonnées se heurte en effet à deux écueils : le foisonnement des institutions internationales et la difficulté à mesurer les atteintes à la cybersécurité.

Une Agence européenne de la cybersécurité renforcée pourra contribuer à rationaliser l’architecture de la cybersécurité européenne, mais les contours de son action devront être bien définis. L’ENISA ne doit pas devenir l’organe supranational de la cybersécurité en Europe, mais peut et doit assurer un rôle utile de coordination et de mobilisation des compétences nationales.

La diversité des instances nationales nous conduit à proposer que soit désignée dans chaque État membre une personnalité politique de référence, susceptible d’offrir une meilleure visibilité aux enjeux de cybersécurité. Il pourrait s’agir en France de créer un ministère de plein exercice, qui permettrait une véritable incarnation politique des problématiques de cybersécurité, tant sur le volet sécuritaire qu’industriel.

Le rapport examine également les modalités de la certification européenne créée par le nouveau règlement : si celle-ci peut constituer un avantage comparatif essentiel pour l’Union, elle n’emporte pas moins certaines difficultés. Véritable opportunité de croissance pour l’Europe sur le marché de la cybersécurité, la certification doit favoriser la convergence vers les plus hautes exigences.

La mise en œuvre de l’Acte de cybersécurité offre à l’Union européenne l’occasion historique de répéter l’affirmation d’un standard, tel que celui établi par le Règlement général de protection des données personnelles (RGPD. Il lui faut pour cela capitaliser sur les réussites de ses meilleurs acteurs, et réussir à faire converger secteurs public et privé dans la promotion de l’intérêt européen.

C’est le sens du modèle que ce rapport vise à défendre, à un moment charnière de la vie de l’Union européenne, avec l’arrivée récente des nouveaux députés au Parlement européen et la prise de fonction prochaine de la Commission européenne.

I. LA LENTE MONTÉE EN PUISSANCE DES ENJEUX EUROPÉENS DE LA CYBERSÉCURITÉ

A. LES ENJEUX SOUS-ÉVALUÉS DE LA CYBERSÉCURITÉ

1. Des menaces diffuses et peu visibles pour le grand public

a. La cybersécurité : une notion aux contours souvent imprécis

Depuis la fin du vingtième siècle, le développement de la société de l'information a fait émerger des enjeux inédits liés aux nouveaux modes de transmission des données publiques et privées, dont la définition apparaît encore problématique. Ainsi, le terme de cybersécurité est-il parfois employé à tort pour qualifier la cyberdéfense, et vice versa.

Pourtant, la notion de cybersécurité renvoie à une définition bien plus large que la cyberdéfense, qui n'est que l'un des moyens pour parvenir à la cybersécurité. Le Ministère des affaires étrangères définit la cybersécurité comme « *l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre les nouvelles pratiques destructrices qui se développent dans le cyberespace : utilisations criminelles d'internet (cybercriminalité), espionnage à visée politique ou économique, attaques contre les infrastructures critiques (transport, énergie, communication…) à des fins de sabotage*. » [(1)] Et selon le glossaire en ligne de l'Agence nationale de sécurité des systèmes d'information française (ANSSI), la cybersécurité désigne *« l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ».* [(2)] Que l'on insiste sur les moyens pour y parvenir ou sur la finalité visée, la cybersécurité serait donc un état de stabilité et de vulnérabilité minimales face aux potentielles menaces qui mettent en cause le bon fonctionnement des systèmes d'information.

Le système d'information est ici entendu à la fois comme un support de ressources techniques (s'appuyant sur le développement continu des technologies informatiques) et une structure organisationnelle propre à chaque entité (avec ses règles de répartition des pouvoirs et des compétences). Au-delà de ces définitions techniques, l'omniprésence de ces systèmes d'information dans de nombreuses organisations (entreprises, administrations…) est de plus en plus visible et la masse de données soumise à des traitements automatisés ne fait qu'augmenter.

---

(1) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/

(2) https://www.ssi.gouv.fr/particulier/glossaire/c/

Toutes ces structures communiquent et interagissent par le biais de réseaux, dont le réseau internet est évidemment le plus connu. Ces réseaux peuvent véhiculer des menaces de sécurité aux conséquences bien réelles pour les usagers, bien qu'ils n'en aient pas toujours pleinement conscience.

En effet, la menace numérique apparaît souvent abstraite, voire invisible pour nos concitoyens, alors que les conséquences des atteintes à la cybersécurité sont pourtant bien concrètes. L'exemple de Jesse McGraw [(1)], arrêté en juin 2009 au Texas par le FBI, est ainsi révélateur : en contaminant les ordinateurs d'une clinique, M. McGraw était parvenu à prendre le contrôle des dossiers des patients et du système de climatisation de l'hôpital, avec des conséquences potentiellement critiques pour les patients traités. Un tel exemple met bien en lumière le spectre important des menaces à l'encontre de la cybersécurité : loin de se limiter aux arnaques en ligne ou aux usurpations d'identité, les atteintes à notre sécurité numérique peuvent véritablement recouvrir des enjeux de vie ou de mort pour les citoyens.

Votre rapporteur estime qu'un important travail de sensibilisation reste à mener de la part de toutes les autorités concernées pour que le grand public se saisisse de ces enjeux et en prenne la pleine mesure. L'acquisition d'un socle minimal de connaissances sur la cybersécurité par les usagers apparaît d'autant plus nécessaire que les menaces existantes ne cessent de se diversifier et de se transformer, rendant leur compréhension et leur évaluation de plus en plus complexes.

b. Une typologie de menaces pour la cybersécurité qui ne cesse de s'enrichir

Les cybermenaces peuvent prendre des formes multiples et leurs auteurs ne cessent de les faire évoluer à mesure que des parades sont trouvées pour les contrer. Ces menaces peuvent viser des individus ou des institutions, avoir des objectifs criminels ou politiques, être perpétrées en grand nombre ou de façon ciblée, à une échelle internationale ou non. Le caractère protéiforme des attaques se conjugue à la difficulté de leur détection pour rendre l'évaluation aussi difficile que la prise de conscience par le grand public des enjeux sous-jacents.

Le rapport sur l'état de la menace liée au numérique en 2019 du Ministère de l'intérieur [(2)] rend compte de cette diversité et présente les phénomènes d'atteinte à la cybersécurité selon qu'il s'agit d'attaques visant les systèmes d'information ou que ces phénomènes recouvrent des utilisations d'internet à des fins criminelles.

---

(1) Cité par Nicolas Arpagian, dans son ouvrage « Cybersécurité », éditions Que sais-je, 2018.

(2) État de la menace liée au numérique en 2019, Rapport n° 3, mai 2019, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces.

Dans le premier cas, on trouve les dénis de services (saturation de sites internet qui empêchent leur fonctionnement), les défigurations de sites, les détournements ou vols de données : ce sont ici les structures mêmes de communication qui sont attaquées. Dans le second cas, le Ministère de l'intérieur liste une série de phénomènes délictueux ou criminels, allant des escroqueries au terrorisme en passant par les extorsions.

Le rapport revient également sur les moyens utilisés pour ces actions répréhensibles : exploitation des vulnérabilités des systèmes [(1)], *typosquatting* [(2)] ou bien logiciels malveillants, avec là aussi une large palette (rançongiciels [(3)], chevaux de Troie d'administration à distance [(4)], *cryptojacking* [(5)] et autres *botnets* [(6)]).

Ces menaces multiformes, aux vecteurs variés, reposent sur une grande diversité de motivations, qu'elles soient financières avec les escroqueries, la captation des données bancaires ou le *cryptomining*, économiques avec certaines formes d'espionnage industriel, ou politiques par le biais des *hacktivistes* ou des attaques à des fins de terrorisme. En outre, sous l'effet de la cyberinfluence et des manipulations des informations [(7)], ce sont les fondements de la démocratie elle-même qui peuvent s'en trouver sapés.

On le voit, et votre rapporteur souhaiterait le souligner : la cybersécurité recouvre des enjeux très larges et de natures différentes (civils et militaires, politiques et économiques), ce qui explique en partie la complexité des actions visant à la garantir. À l'instar des menaces similaires qui lui font écho dans le « monde réel », la cybersécurité sollicite de nombreux acteurs et institutions, et engage des problématiques qui concernent aussi bien les citoyens et les entreprises que les États et administrations publiques, mêlant protection des droits individuels, sécurité pour les acteurs économiques et enjeux de souveraineté.

---

(1) Mode fréquent de compromission des systèmes n'exigeant pas un haut niveau de technicité.

(2) Le typosquatting consiste en l'usurpation par une modification légère du nom d'une institution, marque ou personne dans le but d'escroquer les victimes.

(3) Il s'agit du blocage par un virus de l'accès au système ou aux données, auquel seul le paiement d'une rançon permet de mettre fin.

(4) Logiciels permettant d'intercepter par exemple des frappes au clavier pour opérer des attaques en profondeur en passant inaperçus aux yeux de la victime.

(5) Logiciels installés sur un système à l'insu de son propriétaire et permettant d'utiliser la puissance de calcul des machines infectées pour réaliser des opérations de minage de cryptomonnaie, récompensées par la génération de crytptomonnaie nouvelle.

(6) Un botnet est fait d'un ensemble de machines infectées par un logiciel malveillant se connectant à un système de commande et de contrôle donné.

(7) Le Ministère de l'intérieur définit la manipulation de l'information comme la réunion de trois critères cumulatifs : une campagne orchestrée, une diffusion massive de nouvelles fausses, et un objectif politique préétabli et hostile.

c. Le cyberespace : particularités

Comme le relève Delphine Deschaux-Dutard [(1)] dans un article de 2018 sur la cybersécurité internationale, « *le cyberespace présente des caractéristiques intrinsèques relativement proches de celles du milieu aérospatial. Il constitue en effet un espace dual et transverse qui peut être utilisé à des fins civiles et militaire. Il est omniprésent et constitue un socle sur lequel reposent l'ensemble de nos activités modernes. Il forme également un espace continu, mondial et perméable à toute pénétration en s'affranchissant des frontières physiques des États (…). L'effacement des distances, la fluidité des mouvements et la rapidité des déplacements dans cet espace offrent une grande liberté d'action et lui confèrent un caractère universel et stratégique* ».

Selon Olivier Kempf [(2)], le cyberspace se compose en effet de trois couches :

- Une couche matérielle (avec un ensemble d'infrastructures physiques concrètes et souvent inaperçues) ;

- Une couche logique (ensemble des protocoles, programmes et des langages permettant les connexions automatisées) ;

- Une couche sémantique (qui correspond au contenu de l'information véhiculée et au sens des données transmises par les couches matérielle et logique).

Loin de nous conduire à faire du cyberespace un lieu d'abstraction détaché du réel, ces éléments de définition doivent nous fournir une grille de lecture pour mieux penser les réponses opérationnelles adaptées aux spécificités évoquées. Entendre le cyberespace comme un lieu à la fois symbolique, puisqu'il véhicule un langage, des informations, et très concret, puisqu'il repose en dernier ressort sur des infrastructures tout à fait matérielles, nous invite à créer de nouvelles réponses aux actes délictueux qui s'y produisent. Il nous faut réorganiser nos structures de réponses, voire en inventer de nouvelles, qui tiennent compte de l'ambivalence d'un espace à la fois déterritorialisé, sans frontières, et reposant pourtant sur des lieux physiques (des serveurs, des câbles sous-marins).

Ce travail d'invention de la réponse institutionnelle la plus efficace et la plus efficiente est rendu difficile par cette ambivalence « réel/virtuel », mais aussi par la multiplicité des acteurs impliqués dans le cyberespace et par la volonté légitime des États de rester responsables des champs essentiels de souveraineté que constituent la défense et la sécurité. Construire une réponse coordonnée entre les États prend du temps et se fait essentiellement dans l'expérience partagée.

---

(1) Deschaux-Dutard, Delphine. « Chapitre 11. Cybersécurité internationale », Introduction à la sécurité internationale, sous la direction de Deschaux-Dutard Delphine. Presses universitaires de Grenoble, 2018, p. 209-225.

(2) Stratégie du cyberespace, Olivier Kempf, le 13 février 2013.

Ces efforts pour parvenir à des réponses coordonnées se heurtent en outre, comme nous l'avons vu, à la sous-évaluation des menaces par les citoyens, qui ne poussent pas à l'action publique sur ce sujet, et aux caractéristiques des dangers à prévenir. Les cyberattaques se diversifient plus vite que les moyens de les parer, et leurs auteurs se dissimulent bien souvent grâce à des techniques d'anonymisation. Toutefois, les conséquences actuelles et futures des atteintes à la cybersécurité obligent plus qu'elles n'invitent les pouvoirs publics à se saisir de ces enjeux au plus haut niveau.

2. Les atteintes à la cybersécurité ont pourtant des conséquences sécuritaires et économiques de plus en plus préoccupantes

a. L'évaluation incertaine du nombre d'attaques

Selon la Commission européenne, 80 % des entreprises européennes connaissent au moins un « incident de cybersécurité » par an. Dans certains États membres de l'Union, jusqu'à 50 % des crimes perpétrés interviendraient dans le champ de la cybercriminalité [(1)].

Toutefois, l'ensemble des éléments évoqués précédemment pour définir à la fois le cyberespace et la cybersécurité montrent bien la difficulté intrinsèque à disposer de données précises quant aux attaques, détournements, escroqueries et autres menaces mises à exécution. Aux caractéristiques fluides du milieu concerné vient s'ajouter la faible propension des victimes à déposer plainte, par peur d'une publicité négative concernant les entreprises.

En France, le rapport du Ministère de l'intérieur précédemment cité souligne cette difficulté de l'évaluation, mais estime néanmoins que le coût d'une violation de sécurité pour une entreprise de taille intermédiaire pourrait s'élever en moyenne à plusieurs centaines de milliers d'euros, alors que pour les entreprises victimes d'un détournement de données, le préjudice se compterait en millions d'euros [(2)].

En matière de coût de la cybercriminalité, les estimations les plus diverses peuvent donc être trouvées. Si le rapport annuel de l'*Internet Society's Online Trust Alliance* chiffre le coût de la criminalité informatique à 40 milliards de dollars dans le monde en 2018 [(3)], le *think tank Center for Strategic and International Studies* (CSIS) et la société McAfee l'évaluent à 600 milliards de dollars pour la même année. Faute d'un périmètre clair d'infractions et de victimes, et en raison de phénomènes de sous déclarations, il apparaît complexe de disposer de données stabilisées, et ce d'autant plus que les sociétés faisant

---

(1) Factsheet « Building a strong cybersecurity in Europe », Discours sur l'état de l'Union, Commission européenne, 2018.

(2) État de la menace liée au numérique en 2019, Rapport n° 3, mai 2019, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, p. 12.

(3) Voir la présentation du rapport ici : https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf

commerce de services de cybersécurité ont tout intérêt à présenter les dommages potentiels de la façon la plus inquiétante.

b. La difficile constitution d'un indice de cybersécurité

De la même façon qu'il demeure difficile d'estimer les coûts des dommages par les cyberattaques, la définition d'un indicateur qui permettrait de mesurer le niveau de cybersécurité continue de poser problème. Les indicateurs existent, mais c'est peut-être leur foisonnement et l'absence de consensus sur les paramètres à intégrer qui empêchent l'émergence d'une seule mesure suffisamment consensuelle pour assurer son utilisation large.

Daniel Ventre, chercheur au CNRS et titulaire de la Chaire Cybersécurité et Cyberdéfense de Saint Cyr, distingue trois sortes d'indices [(1)] : les indices visant à mesurer le niveau de cybersécurité des États, les indices à finalité économique permettant d'apprécier les risques pesant sur les entreprises, et les indices financiers appréciant la valeur du secteur industriel de la cybersécurité. Pour chaque catégorie d'indicateur coexistent plusieurs classements, certains élaborés par des acteurs publics [(2)], et d'autres par des acteurs privés, entreprises faisant commerce de solutions de cybersécurité, *thinks tanks* ou laboratoires.

La prise de conscience encore relativement récente de l'importance de ces enjeux explique les interrogations que soulèvent encore les indicateurs : quelle doit être leur finalité ? Comment garantir leur caractère objectif et leur impartialité ? De nombreuses questions demeurent quant aux méthodes à employer pour collecter les données nécessaires à l'établissement de diagnostics fiables de sécurité, dans un domaine où, nous l'avons évoqué, il n'est pas dans l'intérêt des victimes de divulguer leurs vulnérabilités.

C'est pourquoi votre rapporteur estime que le développement au sein de l'Union européenne d'un indicateur de mesure de la cybersécurité apparaît comme un prérequis indispensable à l'affirmation d'un modèle européen de cybersécurité. Cet indicateur devrait répondre à des critères de scientificité ouverts et permettre de mesurer les progrès réalisés d'une année à l'autre, notamment grâce aux outils mis en place pour garantir la cybersécurité au niveau de l'Union.

L'ENISA publie un rapport annuel d'évaluation des menaces [(3)] : à l'avenir, il pourrait être intéressant que ce rapport fasse l'objet d'une plus grande publicité, par le biais d'une présentation au Parlement européen par exemple. En l'état actuel des choses, il fournit déjà un panorama intéressant des tendances rencontrées dans les cybermenaces européennes. La transformation du rôle de l'ENISA s'accompagne d'une implication accrue en matière d'évaluation et de

---

(1) « De l'utilité des indices de cybersécurité », Sécurité et stratégie, Daniel Ventre, février 2016.

(2) Daniel Ventre mentionne par exemple l'Indice Mondial de Cybersécurité créé en 2015 par l'Union Internationale des Télécommunications.

(3) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

cartographie des menaces. L'expertise est l'un des piliers de la raison d'être de l'agence, mais elle pourrait toutefois gagner en visibilité sur ce sujet.

c. Un paysage de menaces amené à se densifier

Les différents rapports officiels et privés existant sur le paysage des cybermenaces tendent tous à montrer que chaque année, alors que certaines formes de cybercriminalité ou d'attaques perdent en intensité, de nouvelles formes font également leur apparition. Ainsi, selon le rapport de l'ENISA de janvier 2019, les actes de cyberespionnage et les rançongiciels connaîtraient une certaine baisse en 2018, tandis que les actes de *phishing* et de déni de service continueraient de progresser, comme en 2017. Mais une nouvelle menace, le *cryptojacking* (1), fait aussi son apparition dans le classement de l'agence européenne. Si l'on peut lutter contre les menaces cyber, et espérer enrayer leur nombre dès lors qu'une forme d'action délictueuse est bien identifiée, l'augmentation continuelle du nombre d'utilisateurs des réseaux, le développement toujours plus grand des interconnexions laissent à penser que les menaces ne feront que croître dans les prochaines années.

Certaines évolutions techniques concourent à ancrer cette tendance de fond dans un futur proche, comme l'explosion de l'internet des objets. On désigne par cette expression l'ensemble des objets, appareils et lieux équipés de capteurs pour recueillir des données, les réseaux par lesquels transiteront ces données et les plateformes qui en effectueront le traitement (2). L'internet des objets (IoT – *Internet of things*), combiné à l'utilisation de l'intelligence artificielle qui offre une plus grande capacité de traitement de la masse des informations générées, pourrait être la prochaine grande révolution connue par l'internet. Après le web 1.0, qui consistait principalement en la mise à disposition d'informations au public dans une configuration « push » (distribution dans un seul sens), et le web 2.0, qui introduisait plus d'interactivité et un réseau plus « social », ou « sémantique », le web 3.0 serait caractérisé par le règne des objets connectés et autres « *smart cities* ».

Avec la multiplication des objets et lieux connectés au réseau, les points d'entrée et de vulnérabilité aux attaques sont également multipliés. Selon le Club des Experts de la sécurité et de l'information du numérique, il faudra compter entre 50 et 80 milliards d'objets connectés dans le monde à l'horizon de 2020. L'attaque par le *malware* Mirai, qui a touché en 2016 entre 4 % et 5 % des

---

(1) Défini sous la note n° 4 p. 13 de ce rapport.

(2) Il n'existe pas de consensus sur cette notion récente et encore en pleine mutation, mais l'Union Internationale des Télécommunications définit l'internet des objets comme « une infrastructure mondiale au service de la société de l'information » permettant « d'offrir des services évolués en interconnectant des objets (physiques et virtuels) grâce à l'interopérabilité de technologies de l'information et de la communication existantes ou en évolution ».

routeurs des clients de *Deutsche Telekom* (900 000 clients ayant souffert de coupures de réseau) donne un aperçu de l'étendue potentielle des infections.

De plus, de nombreux objets connectés d'un usage quotidien ne sont souvent que très faiblement sécurisés, alors même qu'ils pénètrent dans les foyers et sont susceptibles de donner accès à toutes sortes d'informations sensibles. L'épisode récent en France de la découverte dans un robot-cuiseur commercialisé par l'enseigne Lidl d'un micro dont aucune mention n'était faite dans la notice illustre cette vulnérabilité. Destiné à permettre un usage de commande vocale lors d'une mise à jour ultérieure, le micro était présent sur le robot, et dans la cuisine du client, sans que celui-ci n'en ait connaissance.

Cette surface d'exposition sera en outre considérablement accrue par le déploiement de la 5G : les performances supérieures de cette nouvelle infrastructure télécom en termes de débit (bande passante), latence et vitesse permettront le développement d'un ensemble de services pour lesquels toute faille de sécurité devra être évitée. Comme l'explique le rapport d'information de l'OPECST [(1)] sur la 5G, son déploiement devrait « permettre des communications massives, quasiment en temps réel, grâce à l'optimisation des bandes de fréquence par des modulations numériques plus complexes et un meilleur pointage des faisceaux ». La diversification et la multiplication des applications possibles grâce à ces connections considérablement améliorées ne peuvent que mener à des besoins accrus de cybersécurité.

Le développement de la 5G devrait également entraîner la généralisation des réseaux virtualisés, pour lesquels des solutions logicielles déployées dans le *Cloud* se substitueront aux équipements physiques. Outre les nouvelles failles potentielles de sécurité liées au *Cloud* soutenant cette virtualisation, la part croissante prise par la dimension immatérielle du réseau expose aussi celui-ci au besoin de mises à jour fréquentes, qui sont autant de fenêtres de risques.

Les cadres juridiques nationaux commencent d'ailleurs à intégrer ces nouveaux enjeux de sécurité, qui concernent tant les futurs usages que les infrastructures nécessaires à leur mise en œuvre, comme le montre l'adoption en France de 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 [(2)].

---

(1) Rapport de MM. Pierre Henriet, député, et Gérard Longuet, sénateur, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, n° 188 (2018-2019) – 11 décembre 2018.

(2) Voir sur le sujet plus précisément des infrastructures 5G le rapport fait au nom de la commission des affaires économiques sur la proposition de loi 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 (n° 1722, Éric Bothorel).

d. Des menaces en mutation et qui brouillent encore un peu plus les limites entre guerre et paix : la montée des menaces hybrides

Sujet porté haut par la présidence finlandaise de l'Union européenne du second semestre 2019, les menaces hybrides constituent un nouvel objet à la définition aussi flexible qu'elles apparaissent insaisissables.

Selon Cédric Le Bigot, Chef de bataillon de l'Armée de terre, « le concept de menaces hybrides a émergé durant la dernière décennie parmi de nombreux *think-tanks* américains. Dérivé du concept d'*irregular threat*, il décrit une forme émergente de menaces, dans laquelle des acteurs principalement non-étatiques mettraient en œuvre une combinaison de moyens à la fois cinétiques (guerre conventionnelle, asymétrique, crime organisé) et non cinétiques (actions subversives, politiques, sociales) » [(1)].

Si la présidence finlandaise a mis ce concept au rang de ses priorités, c'est aussi que se situe à Helsinki le Centre d'excellence sur les menaces hybrides, une structure de coopération rassemblant 22 États membres de l'Union. Ce centre est né du cadre commun élaboré par la Commission européenne et le Service européen d'action extérieure en 2016, qui proposait une série d'actions destinées à familiariser les États membres à la détection et aux réponses possibles en cas de menaces hybrides. En outre, une coopération approfondie est menée entre l'Union européenne et l'OTAN sur ce sujet, avec plusieurs déclarations conjointes (à Varsovie en 2016, à Bruxelles en 2018). Le centre d'excellence joue un rôle important dans cette collaboration.

Le caractère insidieux des menaces hybrides plaide pour une approche globale, qui nécessite de repenser les liens entre les domaines civils et militaires, et entre capacités défensives et offensives en matière de cybersécurité. Aujourd'hui, la possibilité d'un conflit démarrant sur des bases non conventionnelles mais susceptible de prendre les dimensions d'une véritable guerre n'est plus anecdotique. Or, si la guerre conventionnelle est régie par un ensemble de codes et de conventions, les menaces hybrides et les risques de cybersécurité reçoivent une réponse encore parcellaire et éclatée de la part de la communauté internationale.

Votre rapporteur y voit le signe d'une difficulté persistante à penser au-delà de la frontière civil/militaire et à imaginer une réponse partenariale sous l'impulsion d'une sphère politique encore trop en retrait. La multiplicité des instances dans lesquelles se discutent et se décident les réponses à apporter aux menaces de cybersécurité plaiderait pourtant, selon votre rapporteur, pour une incarnation politique nationale forte sur ces sujets.

---

(1) « L'émergence des menaces hybrides : vers une autre transformation de la guerre ? », Chef de bataillon de l'Armée de terre Cédric Le Bigot, Pensée mili-terre, 10 juillet 2018.

B. UN FOISONNEMENT D'INSTITUTIONS INTERNATIONALES SAISIES DES ENJEUX DE CYBERSÉCURITÉ

La cybersécurité étant par nature un sujet ne connaissant pas de frontière, force est de constater que sa prise en compte par les organisations internationales se fait de façon foisonnante et peu coordonnée, conduisant à un véritable « patchwork institutionnel » de la cybersécurité [(1)].

1. L'ONU

L'Union internationale des télécommunications (institution issue des Nations Unies) a organisé en 2003 à Genève puis à Tunis en 2005, le Sommet mondial sur la société de l'information, destiné à engager une vaste réflexion programmatique et à susciter une prise de conscience sur les différents enjeux du numérique (dont ceux de cybersécurité), à l'instar de ce que le Sommet de Rio avait pu initier pour les questions environnementales.

L'Agenda de Tunis a mené à la création du Forum sur la gouvernance de l'Internet (FGI), qui a depuis réuni chaque année les différentes parties prenantes, société civile, entreprises privées et institutions publiques, afin de débattre des enjeux liés à la gouvernance de l'Internet. Les enceintes de l'ONU, et par extension de l'UIT et du FGI, servent d'abord à diffuser et échanger les meilleures pratiques, à documenter les avancées réalisées aux niveaux national et supranational, comme le montre par exemple le document sur les accords de cybersécurité réalisé en amont de la session de 2019 du FGI devant se tenir à Berlin [(2)]. Ce document d'information préparatoire recense en effet un ensemble d'accords et de textes contraignants au niveau international en matière d'obligations de cybersécurité.

Au-delà de ces missions d'information et d'éducation par les pairs, le système onusien a aussi pour ambition de parvenir à des résultats plus opérationnels en faisant converger la volonté des États sur un certain nombre d'initiatives. Deux programmes spécifiques peuvent être signalés : le programme IMPACT (*International Multilateral Partnership Against Cyber Terrorism*) et un programme de protection de l'enfance en ligne, le COP (*Child Online Protection*). En outre, des groupes d'experts gouvernementaux (GGE) ont été constitués pour travailler à des principes communs, avec des fortunes diverses selon les années. On notera ainsi le rapport du GGE de 2015, qui a permis d'énoncer onze principes de conduite précis pour les États dans le cyberespace, comme l'interdiction d'attaquer les infrastructures critiques d'un État tiers en temps de paix ou l'obligation de porter assistance à un État attaqué par un groupe situé dans un autre État si celui-ci en fait la demande. Dès 2013, le GGE avait établi que les

(1) Nicolas Arpagian, ibid.

(2) https://www.intgovforum.org/multilingual/filedepot_download/4904/1658

principes et règles de droit international s'appliquaient aux comportements des États dans le cyberespace.

Malgré l'échec du GGE de 2017, il convient de noter que les négociations au sein de l'ONU sur les sujets de cybersécurité ont paru relancées avec l'adoption par l'Assemblée générale de 2018 de deux résolutions créant un nouveau GGE (le sixième) et un groupe de travail ouvert à tous les États membres.

Lors de sa réunion de 2018, organisée au siège de l'UNESCO à Paris, le FGI a donné lieu à l'Appel de Paris pour la sécurité et la confiance dans le cyberespace, lancé par le Président Macron. Cette déclaration, soutenue par plus de soixante États et près de cent cinquante organisations internationales, assignait des objectifs à la diplomatie du cyberespace, parmi lesquels accroître la prévention et la résilience face aux activités malicieuses en ligne, protéger l'accessibilité et l'intégrité d'Internet ou encore prévenir la prolifération des programmes et techniques cyber malicieux [(1)] .

Votre rapporteur est d'avis qu'il convient de s'appuyer sur le soutien déjà large recueilli par l'Appel de Paris (plus d'un tiers des pays membres de l'ONU) pour relancer les discussions sur les enjeux de cybersécurité à l'ONU en insistant sur leur caractère opérationnel, et de veiller à ce que le droit international s'applique dans le champ du cyberespace en impliquant ses acteurs dans leur diversité. Il appuie en cela le travail important mené par l'Ambassadeur français du numérique, qui a pu lui exposer à Paris les différentes dimensions de l'action diplomatique d'impulsion sur la cybersécurité.

2. L'OTAN

Depuis 2016, le cyberespace constitue l'un des domaines potentiels d'opération de l'Alliance atlantique, et l'Engagement en faveur de la cyberdéfense pris par les chefs d'État au sommet de Varsovie comporte l'essentiel des lignes directrices de l'action de l'OTAN en ce domaine, pour lequel les Alliés ont réaffirmé le mandat défensif de l'organisation.

Il s'agit tout à la fois d'accroître les capacités opérationnelles des pays membres et de renforcer leur coopération, en organisant des exercices conjoints et en favorisant le partage de l'information.

Plusieurs projets de défense intelligente ont ainsi été lancés, qui consistent à permettre aux pays d'unir leurs efforts pour supporter ensemble les coûts de développement ou d'acquisition de capacités. Parmi ceux-ci, nous pouvons mentionner le projet de plateforme d'échange sur les logiciels malveillants

---

(1) *https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la*

(MISP), le projet de développement d'une capacité multinationale de cyberdéfense (MNCD2), ou encore le projet multinational de formation et d'entraînement à la cyberdéfense (MNCD E&T).

L'OTAN dispose également de partenariats avec l'Union européenne depuis février 2016, et avec le secteur industriel, au titre du cyberpartenariat OTAN-industrie.

3. Interpol

Interpol, l'organisation internationale destinée à promouvoir la coopération policière au-delà des frontières, a naturellement vocation à développer un versant cybersécurité à mesure qu'une criminalité s'invente et se propage sur les réseaux.

Aujourd'hui, Interpol dispose d'une « Stratégie en matière de lutte contre la cybercriminalité » destinée à favoriser la coordination et la mise en œuvre de capacités policières dans les pays membres sur cette période. Cette stratégie comporte cinq axes d'action qui visent à l'identification des cyberattaques et de leurs auteurs par la détection des actes, l'accès aux données, la gestion des éléments de preuves électroniques, leur corrélation avec les données physiques ou encore l'amélioration de l'interopérabilité des systèmes de police.

Ces activités s'articulent autour de trois programmes mondiaux sur l'antiterrorisme, la cybercriminalité et la criminalité organisée.

4. Le Conseil de l'Europe

Le Conseil de l'Europe a joué un rôle précurseur dans la lutte pour la cybersécurité, puisqu'il a permis l'adoption de la Convention de Budapest en 2001, qui reste à ce jour le seul instrument international contraignant sur la question de la cybercriminalité. Cette Convention a une double ambition : celle de fournir un guide au plan interne pour les pays souhaitant mettre en œuvre des législations adaptées, mais aussi celle de pousser vers une action externe plus coordonnée des États parties entre eux.

La Convention établit une liste d'infractions pénales, elle porte en particulier sur des infractions concernant le droit d'auteur, la fraude liée à l'informatique, la pédopornographie, ainsi que sur des infractions liées à la sécurité des réseaux. Le Traité contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception. Ouvert à la signature en 2001, il a été ratifié par la France en 2006. En 2019, le Traité avait été ratifié par soixante-quatre pays, membres et non membres du Conseil de l'Europe. La Convention est complétée depuis 2003 par un Protocole

relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, ratifié par la moitié des pays parties à la Convention de Budapest. La qualité de la mise en œuvre de la Convention de Budapest est évaluée par le Comité de la Convention sur la cybercriminalité (T-CI) représentant les Parties à cette Convention, et qui se réunit deux fois par an à huis clos.

Le Conseil de l'Europe a lancé récemment une consultation pour l'établissement d'un second protocole à la Convention, qui porterait notamment sur le renforcement de la coopération judiciaire et les preuves électroniques.

En outre, le travail du Conseil de l'Europe, également précurseur pour le versant international de la lutte contre la cybercriminalité, dispose aussi d'un volet plus opérationnel, puisque l'institution offre un programme de formation et d'aide à la mise en oeuvre des standards de la Convention (le « *Cybercrime Programme Office of the Council of Europe* (C-PROC) »), ainsi qu'un registre des points de contact rassemblant les autorités nationales concernées par les requêtes d'assistance mutuelle en cas d'attaques.

Parmi les nombreuses actions menées par le Conseil de l'Europe sur ce sujet, on notera le programme Glacy + (succédant à Glacy), programme conjoint avec l'Union européenne (par le biais de l'Instrument contribuant à la Paix et à la Stabilité, IcPS) et qui vise à soutenir certains pays prioritaires en Afrique et Asie-Pacifique, afin d'en faire des relais pour la mise en place d'actions de renforcement de capacité et de création de législations adaptées.

La lente montée en puissance des enjeux de cybersécurité se heurte donc à la difficulté d'une évaluation précise des coûts générés par les cyberattaques, et à une certaine dispersion de l'action internationale requise. Cela justifie d'autant plus, selon votre rapporteur, que l'Union européenne prenne toute sa place pour la préservation de la cybersécurité grâce, notamment, à une Agence européenne pour la cybersécurité au mandat renouvelé.

II. L'ENISA, UNE AGENCE EUROPÉENNE RENFORCÉE AU SERVICE D'UNE CYBERSÉCURITÉ PLUS INTÉGRÉE

A. LE PAYSAGE TRÈS ÉCLATÉ DE LA CYBERSÉCURITÉ EUROPÉENNE

De nombreux pays membres de la Convention de Budapest qui l'ont signée dès 2001 appartiennent à l'Union européenne, mais les initiatives au sein de celle-ci sont longtemps restées rares, ou cantonnées au niveau national. Néanmoins, au cours des années 2000 commencent à s'agréger des éléments disparates qui conduiront à l'établissement d'une véritable stratégie de cybersécurité européenne à partir de 2013.

1. Premières esquisses stratégiques de l'Union européenne

En 2001, la Commission européenne publiait une communication sur la sécurité des communications et des réseaux appelant à l'élaboration d'une politique européenne commune [(1)]. Cette communication prenait appui sur les progrès réalisés en matière de sécurité des signatures électroniques avec la directive adoptée le 13 décembre 1999 [(2)]. Cet objectif plusieurs fois affirmé de sécurité des réseaux (on ne parle pas encore de cybersécurité) s'est poursuivi avec la « stratégie pour une société de l'information sûre » de 2006 [(3)] et le plan d'action et la communication [(4)] sur la protection des infrastructures d'information critiques [(5)] de 2009.

Il faut souligner que si les cybermenaces n'entrent pas dans les menaces prioritaires identifiées dans la première stratégie de sécurité de l'Union européenne parue en 2003, le rapport du Secrétaire général et Haut représentant sur la mise en œuvre de cette stratégie, qui date lui de 2008, place le défaut de cybersécurité au nombre des cinq menaces majeures listées.

Ces enjeux commencent donc à faire l'objet d'une certaine doctrine encore disparate et abordant les enjeux par plusieurs angles, économique ou sécuritaire, au sein de l'Union européenne dans le courant des années 2000.

---

(1) Communication de la Commission au Conseil, au Parlement européen, au Comite économique et social et au comité des régions « Sécurité des réseaux et de l'information : Proposition pour une approche politique européenne », COM (2001)503.

(2) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

(3) Communication de la Commission au Conseil, au Parlement européen, au Comite économique et social et au comité des régions « Une stratégie pour une société de l'information sûre », COM(2006)251.

(4) COM(2009)149 approuvé par la résolution du Conseil 2009/C321/0.

(5) COM(2011)163 approuvé par les conclusions du Conseil 10299/11.

2. Une action de cybersécurité dispersée

a. Sécurité des réseaux et de l'information

i. La création de l'ENISA

La création de l'ENISA [(1)] (l'Agence européenne chargée de la sécurité des réseaux et de l'information, toujours appelée par l'acronyme anglais de « *European Network and Information Security Agency* ») en 2004, concrétise la montée en puissance de ces problématiques sur la scène européenne. En 2005, l'agence est établie à Héraklion, en Crète, et dispose d'un budget et d'un nombre d'agents assez modestes. À titre d'exemple, pour 2012, elle est dotée de 8,5 millions d'euros et d'une soixantaine d'agents [(2)].

Toutefois, les moyens et la durée du mandat de l'ENISA sont d'emblée limités et apparaissent insuffisants au regard de l'étendue des missions qui lui sont dévolues. Plusieurs règlements ont prolongé successivement la durée du mandat de l'ENISA jusqu'au règlement de 2013 [(3)], le dernier avant que l'Acte de Cybersécurité n'établisse la permanence de l'Agence et n'en assure la refondation. Avec ces prolongations se sont également progressivement affirmées des missions toujours plus riches pour l'Agence, notamment pour accompagner la stratégie numérique pour l'Europe qui se mettait en place à partir de 2010. Le mandat de son directeur exécutif a également pu être prolongé et ses moyens accrus durant le cadre financier pluriannuel suivant.

ii. La création d'un centre d'intervention d'urgence

Dans la continuité de cette stratégie pour l'agenda numérique et pour la sécurité des réseaux et de l'information, une décision de la Commission européenne du 11 septembre 2012 a instauré une équipe d'intervention d'urgence dans le domaine de la sécurité informatique ayant pour mission de protéger les institutions européennes contre les cyberattaques.

Le CERT-UE [(4)] compte 30 membres issus de la Commission européenne, du Secrétariat général du Conseil, du Parlement européen, du Comité des régions et du Comité économique et social. Comme les autres CSIRT [(5)] publics et privés, il a vocation à répondre de manière efficace à des incidents de sécurité

---

(1) Par le règlement (CE) n° 460/2004.

(2) Chiffres cités par Olivier Kempf dans « La cyberstratégie de l'Union européenne », revue « Sécurité globale », n° 24, 2013.

(3) Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004.

(4) Pour « Computer Emergency Response Team ».

(5) Un CSIRT est un « Computer Security Incident Response Team », une équipe d'intervention en cas d'incident informatique. Le terme est privilégié en Europe car le terme de CERT provient des États-Unis Toutefois, les CSIRT qui en font la demande à l'Université Carnegie Mellon – la première institution à avoir développé un CERT pour le gouvernement américain – et en obtiennent l'autorisation, peuvent utiliser le terme de CERT, signifiant Computer Emergency Response Team dans leur nom.

informatique et aux cybermenaces, 24 heures sur 24 et 7 jours sur 7. Plus précisément, le CERT-UE doit centraliser les demandes d'assistance émanant des équipes de cybersécurité locales, traiter les alertes et réagir aux attaques informatiques, prévenir les incidents par la diffusion d'informations et de bonnes pratiques, et établir et maintenir à jour une base de données des vulnérabilités. Ses missions recouvrent donc la prévention, la détection, la réponse et la réparation des incidents informatiques.

Au-delà de ces missions traditionnelles qui incombent à tout CSIRT, le CERT-UE vise à construire et compléter les capacités existantes des institutions, organes et agences de l'Union et à encourager l'émergence d'une culture de la confiance au sein de cet environnement protégé.

b. Sécurité intérieure : Centre européen de lutte contre la cybercriminalité

Dans le cadre de la stratégie de sécurité intérieure de l'Union adoptée en 2010, un Centre européen de lutte contre la cybercriminalité (EC3), composante d'Europol, a été créé en 2013 afin d'apporter une réponse institutionnelle à la forte progression de la cybermenace. Sa mission consiste à renforcer la répression de la cybercriminalité dans l'Union, et à protéger les citoyens, les entreprises et les gouvernements. Pour ce faire, EC3 rassemble auprès des pays l'information et l'expertise, soutient les enquêtes pénales menées par les États membres, promeut des solutions et sensibilise aux enjeux de cybersécurité à l'échelle de l'Union.

Votre rapporteur tient à souligner que les représentants de l'ENISA lui ont expliqué le temps qu'avait mis à se développer la coopération pénale à l'échelle européenne sur les sujets de cybersécurité et l'importance des progrès réalisés en ce domaine grâce à des enceintes telles que le groupe de coopération instauré par la directive SRI.

c. Recherche et diplomatie

i. Le Service européen pour l'action extérieure

Le Service européen pour l'action extérieure assiste la Haute représentante pour les affaires étrangères et la politique de sécurité de l'Union dans le but de renforcer la cohérence et l'efficacité de la politique étrangère de l'Union, et d'accroître ainsi l'influence de l'Europe dans le monde.

À ce titre, le directeur général de la politique de sécurité, M. Pauwel Herczynski, a pu expliquer à votre rapporteur la difficulté à faire progresser les enjeux de cybersécurité dans le cadre des enceintes où le SEAE représente l'Union, notamment à l'ONU au sein du nouveau groupe d'experts

gouvernementaux. Sur les questions de la protection de la cybersécurité européenne, du partage des informations en cas d'attaque et de l'attitude à adopter face à celles-ci, la définition d'une doctrine européenne sur la scène internationale demeure une tâche complexe.

Ces difficultés tiennent, d'une part, à la pluralité des visions qui persistent dans l'Union sur des points très sensibles de souveraineté. L'Union européenne n'a pas de position unifiée sur ces sujets. Il existe un groupe de travail, le Groupe horizontal sur les questions de cybersécurité, qui se rencontre régulièrement. Mais le SEAE ne peut s'exprimer que lorsqu'il y a consensus entre les pays membres, et que ce consensus se manifeste dans le groupe, ce qui est loin d'être toujours le cas.

D'autre part, l'Union européenne ne peut d'elle-même avoir une capacité offensive, celle-ci étant réservée aux États membres. L'attribution collective par l'Union européenne d'une attaque, qui pourrait être pour le SEAE un objectif à atteindre collectivement, reste encore aujourd'hui empêchée par des questions de souveraineté.

Le rôle du SEAE est le révélateur parfait de l'ambiguïté de la position européenne, qui serait plus forte à parler d'une seule voix au niveau mondial, mais peine à le faire en raison de la pluralité des perspectives nationales et de ses propres limites opérationnelles (une difficulté qui n'est, malheureusement, pas spécifique à la question de la cybersécurité).

Certains progrès peuvent toutefois être salués dans l'élaboration d'une « boîte à outils cyberdiplomatique », réponse diplomatique conjointe de l'Union aux actes de cybermalveillance, dont le principe a été acté en 2017 par le Conseil [(1)]. Pour parvenir à ces progrès, les questions de souveraineté doivent parfois être contournées : ainsi, et de façon assez paradoxale, la discussion du régime de sanction a pu avancer pour les 28 États membres à condition d'être découplée de la question de l'attribution de l'attaque à un pays en particulier.

ii. L'Institut européen pour les études de sécurité

Cette agence de l'Union européenne, dont votre rapporteur a rencontré l'une des analystes, Mme Nathalie Van Raemdonck, produit des études et des articles de recherche dans les champs de la politique de sécurité et de défense, à destination du Conseil, de la Haute représentante pour les affaires étrangères et la politique de sécurité, ainsi que pour les États membres. Elle développe à ce titre une expertise sur la cybersécurité, notamment à travers les *« Chaillot papers »*.

En outre, l'Institut mène, conjointement avec le *German Marshall Fund of the United State*s et le *Neue Stiftung Verantwortung*, un programme intitulé

(1) Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance, document 9916/17 du 7 juin 2017.

« EU Cyber Direct », financé en partie par la Commission [1], qui consiste à favoriser le dialogue avec de multiples partenaires internationaux, aussi bien publics que privés, pour diffuser les niveaux d'exigence européens en matière de cybersécurité, identifier les meilleures pratiques, et contribuer à la promotion d'une culture partagée de la cybersécurité.

B. UNE STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ QUI TEND À SE CRISTALLISER

1. Le cadre stratégique de 2013 et l'adoption de la directive SRI : concilier volet sécuritaire et volet industriel

En 2013 est véritablement consacrée la cybersécurité comme priorité stratégique de l'Union, et la Commission européenne publie, en liaison avec la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, une stratégie en matière de cybersécurité ainsi qu'une proposition de directive de la Commission concernant la sécurité des réseaux et de l'information (dite directive SRI ou NIS selon l'acronyme anglais).

La vision de l'Union articulée dans cette stratégie de 2013 intitulée « Un cyberespace ouvert, sûr et sécurisé » reposait sur cinq priorités :

- Parvenir à la cyber-résilience ;
- Faire reculer la cybercriminalité ;
- Développer une politique et des moyens de cyberdéfense en liaison avec la politique de sécurité et de défense commune (PSDC) ;
- Développer les ressources industrielles et technologiques en matière de cybersécurité ;
- Instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'Union.

Les enjeux de sécurité et de développement économique sont donc progressivement rapprochés au sein de la doctrine et de la législation de l'Union européenne. La stratégie de 2013 dessine un lien fort entre le renforcement de la cybersécurité et le développement de ressources industrielles et technologiques propres à ce secteur. Votre rapporteur ne peut qu'appuyer cette tendance qui s'affirme encore, nous le verrons, avec les textes plus récents.

---

(1) Par le biais de l'instrument de partenariat dédié au sujet de la coopération numérique internationale à la confiance et à la sécurité dans le cyberespace.

Le mandat de l'Agence européenne de défense et l'articulation avec les agences civiles

La stratégie de 2013 appelait à une évaluation des besoins pour mener à bien une stratégie efficace de cybersécurité au niveau de la défense européenne. En termes opérationnels : il s'agissait de disposer d'une vision claire des capacités opérationnelles et technologies requises pour adresser tous les défis, en termes d'organisation, de personnel, de formation, d'infrastructures, d'interopérabilité au sein de l'Union. Dans la lignée du Cadre stratégique de 2013 a donc été adopté par le Conseil, sur la base des conclusions du Conseil européen de novembre 2013 et de décembre 2013 sur la PSDC, un Cadre d'action de l'Union en matière de cyberdéfense, qui est depuis régulièrement mis à jour et oriente l'action européenne de la cyberdéfense.

Selon le directeur général adjoint de l'Agence européenne de défense (AED), M. Olli Ruutu, que votre rapporteur a rencontré à Bruxelles, le rôle de l'AED, dont les effectifs propres comptent moins d'une centaine de personnes, est donc de former une sorte de pôle de coopération au sein des gouvernements des États membres. Depuis 2004, l'Agence a orienté plus d'un milliards d'euros de fonds européens en direction de projets pour le développement de la cybersécurité européenne, surtout dans le domaine de la recherche, avec un net accroissement des montants engagés ces trois dernières années. Selon M. Ruutu, l'AED veille également à ce que les fonds soient bien ciblés vers les priorités dégagées au niveau de l'Union.

Il faut souligner que dans le cadre de la coopération structurée permanente lancée le 11 décembre 2017 entre 25 États membres, deux projets sont liés à la cyberdéfense, celui « d'équipes d'intervention rapide en cas d'incident informatiques et assistance mutuelle dans le domaine de la cybersécurité », ainsi « qu'une plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques ». Si ces deux projets apparaissent tout à fait utiles et intéressants à votre rapporteur, se pose néanmoins la question de leur articulation avec les missions renforcées dévolues à l'ENISA par ailleurs.

Le directeur général adjoint a indiqué que si l'AED travaille sur le versant défense de la cybersécurité, ce qui nécessite d'avoir pour principaux interlocuteurs les ministères nationaux de la défense, la cybersécurité tend sans nul doute à brouiller la frontière entre activités civiles et militaire. C'est pourquoi l'Agence travaille en étroite collaboration avec d'autres organes européens issus de ces deux champs civil et militaire : le Collège européen de sécurité et de défense, l'ENISA, le CERT-EU, le Centre européen de cybercriminalité, le Service européen pour l'action extérieure, les différentes directions concernées au sein de la Commission européenne. Mais l'AED opère également une collaboration étroite avec l'OTAN.

Les représentants de l'AED ont par ailleurs insisté sur la nécessité de disposer d'une véritable industrie de cybersécurité capable de fournir des solutions européennes tout à fait sécurisées : en ce sens, la certification proposée par l'Acte de cybersécurité prend évidemment une importance éminemment stratégique.

Le cadre de coopération établi et renforcé entre les agences concernées par les récentes décisions européennes parait donc tout à fait profitable aux représentants de l'AED, pour lesquels il permet une complémentarité approfondie et croissante entre les secteurs civils et militaires.

2. La directive SRI : amorcer une architecture européenne de la cybersécurité plus intégrée pour les États membres

a. Une volonté de clarification des acteurs et de leurs missions

Alors que la stratégie intitulée « Un cyberespace ouvert, sûr et sécurisé » est présentée en 2013, la directive sur la sécurité des réseaux et de l'information met trois ans à être adoptée. Les difficultés de sa négociation renvoient de façon claire à l'équilibre très subtil à atteindre entre le maintien de la souveraineté des États membres sur ces sujets très régaliens d'une part, et l'intégration dans une architecture plus resserrée de la cybersécurité européenne d'autre part, avec ce qu'elle implique de partage d'informations et de mise en cause d'aspects traditionnellement régaliens de l'action des États.

La directive vise à « assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union » [(1)].

Cela passe par quatre axes :

- le renforcement des capacités nationales : chaque État membre doit se doter d'une stratégie nationale de cybersécurité, désigner des autorités nationales compétentes, un point de contact unique et mettre en place des CSIRT pour chaque secteur essentiel de l'économie et de la vie en société ;

- l'établissement d'un cadre de coopération volontaire entre les États membres et l'Union : ce cadre repose sur la création d'un groupe de coopération (dimension politique de la cybersécurité) et d'un réseau européen des CSIRT (dimension technique) ;

- le renforcement par chaque État membre de la sécurité informatique de ses opérateurs de services essentiels (OSE), via la définition de mesures nationales en la matière et surtout par l'obligation de notification des incidents ayant un impact significatif sur la continuité du service fourni par un OSE donné ;

- l'instauration de règles européennes communes concernant la cybersécurité de trois types de fournisseurs de services numériques (FSE), à savoir les acteurs de l'informatique en nuage, les moteurs de recherche et les places de marché en ligne.

Cette directive adoptée en 2016 est entrée en vigueur le 9 mai 2018. La directive SRI s'est inscrite pour la France dans le prolongement du dispositif pionnier de cybersécurité des opérateurs d'importance vitale (OIV) mis en place dans le cadre de la loi de programmation militaire de 2013. Notre pays s'était par ailleurs déjà doté d'une stratégie nationale, et dispose d'une autorité nationale de cybersécurité, l'Agence nationale de sécurité des systèmes d'information

(1) Directive sur la sécurité des réseaux et de l'information.

(ANSSI), à la pointe au niveau mondial, et largement reconnue comme telle. A priori, la transposition ne nécessitait donc que des adaptations à la marge, ayant essentiellement pour but de favoriser la coopération européenne. La France, *via* la loi du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, a néanmoins fait le choix d'une transposition ambitieuse, en incluant dans la liste des OSE des secteurs non-prévus dans l'annexe II de la directive.

L'ANSSI élabore les règles de sécurité que doivent respecter les OSE pour prévenir les incidents ou du moins en limiter l'impact, selon une approche de management des risques qui prend en compte la gouvernance, la protection et la défense des réseaux et des systèmes d'information, ainsi que la résilience des activités concernées.

La directive impose également des obligations de sécurité aux fournisseurs de services numériques clés, obligations détaillées dans un règlement d'exécution [(1)].

La directive SRI a poussé chaque État membre à se doter d'autorités nationales compétentes, ou à désigner des autorités chefs de file, sur la cybersécurité. C'est ensuite autour de cette autorité que doivent se cristalliser les différentes capacités nécessaires, de prévention mais également de réaction en cas d'attaque. Bien que ces autorités aient une puissance et des moyens inégaux selon les pays de l'Union, leur désignation a permis d'institutionnaliser un dialogue entre les États sur ces sujets, de créer un réseau européen permettant aux responsables d'échanger les meilleures pratiques, mais aussi des renseignements précieux dès lors que le niveau de confiance le permet.

À ce titre, le groupe de coopération de la directive SRI constitue une vraie réussite. Créé pour permettre d'harmoniser la mise en œuvre de la directive, il s'avère un carrefour de coopération très précieux en réunissant les autorités nationales référentes, l'ENISA et la Commission européenne. Ce groupe de coopération a su devenir un forum efficace en vue de fournir des orientations au réseau des CSIRT européens. Également créé par la directive, celui-ci réunit les CSIRT nationaux dont les États ont depuis 2018 l'obligation de se doter, et le CERT-EU, organe équivalent de l'Union européenne. Ces deux réseaux de coopération permettent de lier un espace de réflexion et d'élaboration de stratégies concertées avec le groupe de coopération d'une part, et un espace à la dimension plus opérationnelle avec le réseau des CSIRT/CERT-EU d'autre part.

La directive SRI constitue une avancée majeure pour la structuration des différents niveaux de gouvernance de la cybersécurité européenne : elle n'a

(1) Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

toutefois pas vocation à une harmonisation totale des modèles nationaux, qui ne serait ni possible, ni souhaitable.

SECTEURS ET SOUS-SECTEURS PERTINENTS POUR L'IDENTIFICATION DES OPÉRATEURS DE SERVICES ESSENTIELS DANS LA DIRECTIVE SRI

Secteur	Sous-secteur
1. Énergie	a) Électricité
	b) Pétrole
	c) Gaz
2. Transports	a) Transport aérien
	b) Transport ferroviaire
	c) Transport par voie d'eau
	d) Transport routier
3. Banques	
4. Infrastructures de marchés financiers	
5. Secteur de la santé	
6. Fourniture et distribution d'eau potable	
7. Infrastructures numériques	

Source : annexe II de la directive SRI, Commission européenne

b. Des modèles nationaux qui restent très divers

La désignation d'autorités pour la cybersécurité et de points de contact nationaux a incontestablement poussé les États membres à accroître leur effort dans ce domaine. Cet effort avait déjà été bien entamé dans certains États membres, qui disposent d'une expérience reconnue et font figure de modèles : la France peut ainsi se targuer de l'excellence de son Agence nationale de sécurité des systèmes d'information (ANSSI), mentionnée de nombreuses fois à votre rapporteur. Cette excellence a contribué à asseoir la légitimité de la France à diffuser dans l'Union européenne un modèle national ayant acquis une solide réputation. La directive SRI a d'ailleurs été largement inspirée du modèle de cybersécurité français et les opérateurs de services essentiels de la directive reprennent en partie les caractéristiques des opérateurs d'importance vitale (OIV) français.

Mais ces éléments n'ont pour autant pas conduit à une uniformisation très poussée des modèles d'organisation de la cybersécurité dans les États de l'Union. Dans plusieurs d'entre eux, une agence centrale dispose d'un budget et d'effectifs importants, et d'une expertise qui a fait ses preuves en raison de nombreuses années de pratique de la cybersécurité dans les pays concernés : qu'il s'agisse de l'ANSSI en France, du *National Cyber Security Center* au Royaume-Uni, du *National Cyber Security Centre* (NCSC) irlandais ou du *Bundesamt für Sicherheit in der Informationstechnik* (BSI) en Allemagne (près de 950 personnes en 2018).

D'autres États membres présentent en revanche un profil beaucoup plus éclaté : l'Italie a ainsi fait le choix d'une structure polycentrique, avec plusieurs ministères désignés comme autorités nationales au sens de la directive SRI [(1)] et un système de coordination de l'action de ces ministères par un comité technique de liaison, sans qu'une agence nationale unique ne soit chargée du champ de la cybersécurité.

Enfin, certains États membres peinent à trouver les moyens et l'expertise nécessaires à la création d'une telle autorité efficace. Au-delà des questions matérielles, des raisons culturelles et historiques peuvent également expliquer la réticence de certains pays à voir s'ériger de nouveaux organes responsables de la sécurité de l'information. Dans certains pays où les agences de cybersécurité sont bien implantées et dotées d'une véritable expertise, les caractéristiques mêmes de l'organisation étatique (fédéralisme, provinces autonomes) ou administrative peuvent constituer des freins, ou des adjuvants.

(1) Le Ministère du développement économique, le Ministère des infrastructures et des transports, le Ministère de la santé et le Ministère de l'environnement et de la tutelle du territoire et de la mer.

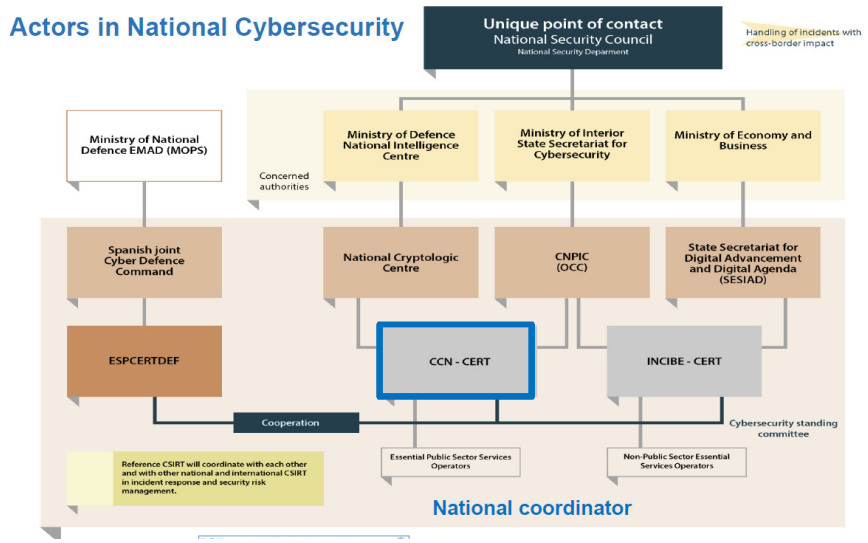
L'organisation de la cybersécurité nationale : l'exemple espagnol

Lors d'une mission effectuée à Madrid durant plusieurs jours, votre rapporteur a pu observer, à travers une série d'auditions des principales institutions responsables du secteur public, la diversité des modèles européens d'organisation de la cybersécurité.

Quatre ministères sont impliqués et chapeautent plusieurs agences ou organisations qui coopèrent entre elles à différents niveaux. Pour la partie « civile », sous la houlette du département de la sécurité nationale (directement rattaché au palais de la présidence du gouvernement espagnol), travaillent le Centre de Cryptologie Nationale (CCN, dépendant du Ministère de la défense et du renseignement), le Centre national de Protection des infrastructures et de Cybersécurité (CNPIC, dépendant du Ministère de l'Intérieur) et le Secrétariat d'État à la société de l'information et au numérique (SESIAD, dépendant du Ministère de l'économie). Tandis que le CCN et le CNPIC ont sous leur autorité un centre de réponse d'urgence – le CCN-CERT – responsable des opérateurs de services essentiels publics, l'INCIBE- CERT, sous l'autorité du CNPIC et du SESIAD, assure cette mission pour les opérateurs de services essentiels appartenant au secteur privé.

À cette pluralité institutionnelle s'ajoutent la répartition entre police nationale et garde civile des capacités d'enquête, ainsi qu'une organisation territoriale moins centralisée que celle d'un pays comme la France.

Les différences de modèles au sein de l'Union européenne ne préjugent en rien de l'efficacité de la lutte contre la cybercriminalité ou de la sensibilisation et de la prévention auprès du public et des entreprises dans le cadre national. Mais selon votre rapporteur, elles appuient la nécessité de disposer, dans chaque pays, d'une personnalité politique qualifiée au plus haut niveau, pouvant servir de point de référence à la fois au plan national, mais également dans les instances de concertation européenne.



Source : Centre de cryptologie nationale espagnol

À la difficulté qui se pose pour identifier dans chaque pays de l'Union l'acteur qui pilote réellement de la cybersécurité nationale s'ajoute la différence évidente des moyens dont sont dotés ces organes selon les États. Or, la force d'une chaîne se mesure à l'aune de celle de son maillon le plus faible : force est de constater que si la diversité des modèles n'est pas en soi un obstacle à une cybersécurité européenne robuste, l'effort (budgétaire, mais aussi politique) consacré par chaque pays dans ce champ d'action pèse irrévocablement sur la solidité de toute la cybersécurité européenne. En outre, le caractère plus ou moins centralisé de l'action de chaque pays facilite ou complique l'établissement de relations européennes.

Votre rapporteur ne saurait remettre en cause la volonté de tous les pays membres de se doter d'institutions fiables et de nature à créer l'indispensable architecture de cybersécurité européenne dont le mouvement a été initié par la directive SRI. Il apparaîtrait désormais opportun de faire véritablement monter cet enjeu au sein du débat public, notamment par l'identification d'une personnalité politique nationale chargée de ces questions.

C'est pourquoi votre rapporteur propose la désignation, dans chaque pays, d'un responsable politique susceptible de faire le lien entre les diverses autorités impliquées sur la cybersécurité (pour une action interministérielle et avec les agences existantes le cas échéant), entre les secteurs privé et public de la cyberdéfense et de la cybersécurité aux niveaux national et européen. Cette personnalité devrait agir comme un relais dans l'opinion publique et l'ensemble des personnes désignées dans les États membres pourraient participer aux forums organisés par les instances européennes.

En France, il existe un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, poste précédemment occupé par M. Thierry Delville et non pourvu à ce jour. Votre rapporteur propose que soit envisagée la transformation de cette fonction en un ministère de plein exercice sur les questions de cybersécurité, afin de donner une véritable responsabilité gouvernementale à la personne de référence en France pour la cybersécurité et les industries de la cybersécurité. Cette fonction permettrait une meilleure incarnation politique des enjeux de cybersécurité, dont la qualité transverse cautionne trop souvent la dispersion.

c. Les conclusions mitigées de la Commission sur l'application de la directive SRI

Dans un rapport publié le 28 octobre 2018, la Commission tire un premier bilan de l'application par les États membres de la directive SRI, entrée en vigueur en mai 2018. La période d'évaluation porte de septembre 2018 à novembre 2019 et le rapport se concentre plus précisément sur la façon dont les États membres ont établi les listes d'opérateurs de services essentiels, ce qui était

l'un des objectifs principaux de la directive SRI. Le bilan s'avère mitigé, ce qui était prévisible, la Commission ayant déjà envoyé à l'été 2019 une lettre de mise en demeure à six États membres tardant à opérer la transposition.

Selon le rapport de la Commission, cinq États membres (Autriche, Belgique, Hongrie, Roumanie, Slovénie) n'ont envoyé que des données partielles sur l'identification des opérateurs de services essentiels. En outre, une grande fragmentation demeure quant à l'identification des opérateurs de services essentiels, tant dans la méthode employée par chacun des États membres (avec un degré plus ou moins grand de centralisation des évaluations) que pour les seuils retenus pour la qualification.

L'harmonisation minimale que demande une directive (qui impose une obligation de résultat mais non une obligation de moyens) rend plus complexe la confrontation des données issues des différents pays.

Votre rapporteur ne peut donc qu'adhérer aux conclusions du rapport de suivi de la Commission : si la mise en œuvre de la directive SRI constitue bien un catalyseur pour la cybersécurité européenne, en ouvrant la voie à de réels progrès institutionnels et réglementaires, elle ne constitue qu'une première étape dans la construction d'une véritable ossature de cybersécurité européenne. Elle agit en outre comme le révélateur de faiblesses intrinsèques à certains États membres, qu'il s'agit de corriger rapidement.

C. L'ENISA PÉRENNISÉE DEVRA CONTRIBUER À RENFORCER L'ARCHITECTURE EUROPÉENNE DE LA CYBERSÉCURITÉ

1. L'ENISA : une agence pour diffuser la culture de la cybersécurité et assister les États membres

Comme nous l'avons vu précédemment, l'Union européenne s'est dotée d'un organe chargé de la cybersécurité dès la constitution, en 2004, de l'Agence européenne chargée de la sécurité des réseaux et de l'information. Dès l'origine, les missions confiées par l'Union à l'Agence paraissent très ambitieuses au regard des moyens affectés et du caractère non permanent de son mandat.

En effet, l'article 3 du règlement de 2004 portant création de l'Agence ne lui fixe pas moins de onze tâches dans des directions aussi différentes que le conseil aux pays membres, aux institutions de l'Union ou aux entreprises privées sur la cybersécurité, la sensibilisation du public sur les problématiques de sécurité des réseaux, le suivi des travaux d'élaboration des normes de sécurité et d'évaluation des risques, la promotion de la coopération aussi bien entre les États membres qu'avec les partenaires extérieurs, la création de réseaux de référence et la réalisation d'analyses indépendantes sur les questions de son domaine. Le tout avec une échéance de cinq ans pour horizon, au terme de laquelle serait posée la

question du maintien ou non de l'ENISA. Dès l'institution de l'ENISA, il est en effet prévu que la Commission européenne évalue la pertinence de sa prolongation trois ans après le début de son activité.

Témoignage de l'utilité de l'ENISA, son mandat a depuis été régulièrement prorogé par des actes modificatifs, jusqu'à ce que le règlement de 2013 vienne remplacer celui de 2004 et repréciser les tâches assignées à l'Agence. On note une nette affirmation du caractère opérationnel des missions confiées, avec le renforcement de l'assistance aux États dans la mise en place de CERT nationaux par exemple, tandis que les tâches d'analyse et de facilitation de différentes formes de coopération se maintiennent (entre les organismes publics à des fins de recherche, entre les États membres pour les activités de détection ou de prévention par exemple, avec la possibilité de soutenir l'organisation par l'Union d'exercices de sécurité). L'indépendance de l'Agence est réaffirmée, et elle se dote d'un Conseil exécutif chargé d'assister le Conseil d'administration et d'améliorer le rapport coût/efficacité du travail de l'ENISA, dans un contexte de moyens alloués toujours modestes.

Depuis ses débuts, l'ENISA a effectivement contribué à la diffusion d'une culture et d'une hygiène de la cybersécurité, en fournissant de nombreuses analyses souvent très pointues sur divers aspects des problématiques de sécurité. Le site de l'Agence recense ainsi plusieurs centaines de notes et documents publics destinés à accroître l'information et les préconisations sur des sujets aussi variés que la protection des données, le *Cloud*, les CSIRT, la certification, les stratégies nationales de cybersécurité. Ce fonds documentaire impressionnant apparaît comme la première contribution de l'Agence.

En outre, l'ENISA a organisé jusqu'à présent cinq exercices de cybersécurité paneuropéens de grande échelle, nommés « Cyber Europe », dont le dernier a eu lieu en 2018. Cyber Europe 2018 a réuni près de 900 participants d'institutions publiques et compagnies privées européennes, avec la simulation d'une crise causée par 600 attaques informatiques concomitantes. Ces exercices réguliers donnent l'opportunité aux équipes d'intervention européennes de tester en conditions réalistes leurs protocoles de réponse, et d'éprouver les mérites de coopérations aussi bien transnationales qu'entre secteurs public et privé. Ils constituent selon votre rapporteur l'un des instruments clés sur lesquels pourrait se concentrer l'ENISA future.

2. Certaines faiblesses justifiaient une révision du rôle de l'agence

Depuis sa fondation, et particulièrement sous les deux mandats du Directeur exécutif Udo Helmbrecht, que votre rapporteur a pu longuement rencontrer lors de la visite de l'ENISA à Athènes, l'Agence a gagné en maturité et acquis une expertise reconnue dans le milieu de la cybersécurité.

Toutefois, certaines faiblesses entravaient la pleine efficacité de son action et ont fait l'objet des corrections nécessaires par les règlements successifs. La localisation de l'Agence est évidemment la première difficulté très concrète susceptible d'obérer son efficience. Il faut en effet rappeler que l'Agence était à l'origine basée à Héraklion, en Crète, choix retenu par le pays hôte de l'institution mais qui ne manquait pas de poser des problèmes très concrets d'attractivité et d'organisation, surtout pour une agence dont les membres sont amenés à réaliser de fréquents déplacements dans l'Union. L'ouverture d'un second bureau à Athènes, où s'est concentré ensuite l'essentiel de l'activité de l'agence, a en partie résolu ce problème.

Néanmoins, on ne saurait nier que dans un secteur où la rareté des experts complique les recrutements, la localisation dans un pays ayant subi une crise économique prolongée n'a pas toujours été facteur de facilitation, notamment au regard des opportunités d'emploi pour les conjoints des personnels de l'Agence. Au-delà même du caractère compétitif des rémunérations proposées, c'est tout un cadre de vie qui doit être engagé dans la réflexion sur les recrutements, ce que nous a confirmé l'audition des membres de l'ENISA. Un effort particulier pourrait en outre être porté sur la féminisation de ces recrutements, enjeu récurrent dans les secteurs de l'analyse et de la sécurité.

L'autre caractéristique pouvant poser problème était le caractère temporaire du mandat de l'Agence et ses moyens relativement limités au regard de l'ampleur des missions qui lui étaient attribuées. Au regard des défis croissants et nouveaux posés par la cybersécurité, la Commission a décidé d'avancer la révision du mandat de l'ENISA, prévu pour s'achever en 2020, pour initier une réforme de façon plus précoce.

3. La réforme de l'ENISA s'inscrit dans une relance plus globale de la stratégie de cybersécurité de l'Union

Le paquet cybersécurité comprend un large ensemble de mesures destinées à faire face aux cyberattaques et à renforcer la cybersécurité dans l'Union.

Le 5 juillet 2016, la Commission a publié une communication visant à « renforcer le système européen de cyber-résilience et favoriser la compétitivité et l'innovation dans le secteur de la cybersécurité ». Celle-ci annonce l'adoption à venir de mesures améliorant la gestion de crise européenne en cas d'attaque informatique majeure, le renforcement de la coopération, et la possibilité de mettre en place un cadre européen de certification de sécurité pour les technologies de l'information et des communications (TIC).

Après la révision du mandat de l'ENISA et de la Stratégie pour un marché unique du numérique de 2015, révisée le 10 mai 2017, du fait, entre autres, des progrès encore insuffisants réalisés en matière de cybersécurité, le Président de la

Commission, Jean-Claude Juncker, annonce le 13 septembre 2017 dans son discours sur l'état de l'Union l'adoption d'un « paquet de cybersécurité » composé de quatre textes :

- la communication conjointe de la Commission et de la Haute Représentante de l'Union pour les affaires étrangères et la politique de sécurité : « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide » ;

- la proposition d'Acte de cybersécurité : la proposition COM (2017)0477 de règlement relative à l'ENISA, Agence de l'UE pour la cybersécurité, et abrogeant le règlement (UE) n° 521/2013, et relatif à la certification des TIC en matière de cybersécurité ;

- la recommandation de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs ;

- la communication précisant certaines modalités de mise en œuvre de la directive SRI.

L'année 2017 voit donc la mise en œuvre d'une stratégie coordonnée de cybersécurité à l'échelle de l'Union, visant à faire de l'ENISA un rouage essentiel au cœur d'un réseau d'acteurs et d'institutions multiples.

4. L'ENISA doit devenir un organe de coordination et de soutien aux missions corrélées à ses moyens

Face aux risques de morcellement national et à la sensibilité des questions de souveraineté que soulève l'enjeu de cybersécurité, l'Acte de cybersécurité apporte en effet selon votre rapporteur une pièce majeure à l'édification d'une architecture solide, appuyé par la stratégie de cybersécurité de 2017 proposée par la Commission, et par la recommandation du Conseil sur la gestion des incidents de sécurité. Mais cela, à condition que les missions de l'Agence soient clairement identifiées et strictement corrélées aux moyens dont l'Agence sera dotée dans les années à venir.

Définitivement adopté le 7 juin 2019, le règlement *Cybersecurity Act* consacre une véritable autonomie stratégique de l'Union pour la cybersécurité. Il fait de l'ENISA la pierre angulaire de la cybersécurité européenne en rendant son mandat permanent et en prévoyant que ses moyens et ses objectifs pourront faire l'objet d'une réévaluation régulière. L'Agence européenne chargée de la sécurité des réseaux et de l'information devient avec ce règlement l'Agence de l'Union européenne pour la cybersécurité, ce qui témoigne de sa réorientation et d'une volonté institutionnelle de refonder l'agence sur un mandat plus précis quant à sa vocation.

Les effectifs de l'Agence devraient passer de 95 agents actuellement (selon les données livrées par l'Agence lors de l'audition de ses représentants à Athènes en juillet 2019) à près de 125 personnes dans les prochaines années, de façon à renforcer ses capacités. Le discours sur l'état de l'Union de 2017 du Président Juncker annonçait également une montée en charge graduelle du budget pour passer de 11 à 23 millions d'euros quatre ans après l'entrée en vigueur du règlement.

Le règlement confirme et étend certaines missions déjà assumées par l'ENISA : le soutien et le travail d'analyse des risques et des bonnes pratiques de cyberhygiène, la sensibilisation du public, le soutien aux États dans la mise en œuvre de la directive SRI et l'acquisition de capacités, appui au renforcement de la coopération opérationnelle entre les pays de l'Union.

Le règlement donne également à l'Agence des pouvoirs renforcés, avec la capacité d'établir des enquêtes sur les incidents dans les pays, ou encore un rôle tout à fait central dans le système de certification européen qu'il vise à établir, et sur lequel nous reviendrons dans la suite de notre rapport.

Au-delà du seul règlement de l'Acte de cybersécurité, il convient de souligner l'importance de la recommandation adoptée par le Conseil du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs, qui donne à l'ENISA la responsabilité du secrétariat du réseau des CSIRT mis en place par la directive SRI. Le réseau des CSIRT européen a un rôle de réponse aux incidents de cybersécurité : la recommandation du Conseil place donc l'ENISA au cœur de ce réseau en appui à la réponse aux crises.

Le chef des opérations de l'ENISA, M. Steve Purser, a confirmé à votre rapporteur l'importance de ce « *Blueprint* » pour créer une réponse unique et coordonnée là où, pour l'instant, il n'existe que des réponses sectorielles.

Votre rapporteur souhaiterait toutefois insister sur le niveau de confiance que requiert la mise en place d'une telle coopération entre les CSIRT : s'il apparaît indiqué que l'ENISA contribue à promouvoir et supporter cette coopération, les exercices réguliers prévus par le règlement sont un prérequis indispensable à l'instauration d'une telle confiance.

Autre élément introduit par la recommandation du Conseil et sur lequel les représentants de l'ENISA ont attiré l'attention de votre rapporteur : l'indispensable établissement d'une taxonomie et de modèles communs pour les rapports de situation revenant sur les causes des incidents. L'ENISA aura également un rôle à jouer pour cette forme d'harmonisation. Selon votre rapporteur, cette taxonomie devrait pouvoir s'inspirer des modèles les plus performants existant dans les États membres les plus avancés dans le domaine de la cybersécurité. Cette convergence des modèles doit permettre d'élever le niveau général de la cybersécurité européenne.

5. L'ENISA doit être une agence facilitatrice, mais ne peut ni ne doit devenir l'organe supranational de cybersécurité de l'Union

L'écart existant entre la proposition de règlement de la Commission pour le renouvellement du mandat de l'ENISA et le texte final auquel ont abouti les négociations au sein de l'Union montre bien le caractère encore très sensible des enjeux de cybersécurité, qui touchent à des éléments essentiels de la souveraineté des États.

Le règlement final semble être parvenu à un bon équilibre entre la préservation des prérogatives nationales régaliennes et le renforcement d'une Agence tête de pont de la cybersécurité européenne. Votre rapporteur souhaite particulièrement insister sur cet aspect du mandat de l'ENISA, qui doit à son sens agir comme créatrice de liens entre les États membres et être le fer de lance d'un réseau dont elle ne sera pas un donneur d'ordre supranational. Elle n'en aurait de toute façon pas la légitimité sur des pans aussi souverains de l'action publique.

Face à des menaces susceptibles de frapper de manière rapide et en des lieux multiples, c'est véritablement sur le réseau des compétences nationales que doit venir s'appuyer une agence européenne de la cybersécurité, afin de mutualiser les moyens et de favoriser la concertation nécessaire aux résolutions rapides des crises. La création d'un réseau de liaison d'officiers nationaux sur lesquels pourrait s'appuyer l'ENISA nous parait un point particulièrement positif, et répond d'ailleurs à une demande exprimée par les représentants de l'Agence auditionnés par votre rapporteur.

L'Agence européenne de la cybersécurité ne doit, ni ne peut, se substituer aux agences nationales qui sont les premières à devoir assurer les missions de détection, de diagnostic et de réponse aux crises en matière de cybersécurité. L'ENISA n'aurait de toute façon ni les moyens, ni l'agilité requis pour une telle mission. Elle peut en revanche devenir le point de référence auprès des institutions de l'Union et des États membres, et favoriser l'émergence d'une véritable plateforme de la cybersécurité européenne, susceptible de contribuer à la robustesse des systèmes de défense nationaux en favorisant les collaborations multilatérales.

L'ENISA pourra également utilement accompagner les États les moins avancés sur le terrain de la cybersécurité, sur leur demande, dans l'évaluation des conséquences d'un incident et dans la gestion technique de ses suites. Si ce type d'intervention est conditionné aux requêtes des États et leur permet d'acquérir une expertise et de renforcer leurs capacités de réaction aux attaques, il ne contrevient pas à la subsidiarité et profite à l'ensemble de la cybersécurité européenne. En revanche, il parait peu réaliste de vouloir faire de l'ENISA le pompier volant de la cybersécurité européenne. Selon votre rapporteur, l'action de l'ENISA doit donc être d'accompagner les États membres, auxquels la directive SRI impose de se doter des institutions et moyens appropriés, sans se substituer à leurs réponses en cas de défaillances.

6. Il sera nécessaire de clarifier les liens entre l'ENISA et le futur Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité

Dans un projet de règlement du 12 septembre 2018, la Commission a proposé la constitution d'un réseau de centres de coordination nationaux sur la cybersécurité, qui pourraient bénéficier d'un soutien financier direct de l'Union. Ce réseau serait chapeauté par un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité.

La fin de la mandature de la Commission européenne et du Parlement européen a interrompu les discussions sur le texte, mais votre rapporteur souhaite attirer l'attention sur la nécessité, pour une telle structure, de rester la plus légère possible afin de ne pas faire doublon avec une Agence européenne de la cybersécurité (ENISA) renforcée par l'Acte de Cybersécurité, ou avec les initiatives prises dans le cadre du partenariat public-privé de l'Union sur la cybersécurité.

III. LA CERTIFICATION EUROPÉENNE DOIT DÉFINIR UN STANDARD PERMETTANT DE CONCILIER SÉCURITÉ ET PROSPÉRITÉ

L'autre innovation majeure de l'Acte de cybersécurité réside dans la mise en œuvre d'un système de certification européen, dont la coordination est confiée à l'ENISA. Un tel système pourrait conférer un véritable avantage de compétitivité à l'Union européenne sur le marché mondial de la cybersécurité. Si la certification ainsi constituée se hissait au niveau d'un standard tel que celui du Règlement général de la protection des données, l'Europe pourrait trouver dans la cybersécurité un véritable gisement de croissance.

Outre les enjeux de sécurité et de souveraineté qu'elle emporte du fait de sa nature très régalienne, la cybersécurité doit en effet, selon votre rapporteur, être envisagée comme une opportunité de croissance et de prospérité pour l'Europe.

A. LA CERTIFICATION EUROPÉENNE DOIT COMPOSER AVEC DES CERTIFICATIONS QUI EXISTENT DÉJÀ AUX NIVEAUX NATIONAL ET INTERNATIONAL

Si la certification est un processus qui existe déjà dans plusieurs États membres, la création d'un tel système européen pourrait favoriser une forme d'harmonisation des pratiques au service d'un marché unique du numérique européen, mais aussi l'émergence d'une référence européenne de qualité au plan mondial.

1. La certification existe déjà dans des versions nationales

La certification de cybersécurité consiste selon l'ANSSI en « l'attestation de la robustesse d'un produit réalisée par un évaluateur tiers, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques ». La création des schémas européens de certification prévue par le *Cybersecurity Act* vise à harmoniser les conditions de la certification par les autorités nationales et à favoriser de cette façon à terme la reconnaissance mutuelle des certifications au sein du marché unique.

À l'heure actuelle, la certification de cybersécurité relève strictement des autorités nationales qui peuvent exister ou non au sein des pays de l'Union, sans qu'aucun cadre européen n'établisse d'exigences minimales.

En France, la certification de sécurité des produits dans ce domaine est réalisée sous l'autorité de l'ANSSI. Elle répond à trois objectifs [(1)] :

(1) Ces informations sont issues du site de l'ANSSI : voir le document https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf

- des objectifs réglementaires, certains règlements nationaux ou européens imposant un niveau élevé de sécurité aux solutions utilisées dans des domaines sensibles par exemple ;

- des objectifs contractuels, imposés par des donneurs d'ordres qui exigent des visas de sécurité ;

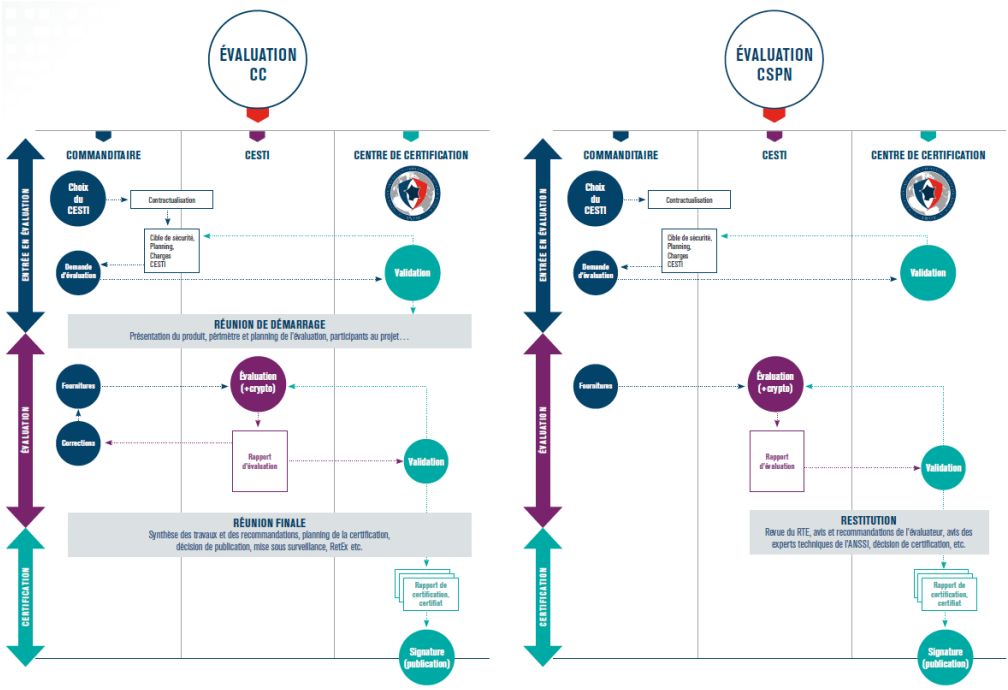
- des objectifs commerciaux, l'obtention d'un visa de sécurité étant le gage d'un niveau élevé d'exigence par le respect de certaines normes prédéfinies ; le visa de sécurité s'avère alors un avantage comparatif sur un marché donné.

La certification consiste à s'assurer de la conformité d'un produit (en référence à certaines attentes de sécurité) et à tester la vulnérabilité de ce produit aux menaces contre la sécurité.

Le schéma français offre deux types de certification, une certification de sécurité de premier niveau (CSPN) et une certification dite « critères communs » (CC). Tandis que la certification CC répond à un standard international doté de sept niveaux d'assurance de plus en plus élevés, la certification CSPN a été élaborée par l'ANSSI pour fournir une solution de certification répondant à un risque plus modéré, et mettant en jeu une évaluation moins exhaustive.

Ces deux types de certification engagent notamment le type de laboratoire d'analyse technique, nommé Centre d'évaluation de la sécurité des technologies de l'information (CESTI), qui pourra mener l'évaluation. Pour une évaluation CC, le CESTI devra avoir été lui-même accrédité par le Comité français d'accréditation (le Cofrace) à l'aune de standards internationaux, et agréé par l'ANSSI. Pour une évaluation CSPN, le laboratoire devra simplement bénéficier d'un agrément de l'ANSSI.

L'ANSSI exerce un contrôle continu sur les évaluations. Si ce contrôle est gratuit, les frais d'évaluation d'un produit par un CESTI sont à la charge du commanditaire de l'évaluation. Il convient de souligner que dans d'autres pays, comme en Allemagne, le contrôle par l'autorité nationale (en l'occurrence, le BSI) peut entraîner des frais.



Source : ANSSI

2. Des standards internationaux préexistent également

Le besoin de reconnaissance mutuelle des certifications se comprend aisément pour les industriels du secteur. Les processus d'évaluation et de certification engagent du temps et des moyens qui grèvent d'autant la mise sur le marché des produits qui y sont soumis. Permettre qu'une certification opérée dans un État soit reconnue dans un autre représente donc un gain d'efficience pour les entreprises. En ce sens, la certification rencontre le même type de problématique que les brevets d'exploitation.

Des formes de standardisation des exigences de cybersécurité existent déjà actuellement. Le SOG-IS (pour *Senior Official Group – Information Security*) est ainsi un regroupement de quatorze pays européens permettant la reconnaissance entre les États signataires des certificats « critères communs » délivrés par leurs autorités par défaut jusqu'à un certain niveau de certification. Cet accord intergouvernemental a été mis à jour en 2010.

L'accord du CCRA (*Common Criteria Recognition Arrangement*) regroupe, lui, un plus grand nombre de pays et est applicable depuis 2014. Parmi les pays de l'accord, certains disposent d'organismes de certification qualifiés chargés d'émettre des certificats, tandis que d'autres États reconnaissent ces certificats sans en émettre eux-mêmes. Un tel type d'accord permet donc de regrouper des États fournisseurs et consommateurs de certification, et des États

uniquement receveurs, établissant ainsi une forme de complémentarité qui pourrait se retrouver dans le futur système de certification de l'Union européenne.

Des formes de coopération internationale existent donc déjà : il convient que la certification européenne proposée par le règlement s'inspire de ce qui fonctionne dans ces processus et ne soit pas redondante, ce qui serait contreproductif.

B. SUR LA BASE DE CES ACQUIS, LA CERTIFICATION DOIT DEVENIR UN AVANTAGE COMPARATIF POUR LA CYBERSÉCURITÉ EUROPÉENNE

1. Le système prévu par le règlement

a. Le règlement européen prévoit une certification facultative et sur trois niveaux :

- un niveau élémentaire pour des produits destinés au grand public, avec la possibilité d'une auto-évaluation de conformité (le producteur de l'objet ou du service s'engage à remplir certains critères de sécurité) ;

- un niveau substantiel, pour lequel entre en jeu un tiers de confiance accrédité qui effectue des tests de conformité ;

- un niveau élevé, qui voit s'ajouter aux tests de conformité, exigés pour le niveau substantiel, des tests de pénétration (soit des tentatives d'attaque du système évalué), en raison de la gravité des conséquences d'une potentielle faille de sécurité.

Ce système de certification européenne doit conduire à une meilleure lisibilité pour les utilisateurs et à une montée des exigences pour tous. Selon votre rapporteur, il ne s'agit pas de mettre certains pays en mesure de délivrer des « certificats de complaisance » en se prévalant d'un standard européen. La certification européenne ne doit pas mener à un nivellement par le bas mais bien entraîner l'ensemble des acteurs vers les niveaux de normes les plus élevés déjà pratiqués par les acteurs les plus exigeants.

b. Certains aspects du rôle de la Commission européenne et de l'ENISA dans la certification seront à préciser dans la pratique

Le règlement sur l'Acte de cybersécurité accorde à l'ENISA et à la Commission un rôle primordial dans la future certification européenne. En effet, le futur cadre européen de certification de cybersécurité reposera sur un programme

de travail établi par la Commission elle-même [1] (qui établira des priorités stratégiques pour les schémas européens de certification à venir et des listes des produits, services, et processus des technologies de l'information) et des communications qui feront l'objet de schémas.

Plusieurs motifs pourront justifier l'inclusion des schémas de certification à élaborer dans le programme de travail glissant, comme la demande du marché, l'évolution de la situation des cybermenaces, la disponibilité ou le développement de schémas nationaux, pour éviter un risque de fragmentation. Il faut toutefois noter, et votre rapporteur souhaite le souligner, que l'inscription dans le programme de travail ressortira *in fine* d'une décision de la Commission. Celle-ci devra tenir compte de l'avis du groupe des parties prenantes et du Groupe européen de certification de cybersécurité (GECC), qui sera composé des représentants des autorités nationales de certification compétentes ou d'autres autorités nationales désignées.

Au vu des divergences, voire des dissensions, qui peuvent parfois exister au sein des différentes directions de la Commission actives sur les sujets de cybersécurité, il sera important de veiller à ce que la stratégie européenne en matière de certification suive une ligne claire, sans toutefois manquer de la réactivité nécessaire eu égard au caractère imprévisible des enjeux de la cybersécurité. Le premier programme de travail devrait être publié au plus tard le 28 juin 2020.

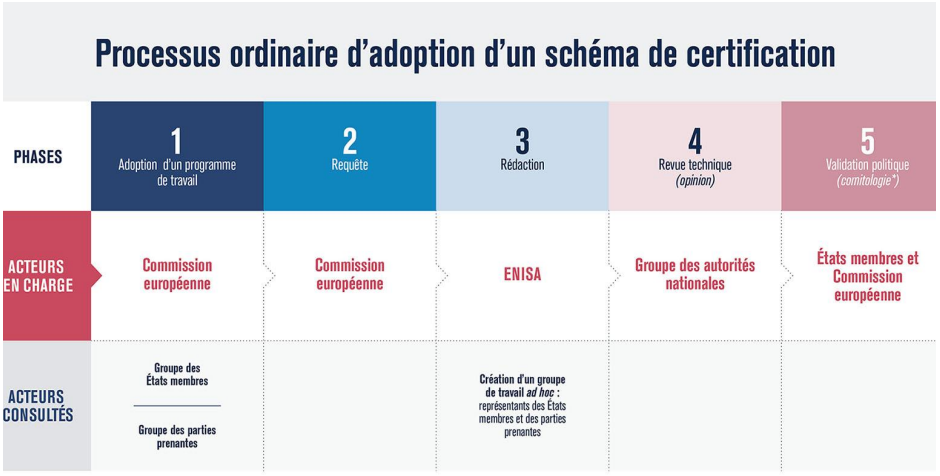
En outre, c'est sur la demande de la Commission que l'ENISA sera chargée de préparer un schéma candidat sur la base du programme de travail, et c'est seulement si ce schéma n'est pas inclus dans le programme de travail que la demande pourra provenir du GECC, et dans des « cas dûment justifiés », sans que cela soit précisé de quelle manière par le règlement. La Commission dispose donc d'un avantage d'initiative sur les autorités nationales de certification composant le GECC quant aux demandes de préparation de certificat.

La préparation du schéma est ensuite prise en charge par l'ENISA et devient une des missions essentielles de l'Agence. L'ENISA doit mener une consultation formelle et constituer un groupe de travail *ad hoc* d'experts pour chaque schéma. La constitution de ces groupes, dont les modalités devront être fixées par le règlement interne de l'ENISA, devra faire l'objet d'une attention particulière, selon votre rapporteur, à la fois pour représenter toutes les sensibilités européennes, mais également pour que tous les acteurs concernés puissent disposer de capacités à apporter leur expertise propre.

La décision repasse ensuite du côté de la Commission, qui pourra adopter des actes d'exécution afin de prévoir les schémas de certification européens sur la base de la proposition de l'ENISA.

---

(1) Le « programme de travail glissant de l'Union pour la certification européenne de cybersécurité », comme l'indique l'article 47 du règlement 2019/881 du 17 avril 2019



Source : ANSSI

2. Les points d'attention dans la mise en œuvre prochaine du règlement

a. La multiplication des enceintes

Comme nous l'avons souligné plusieurs fois, le domaine de la cybersécurité recouvre des enjeux très transverses et ses acteurs sont naturellement très divers et fragmentés. À ce titre, votre rapporteur souhaite attirer l'attention sur le fait que, sous couvert d'implication maximale des acteurs, le règlement de cybersécurité introduit encore de nouveaux groupes et de nouvelles enceintes de discussion qui contribuent à une complexification et un manque de lisibilité institutionnels.

Ainsi, l'Acte de cybersécurité prévoit la création pour l'ENISA [(1)] d'un groupe consultatif. Ce groupe, dont la création sera entérinée par le conseil d'administration de l'ENISA sur proposition du directeur exécutif de l'Agence, sera composé d'experts et de représentants du secteur privé. Le groupe consultatif jouera un rôle dans l'élaboration du programme de travail annuel de l'Agence.

Votre rapporteur estime que si la consultation de partenaires extérieurs à l'ENISA apparaît indispensable pour définir ses objectifs et sa stratégie, la création d'un nouveau groupe consultatif n'était peut-être pas indispensable et risque au contraire de nuire à la lisibilité de la nouvelle organisation de l'ENISA, alors même que les groupes et institutions sont déjà fortement éparpillés dans le

(1) Article 21 du règlement 2019/881 du 17 avril 2019.

domaine de la cybersécurité. Était-il véritablement nécessaire d'institutionnaliser un tel collège de représentants, alors qu'existe déjà depuis 2016 un partenariat public-privé permettant une telle représentation auprès de l'ENISA, par le biais de l'organisation ECSO [(1)] ?

De la même façon, pour le versant certification du règlement, un groupe des parties prenantes pour la certification est également institué. Votre rapporteur ne peut que saluer la volonté de créer des processus consultatifs ouverts pour l'élaboration des schémas de certification de cybersécurité. Il apparaît opportun, pour une agence telle que l'ENISA, de travailler en réseau en mobilisant les meilleures expertises. Toutefois, votre rapporteur s'interroge là aussi sur la nécessité d'institutionnaliser de telles formations. Le règlement ne fixant pas les règles inhérentes à la constitution du groupe des parties prenantes, il conviendra de rester attentif à ses règles de composition. Un tel groupe doit atteindre l'équilibre délicat entre la fourniture d'une expertise adaptée et l'adéquation aux besoins réels du marché, sans pour autant pouvoir être soupçonné de conflit d'intérêts en représentant tel ou tel secteur concerné par les enjeux de cybersécurité.

Selon votre rapporteur, l'ENISA exerce le mieux ses missions lorsqu'elle réussit à mobiliser des réseaux d'experts et à faire travailler ensemble des communautés, nationales, ou sectorielles, déjà constituées mais se parlant peu. Elle doit, selon lui, continuer à jouer ce rôle de plateforme et se nourrir des correspondances qu'elle parvient à établir dans tous les pays de l'Union.

À ce titre, l'instauration d'un réseau d'officiers de liaisons nationaux avec le règlement de 2019 est une bonne nouvelle. Mais il reste permis de s'interroger à nouveau sur la coordination qui adviendra avec d'autres cercles, comme le groupe de coopération institué par la directive SRI, qui fonctionnait déjà fort bien, et de la pertinence à les multiplier.

Selon votre rapporteur, le groupe de coopération de la directive SRI constitue un modèle qui devrait inspirer les nouvelles structures créées. En raison de son fonctionnement souple et pragmatique, il permet aux acteurs un apprentissage par la pratique qui mène à des coopérations efficaces. Ce type de fonctionnement peu formalisé répond bien aux exigences de la cybersécurité : réactivité, collaborations au cas par cas et renforcement de la confiance par des expériences partagées.

b. La prise en compte des schémas existants

Dans plusieurs États membres, nous l'avons vu, il existe déjà des schémas de certification horizontaux ou sectoriels, et ces schémas se sont encore

(1) European Cybersecurity Organisation

développés depuis la directive SRI, qui imposait des obligations spécifiques de sécurité aux opérateurs de services essentiels.

Le règlement examine l'articulation entre les schémas nationaux et les schémas européens selon plusieurs cas de figure :

- les schémas nationaux déjà existants resteront valables jusqu'à leur date d'expiration, même après la mise en place d'un schéma européen portant sur le même objet ;

- dans le cas où un schéma européen existe, les États membres doivent s'abstenir de produire de nouveaux schémas nationaux ;

- dans le cas où un ou des États membres souhaiterait créer un schéma de certification national sur un secteur non couvert par un schéma européen, il devrait en informer la Commission et le Groupe européen de certification de cybersécurité ; une initiative pourrait alors être prise pour créer un tel schéma plutôt au niveau européen en l'incluant dans un programme de travail modifié.

La question demeure toutefois de l'harmonisation qui sera effectuée pour que des schémas européens succèdent à des schémas nationaux existants, qui conserveraient des particularités ou exigences nationales spécifiques, en dépit des cadres d'harmonisation internationaux tels que le SOG-IS ou le CCRA. Il est en outre possible d'imaginer que certains secteurs industriels puissants dans un ou plusieurs États membres cherchent à imposer leurs modèles au niveau européen au détriment d'autres États membres. Pour que la reconnaissance mutuelle fonctionne au mieux, la concertation la plus aboutie devra être de mise.

C'est pourquoi votre rapporteur est d'avis que l'application du règlement devra mettre en lumière le gain de tous les acteurs européens à « jouer collectif » pour que les standards communs s'imposent et deviennent la signature d'une qualité européenne compétitive au niveau mondial. Pour la certification, la prospérité espérée se joue à la fois au niveau interne, avec le potentiel d'approfondissement du marché unique du numérique qu'emporte la simplification d'une reconnaissance mutuelle, et au niveau externe, avec l'affichage sur la scène mondiale d'un label d'excellence européen en matière de cybersécurité.

Il faudra pour cela respecter un juste équilibre entre une certification à l'exigence trop élevée (en termes de temps, de coûts, d'assurance du risque), qui pourrait décourager une démarche de certification qui reste encore volontaire, et une exigence trop faible qui viderait de son sens la certification si elle ne prévient pas réellement des menaces.

c. La question du périmètre des schémas de certification de sécurité

Une des interrogations récurrentes chez les nombreux acteurs du secteur des technologies de l'information et de la communication porte sur le périmètre des schémas de certification, et la nécessité, dans la définition d'un programme de travail et d'une stratégie européenne, de procéder de façon méthodique. Votre rapporteur estime qu'il aurait été utile, au préalable, de se poser certaines questions sur la nature des projets de schémas à venir : doivent-ils correspondre à des secteurs industriels, à des types de produits ? Faut-il chercher à travailler sur des schémas très larges, horizontaux, ou au contraire à spécialiser ceux-ci sur une verticale plus précise ?

Selon votre rapporteur, les parties prenantes auront ici un rôle crucial à jouer, mais l'ENISA devra veiller à permettre le dépassement des clivages sectoriels pour faciliter une approche transversale des schémas entre plusieurs branches d'activité. Il s'agit là aussi de trouver un juste équilibre entre la précision d'un modèle au plus près de toutes les spécificités sectorielles et la souplesse d'un type de schéma plus large.

d. La difficile conciliation entre réactivité et stabilité des schémas de certification

Cet équilibre à trouver pose également la question de la temporalité de la certification de cybersécurité. Le règlement pose des jalons très larges : un programme de travail glissant mis à jour au moins tous les trois ans (« et plus souvent si nécessaire » [(1)]) et une évaluation des schémas adoptés par l'ENISA « au moins tous les cinq ans ». Mais le règlement reste, selon votre rapporteur, trop imprécis sur la nécessaire célérité avec laquelle l'élaboration des schémas de certification devra être menée pour leur donner une valeur véritablement opérationnelle sur le marché.

En outre, la question importante des mises à jour et de la possible révision partielle des schémas de certification emporte également des problématiques de délai et de réactivité. Les produits et systèmes des technologies de l'information et de la communication progressent en effet souvent de façon incrémentale, par ajouts successifs, modifications et correction d'erreurs. Il est donc peu envisageable de reprendre à chaque étape un processus assez contraignant de certification. En outre, la part logicielle de l'exposition aux cyberattaques, dont nous avons vu qu'elle ne fera qu'augmenter, rend cette problématique particulièrement aiguë. Pour que la certification devienne un atout de compétitivité de l'Europe en garantissant des produits plus surs, il faut à tout le moins qu'elle permette une mise sur le marché dans des délais rendant possible la compétition avec d'autres produits.

---

(1) Article 47 du règlement 2019/881 du 17 juin 2019.

TRAVAUX DE LA COMMISSION

La Commission s'est réunie le jeudi 14 novembre 2019, sous la présidence de Mme Sabine Thillaye, Présidente, pour une table ronde sur la cybersécurité et la présentation du rapport d'information de M. Éric Bothorel sur l'avenir de la cybersécurité européenne.

I. TABLE RONDE SUR LA CYBERSÉCURITÉ EN PRÉSENCE DE M. JUHAN LEPASSAAR, DIRECTEUR EXÉCUTIF DE L'ENISA, M. STEVE PURSER, DIRECTEUR DES OPÉRATIONS DE L'ENISA, M. JEAN-BAPTISTE DEMAISON, PRÉSIDENT DU CONSEIL D'ADMINISTRATION DE L'ENISA, ET M. CYRIL CUVILLIER, SOUS-DIRECTEUR ADJOINT DE LA STRATÉGIE DE L'ANSSI

Mme la Présidente Sabine Thillaye. La cybersécurité, sujet de la table ronde qui nous réunit aujourd'hui, est d'une brûlante actualité. 80 % des entreprises européennes auraient été victimes d'attaques informatiques, ce qui pose la question de l'action de l'Union européenne en matière de prévention de celles-ci, mais aussi en termes de réaction. La cybersécurité est également un enjeu technologique et industriel majeur car elle constitue un marché qui ne doit pas être abandonné aux entreprises américaines ou chinoises.

Pour nous éclairer sur ces enjeux ainsi que sur la politique européenne en matière de cybersécurité, nous accueillons M. Juhan Lepassaar, directeur exécutif de l'ENISA, l'Agence européenne de cybersécurité, M. Steve Purser, directeur des opérations de l'ENISA, M. Jean-Baptiste Demaison, président du conseil d'administration de l'ENISA et M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Je tiens en préalable à vous remercier pour cette invitation à présenter le point de vue de l'ENISA sur la cybersécurité et la France pour le soutien qu'elle apporte à notre Agence. Je souligne également la très bonne coopération entre l'ENISA et les différentes agences nationales, parmi lesquelles l'ANSSI.

Je commencerai mon intervention par rappeler que l'Union européenne avait une opportunité unique d'établir un cadre de régulation qui pourrait devenir une norme internationale en matière de cybersécurité. Elle l'a saisie en adoptant la directive SRI qui constitue le cadre actuel de protection des infrastructures critiques contre les attaques informatiques : réseaux énergétiques, de transport, de santé, financiers… L'Union européenne est la seule à disposer d'un tel cadre, utile aux États membres comme aux citoyens, qui doit certes être renforcé et opérationnalisé. Quant à l'Acte sur la cybersécurité, entré en vigueur cette année,

il représente une opportunité à saisir pour accroître la production et la distribution de produits et services liés à la cybersécurité.

S'agissant maintenant plus précisément de l'ENISA, celle-ci a deux missions principales. La première est d'aider l'Union européenne et les États membres à avoir une approche commune des enjeux liés à la cybersécurité. Par exemple, s'agissant de la 5G, l'ENISA a contribué, avec la Commission européenne et les États membres, à cartographier et évaluer les risques, ainsi qu'à déterminer les moyens de les réduire. L'ENISA assure également le secrétariat du réseau des CSIRT européens, qui permet l'échange d'informations et d'expériences sur les attaques informatiques. En d'autres termes, même si tous les experts européens ne travaillent pas pour elle, l'ENISA a un rôle majeur d'animation de la communauté cyber européenne.

La deuxième mission de l'ENISA est la certification en matière de cybersécurité. Plus précisément, elle travaille, par l'intermédiaire de groupes de travail composés notamment d'experts nationaux, à établir des normes communes de certification, pour les objets connectés ou les réseaux systémiques.

M. Steve Purser, directeur des opérations de l'ENISA. L'ENISA, qui ne dispose que de 70 collaborateurs, est avant tout une agence de coopération. Elle travaille étroitement avec les Agences nationales de cybersécurité ainsi qu'avec les entreprises privées. Parmi les sujets dont elle s'occupe, je voudrais citer l'intelligence artificielle, la 5G, l'économie et la souveraineté numérique, les *fake news*, l'économie de la cybersécurité et la sécurité informatique.

Pour l'intelligence artificielle, vous êtes sans doute au courant que la Commission étudie actuellement la partie éthique du sujet. L'ENISA, avec son conseil d'administration, a défini une première tâche pour l'année prochaine, qui est principalement de comprendre l'intelligence artificielle (IA) du point de vue de la cybersécurité, et d'assurer une base de cybersécurité dans l'IA elle-même. Beaucoup de gens parlent de garantir la sécurité grâce à l'IA ; pour notre part, nous voulons être certains que l'IA elle-même est bien sécurisée.

Je pense que nous serons rapidement dans les contenus : comment combattre la *fake logic* par exemple ? Cela m'amène à un commentaire très important : le sujet qui revient sans cesse est celui de la sécurisation des logiciels dès leur conception, puis au cours de leur existence. C'est très difficile, mais je pense que c'est à la base de beaucoup de problèmes.

Plusieurs choses nous empêchent de faire cela. Le nombre de lignes de codes dans une voiture est d'environ 100 millions à l'heure actuelle. Vous imaginez le travail nécessaire pour sécuriser un tel volume. Or, on cherche aussi des méthodes économiquement viables, qui marchent en un temps et à un coût raisonnables.

Je ne vais pas beaucoup parler de la 5G, mais simplement dire que c'est d'une complexité énorme. Il faut procéder lentement mais sûrement. Ce n'est pas

un concept fixe : les normes évoluent au jour le jour, ce qu'il faudra prendre en compte. La sécurité a trois aspects : les gens, les processus et la technologie. En l'espèce, le processus est très important.

Je souhaiterais insister sur la notion d'autonomie stratégique numérique. Cela signifie que chaque État membre contrôle sa propre infrastructure, tout comme l'Union européenne. Cela ne signifie pas que les États membres doivent fabriquer totalement les infrastructures, mais qu'ils contrôlent la chaîne d'approvisionnement et que rien n'est ajouté dans leurs produits sans leur consentement.

J'aimerais également évoquer le concept de souveraineté numérique. Il correspond à l'idée qu'en Europe, et c'est très vrai de la France, il y a une compétence très poussée en matière de cybersécurité. On peut l'utiliser en lien avec notre politique industrielle et pour stimuler nos marchés. Vous avez sans doute constaté le lancement de discussions sur un *Cloud* européen, Gaia.

Enfin, les *fake news* et la désinformation sont un sujet important. Vous vous interrogez peut-être sur le rapport avec la sécurité informatique. En réalité, nous nous préoccupons de tout ce qui est trompeur (le *bad looking good)*. Les fausses nouvelles ne font pas exception. Nous avons un rôle à jouer en la matière.

Pour finir, j'aimerais dire quelques mots de la dimension économique de la cybersécurité. L'Union européenne et les États membres dépensent des sommes considérables mais il existe très peu d'instruments pour en mesurer l'impact. Il faut essayer de trouver des données sur le retour sur investissement. Les études, quand elles existent, sont insuffisantes. Quelqu'un doit commencer à vous donner les informations de base relatives aux effets de vos décisions, tant au niveau macro que microéconomique.

Vous avez sans doute entendu parler du débat sur les ordinateurs quantiques, qui vont changer la sécurité d'une façon radicale. Dès qu'on a un ordinateur quantique, le système de cryptographie est mis à plat. Depuis longtemps, nous travaillons sur la réponse, qu'est la cryptographie post-quantique. À mon avis, cela mérite d'être défendu. Nous serons dans quelques années dans une situation difficile, si nous ne réagissons pas. Sur le calcul quantique en lui-même, beaucoup de gens préconisent de l'utiliser pour faire de la cryptographie. Toutefois, il faut être prudent : à l'ENISA, nous ne voyons pas la pertinence de ce procédé très coûteux pour le moment.

L'ENISA est ici pour vous soutenir, en tant qu'État membre, mais aussi comme État qui dispose d'une agence de cybersécurité très développée. Nous sommes à l'écoute de vos conseils

M. Cyril Cuvillier, sous-directeur de la stratégie de l'ANSSI. Nous sommes très heureux d'avoir été conviés ce matin et qu'un rapport d'information ait été rédigé pour informer les parlementaires.

Je souhaite dire quelques mots sur la manière dont l'état de la question cyber est perçu à l'échelle européenne. La législature précédente a fait un énorme travail en posant des fondations. Cependant, chaque sujet qui a avancé n'est que le premier étage d'une structure à consolider. Nous devons faire preuve de vigilance et ne pas passer immédiatement aux sujets suivants. Il faut encore rationaliser, piloter, améliorer les démarches entreprises.

D'abord, nous avons renforcé la résilience de l'Union face aux risques cyber. Il faut évidemment citer la directive NIS (ou SRI). Elle s'intéresse au cadre de sécurité sur les infrastructures dites critiques. En France, nous avions un modèle déjà bien développé pour les infrastructures vitales, mais l'Europe a commencé à parler d'opérateurs essentiels à la prospérité économique. Cette démarche a très bien démarré et elle se poursuit ; un de nos rôles dans les prochaines années est d'observer comment cela se poursuit.

La question est la façon de résoudre des crises à l'échelle européenne. Nous avons réalisé qu'il fallait pouvoir échanger entre nous à un niveau plus opérationnel et plus stratégique, de manière à ce que les États membres réfléchissent entre eux. La France a accueilli le 2 juillet dernier un exercice de cette nature, avec la grande majorité des directeurs d'agences et de structures nationales. Il va probablement avoir à nouveau lieu, parce que nous nous sommes rendu compte qu'il était nécessaire d'avoir ce niveau de préparation aux crises.

Au cours de cette législature, nous nous sommes aussi rendu compte que la sécurité des institutions européennes elles-mêmes doit faire l'objet d'une vigilance régulière. Il ne faut pas prendre la sécurité comme acquise, comme en témoignent certains incidents qui ont fait l'objet de communications officielles.

Enfin, je souhaite aborder la question de la résilience. Le travail a beaucoup avancé dans le domaine de l'édification d'un réseau industriel. Comment faire émerger une industrie apte à répondre au défi de la confiance dans le domaine du numérique ? La législature qui se termine a donné lieu à une expérimentation autour d'un partenariat public privé. Ce sujet va perdurer sous la forme d'un texte sur un centre de compétences, qui vise à mieux structurer les compétences dans le temps, mieux flécher les budgets de recherche. L'objectif est de faire émerger un réseau industriel pour répondre au défi d'autonomie stratégique dans le domaine du cyber. Nous devons être très aidants dans la relation dans la relation entre nos moyens budgétaires et les moyens de l'industrie.

Le troisième point, qui n'est pas à négliger, est le développement d'outils diplomatiques. Nous avons vu que les crises ont une dimension diplomatique. Les politiques ont besoin que nous sachions les accompagner d'une lecture technique. Des textes ont été générés au cours des dernières années.

Nous sommes persuadés que l'échelle européenne est la bonne pour traiter ces sujets. En même temps, nous nous assurons que les textes intègrent des exceptions de souveraineté, par exemple dans le cas de la certification des produits

cryptographiques. Dans les domaines régaliens, nous souhaitons pouvoir mener les projets qui nous semblent nécessaires. Toutefois, de manière générale, pour rendre les producteurs responsables, en appeler à des démarches qui standardisent les efforts qu'on leur demande, l'Union européenne est le bon niveau.

Nous l'avons vu avec le RGPD : la force d'un texte de ce périmètre a été absolument magistrale dans la prise de conscience des responsables. On peut alors obtenir un impact réel.

L'ENISA est une agence qui est au cœur de cela car elle apparaît, au sein des entités de l'Union européenne, comme un lieu vers lequel se tourner lorsque des questions se posent. Les parlementaires européens veulent savoir ce qu'est la « *blockchain* », le « quantum » et tous ces concepts complexes. Il faut donc que nous ayons un centre qui soit non pas expert mais en capacité de repérer que tel État membre a écrit un texte intéressant sur ce sujet et que c'est ce texte-là qu'il faudrait lire en premier, que tel État membre dispose de compétences qui peuvent nous aider à appréhender le sujet.

Sur la 5G, l'ENISA se pose en animateur d'un effort collectif des États membres pour rédiger un document qui analyse le risque, non pas dans l'idée de dessaisir les États du problème mais de proposer de le résoudre, en invitant les États à développer leurs expertises, leurs analyses de risque, leurs stratégies politiques. L'ENISA a montré au cours des dernières années le rôle remarquable qu'elle a joué. Quand on considère par exemple la question de la sensibilisation de nos concitoyens, l'ENISA organise un mois européen de la cybersécurité tous les ans. Quand nous parlons de renforcer le rôle des étudiants dans l'informatique et le cyber, il s'agit d'un challenge européen animé par l'ENISA. La France s'inscrit, comme les autres États, dans cette démarche, les incitant à s'inscrire à ce challenge et les étudiants se prêtent à cet exercice.

Il faut que nous apprenions à nous entraîner à l'échelle européenne et l'ENISA encadre la mise en œuvre de « cyber Europe », exercice de dimension européenne très utile pour convenir de méthodes partagées. Nous avons également évoqué le réseau de CERT qui profite beaucoup du soutien de l'ENISA.

Il faut aller au-delà et nous nous réjouissons que l'ENISA, après plusieurs mandats provisoires, se soit installée dans un mandat définitif, durable, sous la forme d'une agence européenne. Nous sommes heureux que la France, en la personne de Jean-Baptiste Demaison, se soit vue à nouveau confier la présidence du conseil d'administration de l'ENISA. Monsieur Demaison occupait déjà cette fonction et a été renouvelé à l'unanimité par ses collègues, signe d'une réelle adhésion à sa démarche de travail. Cette démarche vise à continuer les efforts par lesquels l'ENISA doit impliquer les expertises des États membres pour fédérer ce travail, comprendre les nouveaux sujets et aider les États à renforcer leurs capacités.

M. Jean-Baptiste Demaison, président du Conseil d'administration de l'ENISA. Le Conseil d'administration de l'ENISA est composé de vingt-huit États membres et de deux représentants de la Commission européenne. Notre travail est de doter l'ENISA d'un programme de travail et plus généralement d'orientations stratégiques guidant son action. Je suis par ailleurs également agent de l'ANSSI et conseiller du sous-directeur à la stratégie de cette agence nationale.

Les précédents intervenants ont parlé des défis politiques et technologiques pour l'Europe, de l'enjeu de la souveraineté numérique de l'Union européenne et de l'autonomie stratégique en matière de sécurité. Je crois que nous abordons en 2020 une nouvelle ère pour la cybersécurité européenne. Le cadre européen de certification devrait permettre à l'avenir de relever significativement le niveau de sécurité des solutions et services numériques utilisés par les administrations, les entreprises et les citoyens européens. Il s'agit d'un pas de géant et l'ENISA est appelée à jouer un rôle central et opérationnel dans le fonctionnement de ce réseau. C'est une nouvelle ère, car l'enjeu est gigantesque pour relever le niveau de cybersécurité de l'ensemble de l'Union. L'ENISA devra plus que jamais jouer un rôle de facilitatrice active qui ne se contente pas de mettre les gens autour de la table, mais qui fasse émerger une expertise européenne et progresser les États membres dans leurs capacités nationales, tout en renforçant la coopération entre les agences nationales en matière opérationnelle.

J'utilise le concept « d'agence-plateforme », qui permet de prendre et rendre le meilleur à la communauté européenne. Ce changement dans le panorama des défis pour la cybersécurité occupe beaucoup le conseil d'administration. Je conclurai en disant que l'enjeu dans les mois à venir est de doter l'agence d'une nouvelle stratégie, afin de fixer des objectifs à cinq ans. Nous nous félicitons de la nomination de Juhan Lepassaar comme nouveau directeur exécutif de l'agence. Il s'agit d'un moment pivot pour l'agence et nous ferons en sorte d'accompagner le nouveau directeur exécutif dans ses missions face aux défis évoqués.

Mme la Présidente Sabine Thillaye. Est-ce que ce sujet de la cybersécurité, auquel nous avons donné un cadre, prend suffisamment en compte les PME et les personnes physiques ? Nous avons tous une responsabilité quant à l'utilisation des outils informatiques à notre disposition. Une revue juridique parlait de « monstre doux » pour désigner ces technologies. Nous nous faisons d'une certaine manière happer par les facilités que tous ces outils nous offrent, sans tenir compte de la nécessité de se protéger en tant que personne privée. Je souligne que pour les PME il est parfois complexe de s'informer et de faire les démarches nécessaires.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. La cybersécurité ne s'applique pas uniquement aux entreprises informatiques ou à l'industrie. Sa fonction primaire est de protéger la société. L'ENISA travaille sur la sensibilisation dans toute l'Europe avec différentes mesures, par exemple le mois « cyber ». Nous collaborons avec des entités européennes et nationales pour avoir

des supports de sensibilisation à distribuer dans l'Union européenne. Mais la tâche la plus importante pour l'ENISA et pour toutes les autorités de cybersécurité est de promouvoir la cybersécurité par défaut, intégrée dans les solutions. Il vaut toujours mieux sécuriser l'infrastructure avant une crise, plutôt que de retourner en arrière et d'essayer de réparer les failles.

Intégrer la sécurité dans la conception des outils est une tâche que je prends très à cœur et c'est une nécessité qui découle de l'acte de cybersécurité. Il nous incombe de trouver des mécanismes pour faire en sorte que les fabricants créent des outils qui soient déjà sécurisés. On ne peut pas présumer que les consommateurs soient experts dans la cybersécurité et sachent déjà comment protéger les services qu'ils utilisent. Il y a des fonctionnalités basiques que tout le monde connaît, comme mettre à jour les logiciels régulièrement, ce qu'il faut faire car cela protège les systèmes. Mais cela devrait être automatique.

Mme la Présidente, vous avez parlé des PME : lorsqu'on met en œuvre ce nouveau cadre de régulation, il faut toujours garder les PME à l'esprit. L'acte sur la cybersécurité, en ce qui concerne la certification, a déjà une approche proportionnée. Il y a différents niveaux de certification : on peut avoir une auto-certification, plus simple pour les PME, puis un niveau supérieur qui serait une certification validée par un tiers, ce qui coûte plus cher et prend plus de temps. Toutes les PME n'ont pas le temps ou les moyens nécessaires pour se faire certifier par un tiers. Il est nécessaire d'aider les PME, les petits employeurs et les *start-up* à se sécuriser et à utiliser le cadre de régulation. Un système d'auto-certification constitue la première étape.

M. Éric Bothorel, rapporteur. Avant d'entrer dans le détail au travers du rapport qui m'a été confié, je voudrais revenir sur plusieurs points qui ont été évoqués. Le directeur de l'ANSSI voit la cybersécurité comme « positive » ou « heureuse ». Il me semble que dans les expressions évoquées jusqu'ici on retrouve un élément important, à savoir la nécessité de considérer la cybersécurité comme un vecteur potentiel de développement économique, au travers la capacité à faire émerger des standards. L'exemple le plus concret est celui du règlement général de protection des données (RGPD), qui est un modèle qui s'exporte. Il est nécessaire qu'au sein de l'Union européenne puissent émerger des standards ambitieux, à la hauteur de l'état de la menace. Ces standards doivent être reconnus à l'échelle internationale et exportables.

Il est parfois difficile de faire adhérer nos concitoyens, en particulier les PME, et à leur faire prendre conscience des risques auxquels ils s'exposent, avec des outils de plus en plus interconnectés et immatériels. Il y a trente ans, nous étions majoritairement dans un système « *hardware* » et la garantie de sécurité d'un produit reposait avant tout sur la chaîne d'approvisionnement, la fabrication des composants et le jeu de puces. Aujourd'hui, nous sommes passés à un système beaucoup plus immatériel et il a été rappelé combien de millions de lignes de codes il existe dans une automobile. C'est vrai pour presque l'ensemble des systèmes. C'est ce à quoi l'Assemblée nationale a été sensibilisée dans le cadre de

l'examen du texte de loi sur la 5G dont je fus le rapporteur. La 5G constitue une avancée technologique qui repose aussi sur le fait que les infrastructures sont de plus en plus immatérielles et totalement évolutives, avec des mises à jour permanentes.

C'est dire si la capacité qu'ont les agences, et notamment la plus belle d'entre elles, l'ANSSI (pardon pour les autres !), dépend des crédits votés par le législateur. Notre responsabilité n'est donc pas seulement de commenter ou de subir l'actualité, mais aussi de prendre des initiatives et d'allouer des moyens aux agences à qui l'on confie ce genre de missions. Nous avons aussi su largement déléguer à l'ANSSI, confiants dans ses compétences, pour lui permettre de faire sur la 5G ce qu'elle a fait déjà fait sur la 3G et la 4G.

Il faut prendre conscience des difficultés posées par les menaces hybrides, que l'on va rencontrer de plus en plus. Ces menaces sont appelées « hybrides » parce qu'elles émanent d'États ou de proto-États et conjuguent les nouvelles technologies et des moyens conventionnels. En Arabie Saoudite, une simple attaque par drone sur quelques puits pétrolifères a causé de grands désordres. Une autre problématique nouvelle : la sécurisation des processus électoraux dans un contexte de *fake news*, où le vraisemblable devient le vrai et où les régimes politiques et les opinions publiques sont susceptibles d'être manipulés.

Ainsi l'ENISA a-t-elle un rôle indispensable d'animation auprès de l'ensemble des agences nationales, dans une logique à la fois offensive (se prémunir contre les risques futurs) et défensive (se prémunir contre les risques actuels). Il faut toujours penser au volet anticipation et au volet protection.

Je termine en disant qu'il est fondamental que, tout en recherchant un bon niveau de sécurité, nous traduisions nos efforts au niveau économique. La cybersécurité en tant que domaine de recherche est un relais de croissance pour toutes les entreprises européennes qui travaillent dans ce secteur, et qui sont parmi les meilleures au monde. Il faudra pouvoir construire des champions industriels de la cybersécurité européenne.

M. Jean-Louis Bourlanges. J'ai peine à intervenir dans un domaine où, comme disait Aristide Briand, « je suis d'une ignorance encyclopédique ». Je dois dire que si j'étais candidat à la Commission européenne sur ces questions, il n'y aurait aucun risque qu'on me reproche une familiarité excessive avec le secteur…

Une question donc d'une innocence absolue : celle de la subsidiarité. Sans remettre en cause l'utilité de votre travail, qu'est-ce qui, dans ce que vous faites, doit être fait spécifiquement au niveau européen ? C'est un domaine où la compétence de droit commun revient en principe aux États membres, et où l'Union européenne n'a qu'une compétence d'attribution conditionnée par le principe de subsidiarité. Quelle est la spécificité de l'intervention au niveau européen par rapport à l'intervention des États au niveau national ?

Mme Christine Hennion. Il est important de maintenir et de développer nos capacités technologiques et industrielles dans la cyber, à la fois pour nous protéger et pour construire cette économie du monde de la cyber qui nous permettra d'avoir notre indépendance numérique européenne.

Comme le souligne le rapport de notre collègue, les moyens de l'ENISA sont encore très limités, et sans doute insuffisants ; par ailleurs la directive SRI (2016) est une première étape vers le chemin qui nous permettra de disposer de l'ossature de la cybersécurité au niveau européen, mais il y a un manque de coordination entre certaines instances internationales (l'ONU, l'OTAN, Interpol…), dont les compétences et les missions ne sont pas toujours bien définies et partagées. Saluons tout de même certaines initiatives de la Commission européenne : le nouveau cadre du « paquet cyber » qui prévoit un élargissement du mandat de l'ENISA et une augmentation de ses moyens ; un cadre de certification à construire pour avoir un espace de sécurité uniforme ; le nouveau centre de compétence industrielle, technologique et de recherche en matière de cybersécurité.

Comment construire progressivement et pragmatiquement le cadre de cybersécurité par le « paquet cyber » ? Comment, en tant que parlementaires nationaux, pouvons-nous contribuer à la mise en place de ces nouvelles missions au niveau européen ?

M. André Chassaigne. Je dirai d'abord à mon collègue Bourlanges, avec qui nous avons l'habitude d'échanger, qu'il faut sortir de l'ignorance encyclopédique, ce qui suppose certes de faire des efforts intellectuels, voire une « révolution copernicienne »…

Je voudrais revenir sur le travail fait par la commission de la Défense, avec le rapport de Bastien Lachaud et d'Alexandra Valetta-Ardisson publié en juillet 2018 à la suite d'une mission d'information sur la cyberdéfense. Ce rapport insistait sur la nécessité d'accompagner les efforts d'harmonisation de la certification au niveau européen. Il s'appuyait sur le fait que le système européen de certification vise à garantir la sécurité d'utilisation des produits et des services dans l'environnement numérique en veillant à ce qu'ils respectent les exigences de cybersécurité, les certificats délivrés devant être reconnus dans tous les États membres. D'où ma première question : y a-t-il aujourd'hui des avancées concrètes à propos de la reconnaissance des certificats dans les États membres ?

Deuxième question : cette certification harmonisée, si elle prospère, doit être effectuée sur la base de critères exigeants, et non en fonction du « plus petit dénominateur commun ». Êtes-vous sensible à ce risque de « tirer vers le bas » les exigences de cybersécurité au lieu de les renforcer ?

Troisième observation : le rapport de la commission de la Défense souhaitait « mener une diplomatie normative active, afin de promouvoir les modèles et les valeurs de la France dans le domaine cyber ». Cette « diplomatie »

devrait permettre de développer l'influence normative de la France à l'international. Est-ce que cette diplomatie se limite aux pays de l'Union européenne, ou ne touche-t-elle pas plus largement à l'OTAN ? Peut-on espérer un jour – mais sans doute est-ce un rêve – qu'il puisse y avoir un corpus juridique international commun au niveau mondial, organisé autour de l'ONU ?

Mme Aude Bono-Vandorme. Le 31octobre dernier, le Centre européen de lutte contre la cybercriminalité et l'ENISA ont organisé une simulation afin de tester le protocole de réaction d'urgence de l'Union européenne face aux cyberattaques transfrontalières affectant les secteurs privé et public. Vos analyses ne sont certes pas terminées, mais quelles sont vos premières impressions sur la mutualisation des moyens et l'efficacité de la réaction conjointe des pays qui ont participé à cette simulation ?

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. Je réponds à M. Bourlanges au sujet de la subsidiarité. Quelle action spécifique y a-t-il à mener à l'échelle européenne ? Je prends l'exemple de la démarche de certification. À une échelle trop petite, il est difficile de structurer le marché autour des règles attendues quant aux équipements et aux façons de les installer, de les maintenir ou de les retirer du service lorsqu'ils sont obsolètes, etc. Ces questions sont extrêmement importantes. Dès le début, lorsqu'on achète un équipement et qu'on le met en service, il faut s'assurer qu'il a été bien conçu et que son installation est conforme aux meilleures pratiques. C'est ce qu'on appelle la *security by default*.

Or aujourd'hui, nos entreprises ont toutes des zones de chalandise qui dépassent la France. Les jeunes entreprises, en particulier, ont besoin d'une zone économique plus grande pour saisir des opportunités sur un domaine technologique très vaste. Pour aider ces entreprises, il faut leur apporter de la clarté quant aux règles que l'on souhaite édifier. C'était l'objet du texte très ambitieux sorti l'an dernier sur le schéma de certification. L'objet de ce texte n'était pas de dire comment certifier tel ou tel équipement, mais d'organiser le travail à 28 pour parvenir à mettre en place un schéma de certification. C'est ce que l'on fait à l'échelle européenne et que l'on ne peut pas faire à l'échelle nationale : convenir des règles du jeu grâce auxquelles les États membres vont se mettre d'accord, reconnaître leurs centres de certification respectifs et s'assurer que ces centres soient indépendants des entreprises dont ils doivent certifier les produits. Il ne doit en effet pas y avoir d'intéressement à certifier. S'il y a dans un pays européen un centre de certification aux prestations coûteuses et aux exigences assouplies, cela ne fonctionne pas. Il était nécessaire de créer la confiance dans notre capacité à observer nos centres respectifs, à les reconnaître, à préciser leurs compétences et à fixer des prérequis techniques.

C'est pour cette raison que ce texte était très ambitieux. Il entendait à la fois traiter les besoins du quotidien, avec des niveaux de certification peu coûteux à établir, et installer des schémas de certification de haut niveau pour protéger les produits qui peuvent être attaqués par des menaces de très haut niveau. Les règles

du jeu pour l'élaboration des schémas de certification sont en place. L'ENISA va avoir un rôle particulier pour accompagner les États membres dans leur rédaction.

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Au sujet de la subsidiarité, il faut être clair sur la répartition des responsabilités entre le niveau européen et le niveau national.

Je vais m'appuyer sur une métaphore simple. S'il y a un incendie, ce n'est pas l'ENISA qui va venir éteindre l'incendie, cela relève de la responsabilité des autorités nationales. L'ENISA est là pour s'assurer qu'il y ait des mécanismes d'alerte incendie dans les établissements, que les pompiers sont bien formés et elle aide les différentes brigades de pompiers, lorsque l'incendie est important, à échanger les informations pour qu'elles puissent mieux se préparer. Elle est également là pour les aider à tirer les enseignements de l'événement. C'est la mission de l'échelon européen.

L'échelon national est le premier à aller sur le terrain, mais nous souhaitons qu'il y ait une coordination toujours plus poussée. Je suis ravi de constater que l'ANSSI appelle de ses vœux la mise en place de mécanismes européens.

Les parlements nationaux ont un rôle à jouer pour s'assurer que la cybersécurité reste au cœur des priorités des gouvernements. Il ne s'agit en effet pas uniquement d'une question technologique, mais d'une question hautement stratégique et politique.

Deuxièmement, le cadre de certification de cybersécurité soulève la question du type de produits et de services devant relever de cette certification. Chaque État membre est représenté au sein du groupe de certification européen qui discute des catégories de produits et services qui doivent être certifiés en priorité. Il faut certes identifier les lacunes, mais c'est aussi une question de priorités politiques. Je serais intéressé de connaître celles des parlements nationaux.

L'ENISA a également un rôle à jouer pour ce qui concerne l'identité numérique. Un mécanisme de rapport des incidents a été mis en place, qui nous permet de tirer des enseignements de nos vulnérabilités afin de s'assurer que les identités numériques nationales soient préservées. Il nous faut évaluer ce cadre, l'améliorer et peut-être l'inscrire dans le cadre général de lutte contre la cybercriminalité.

Des questions très spécifiques ont été posées sur la certification. Je rappelle que l'ENISA est une agence qui relève du marché intérieur ; elle n'a pas compétence en matière de défense nationale. L'ENISA est dotée de la capacité d'aider les États membres et l'Union Européenne en matière de coopération internationale, mais elle n'est pas chef de file. C'est aux États membres de faire appel à l'ENISA. Celle-ci ne peut pas avoir une approche proactive, mais elle est toujours là pour aider à définir une approche commune et apporter son expertise.

M. Steve Purser, directeur des opérations de l'ENISA. Pour répondre correctement à la question posée sur l'exercice de simulation, il faut revenir au point de départ, en 2010, lorsque nous avons commencé les exercices.

Le premier exercice, en 2010, était relativement simple. Nous cherchions à répondre à trois questions : en cas d'urgence, savons-nous qui appeler dans un autre pays ? Si oui, connaissons-nous son niveau de responsabilité et ses possibilités de réaction ? Enfin, quels sont les protocoles utilisés pour échanger les informations ? Cet exercice a révélé que nous étions très peu préparés : les résultats ont été mauvais sur chacun des trois points.

La bonne nouvelle, c'est que, depuis 2010, plusieurs exercices ont montré que nous savions désormais très bien répondre à ces trois questions. Les *standard operating procedures* ont bien évolué, notamment grâce à l'ANSSI et aux autres agences. Les protocoles ont été testés à de multiples reprises. Ils ont notamment été utilisés à l'occasion des crises de *WannaCry* et *NotPetya*, au cours desquelles ils se sont avérés relativement efficaces. Les conséquences de ces attaques auraient été pires si nous n'avions pas utilisé ces procédures. Nous avons encore un long chemin à parcourir, mais nous sommes relativement bien positionnés.

Pour en revenir à la question de Mme Bono-Vandorme, il y a eu un exercice il y a deux ou trois semaines pour tester le protocole développé par Europol. J'ai eu des retours très positifs, mais j'insiste sur le fait qu'il ne s'agit que d'un premier pas.

En Europe, nous n'avons pas de *cyber-tsar*, de contrôle centralisé. Nous travaillons ensemble, avec une réponse multilatérale. Les États membres ont fait un excellent travail en concevant un système qui nous permet de réagir très rapidement. Il nous reste à le rendre encore plus rapide, à hiérarchiser les informations transmises et à s'assurer de l'émergence d'une véritable communauté. Il est extrêmement important que les gens se connaissent pour que les choses avancent plus rapidement.

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. Les enjeux en matière de cybersécurité sont également débattus dans plusieurs enceintes internationales, notamment au sein du groupe de travail de l'ONU sur le désarmement. En 2017, le dernier rapport de ce dernier n'avait pas été très conclusif. J'espère que le prochain le sera, en particulier sur les modalités d'application du droit international dans le cyberespace. Sur ce point, la position française est très claire : il doit s'appliquer. Parmi les autres enceintes pertinentes en matière de cybersécurité, je citerai l'OSCE ou l'OCDE, où la France est représentée par le ministère des Affaires étrangères.

M. Jean-Louis Bourlanges. Vous avez évoqué la séparation du militaire et du civil en matière de cybersécurité. N'y aurait-il pas, à l'inverse, une logique à les réunir ?

M. Cyril Cuvillier, sous-directeur adjoint de la stratégie de l'ANSSI. La notion de « Défense » doit être précisée. Pour nous, la cyberdéfense signifie se défendre contre une attaque et non pas attaquer afin de mettre hors d'état de nuire ceux qui nous attaquent. Là n'est pas le travail de l'ANSSI. J'ajoute qu'il est nécessaire pour nous de maintenir des relations de confiance avec les entreprises qui doivent être assurées que les informations qu'elles nous transmettent ne pourront pas être utilisées contre elles.

M. Éric Bothorel, rapporteur. La doctrine en France est en effet de distinguer entre la cyberdéfense et la cybersécurité. En effet, certaines technologies nécessaires pour protéger les infrastructures militaires ne sont pas utilisables dans les domaines civils, notamment parce qu'elle devrait être conciliée avec les droits fondamentaux comme la liberté d'expression. Certes, cyberdéfense et cybersécurité peuvent s'enrichir mutuellement, mais c'est la force de la France que de maintenir une distinction entre les deux.

II. PRÉSENTATION DU RAPPORT D'INFORMATION

Mme la Présidente Sabine Thillaye. Je propose à nos invités de rester parmi nous pour la présentation du rapport d'information et je les invite à réagir s'ils le souhaitent. M. le rapporteur, vous avez la parole.

M. Eric Bothorel, rapporteur. Le rapport que je vais vous présenter aujourd'hui porte sur l'avenir de la cybersécurité européenne, à l'aune des changements législatifs intervenus récemment dans l'Union. Ces changements ont fait l'objet de la table ronde qui a précédé la présentation du rapport, aussi ne reviendrai-je pas dans le détail sur le contenu de l'Acte de cybersécurité européen ou sur la directive SRI qui l'a précédé.

Ce travail m'a conduit à réaliser une large consultation d'acteurs concernés par l'introduction de l'Acte de cybersécurité européen, avec près d'une trentaine d'auditions menées, aussi bien à Paris qu'à Bruxelles, Athènes et Madrid. Ces auditions ont permis de recueillir la position des principales institutions publiques impliquées par la mise en œuvre de l'Acte de cybersécurité, ainsi que des acteurs majeurs du secteur privé.

Selon la Commission européenne, 80 % des entreprises européennes connaissent au moins un « incident de cybersécurité » par an. Dans certains États membres de l'Union, jusqu'à 50 % des crimes perpétrés interviendraient dans le champ de la cybercriminalité. Les cybermenaces peuvent prendre des formes multiples, comme en rend compte le rapport sur l'état de la menace liée au numérique en 2019 du Ministère de l'intérieur français : *typosquatting*, rançongiciels, chevaux de Troie d'administration à distance, *cryptojacking* et autres *botnets*. La liste est longue et ne cesse de s'allonger.

Autant de termes peu familiers aux oreilles des non-initiés qui composent la majorité des utilisateurs, mais qui représentent pourtant des menaces bien réelles, et aux conséquences potentiellement très graves. Force est de constater que l'écart reste encore trop grand aujourd'hui dans le public entre l'usage au quotidien des réseaux, très répandu, et la perception des dangers, qui reste encore bien trop faible. Comme si les actes délictueux commis dans le cyberespace n'avaient pas d'implications concrètes dans la « vraie vie » : or, rien n'est plus faux.

De plus, la multiplication des objets connectés et des services en ligne sera renforcée par de futurs réseaux techniquement plus performants mais aussi peut-être plus vulnérables en termes de sécurité du fait de leurs caractéristiques propres (avec leur plus grande surface d'exposition aux risques, la part croissante jouée par leur dimension logicielle les soumettant à de nombreuses mises à jour). La cybersécurité est donc non seulement un enjeu actuel et souvent sous-estimé, mais devrait également devenir un sujet majeur pour les années à venir dans une société toujours plus numérisée.

La France occupe une place tout à fait spécifique sur le terrain de la cybersécurité en Europe, car elle dispose d'une expertise ancienne et reconnue, expertise plus particulièrement incarnée par son agence nationale, l'ANSSI. Mais la force d'une chaîne se mesurant à l'aune de son maillon le plus faible, une coopération de qualité entre les autorités européennes responsables de ce sujet dans leur pays apparaît déterminante. Jusqu'à récemment, l'existence même de telles autorités n'était pas acquise dans tous les États membres de l'Union, et lorsqu'elles existaient, toutes n'avaient pas la puissance de frappe de l'agence française.

La législation européenne récente (la directive SRI et l'Acte de cybersécurité) s'est donc employée à remédier à cela, en cherchant à concilier le respect de la souveraineté des États membres sur ce sujet très régalien avec une collaboration européenne efficace sous la houlette d'une agence dédiée à la sécurité des réseaux, l'ENISA.

Selon votre rapporteur, cet enjeu majeur doit évidemment être considéré sous l'angle de la sécurité et de la défense des intérêts à la fois nationaux et européens. Mais sa dimension économique ne doit pas être négligée : la cybersécurité peut aussi être source de prospérité, et l'Union européenne a tout à gagner à présenter un front cohérent et uni pour affronter la concurrence mondiale et proposer des standards faisant référence.

C'est pourquoi notre rapport porte sur les deux volets de l'Acte de cybersécurité : sécuritaire et opérationnel avec le renforcement de l'ENISA, et plus économique avec l'introduction d'un système européen de certification pour la cybersécurité.

À partir des observations recueillies lors des auditions et de l'étude des textes adoptés dans le cadre de l'Acte de cybersécurité européen, le rapport d'information se propose donc, d'abord, de présenter l'émergence des grands enjeux de la cybersécurité en Europe ces dernières années et les tendances en termes de menaces.

L'élaboration de réponses européennes coordonnées aux problèmes de cybersécurité par les pouvoirs publics se heurte en effet à deux écueils : le foisonnement des institutions destinées à répondre aux menaces sur le plan international d'une part, et la difficulté à évaluer et caractériser les atteintes à la cybersécurité d'autre part.

La cybersécurité étant par nature un sujet ne connaissant pas de frontière, sa prise en compte par les organisations internationales se fait de façon foisonnante et peu coordonnée, conduisant à un véritable « patchwork institutionnel » de la cybersécurité. En tracer les contours permet au rapport de mettre en lumière le chemin qui reste à parcourir pour une véritable coordination internationale, à la hauteur des enjeux. Encore faut-il être en mesure d'évaluer ceux-ci : le développement au sein de l'Union européenne d'un indicateur de mesure de la cybersécurité apparaît en effet comme un prérequis indispensable à l'affirmation d'un modèle européen de cybersécurité. Cet indicateur devrait répondre à des critères de scientificité ouverts et permettre de mesurer les progrès réalisés d'une année sur l'autre, notamment grâce aux outils mis en place pour garantir la cybersécurité au niveau de l'Union. L'ENISA publie un rapport annuel d'évaluation des menaces : à l'avenir, il pourrait être intéressant que ce rapport fasse l'objet d'une plus grande publicité, par le biais d'une présentation au Parlement européen par exemple. Ce rendez-vous régulier pourrait être mis en place dès à présent avec le début du mandat des députés européens, et constituer ainsi un temps de discussion annuel qui contribuerait à la sensibilisation autour des enjeux de la cybersécurité européenne.

Le rapport cherche également à montrer comment une Agence européenne de la cybersécurité renforcée pourra contribuer à rationaliser une architecture de la cybersécurité européenne encore trop éclatée. Votre rapporteur salue le renforcement de l'ENISA mais appelle à la vigilance sur les contours du rôle que l'Agence devra endosser, afin que soient conciliées au mieux les exigences de coopération européenne et de respect de la souveraineté des États membres. L'ENISA ne doit pas devenir l'organe supranational de la cybersécurité en Europe, mais peut et doit assurer un rôle utile de coordination et de mobilisation des compétences nationales.

La diversité des instances nationales nous conduit à proposer que soit désignée dans chaque État membre une personnalité politique de référence, susceptible d'offrir une meilleure visibilité aux enjeux de cybersécurité. Il pourrait s'agir en France de créer un ministère de plein exercice, qui permettrait une véritable incarnation politique des problématiques de cybersécurité, tant sur le volet sécuritaire qu'industriel.

Le rapport examine également les modalités dans lesquelles s'inscrira la certification européenne créée par le nouveau règlement : si la certification de cybersécurité peut constituer un avantage comparatif essentiel pour l'Union, elle n'emporte pas moins certaines difficultés dont il faut être conscient. La certification introduite par le règlement sur la cybersécurité représente une véritable opportunité de croissance pour l'Europe sur le marché de la cybersécurité, à condition qu'elle favorise la convergence vers les plus hautes exigences. Pour cela, le rapport appelle à la bonne prise en compte des acquis existants et attire l'attention sur les problématiques de périmètres et de durabilité des schémas d'évaluation de certification. En effet, dans un domaine, le numérique, où les mises à jour sont nombreuses et les évolutions rapides, la certification devra tenir la gageure de réconcilier réactivité et stabilité

La mise en œuvre de l'Acte de cybersécurité offre à l'Union européenne l'occasion historique de répéter l'établissement d'un standard, tel que celui qu'elle a réussi à proposer pour la protection des données personnelles avec le RGPD. Il lui faut pour cela capitaliser sur les réussites des meilleurs acteurs en son sein, et réussir à faire converger secteurs public et privé dans la promotion de l'intérêt européen. C'est le sens du modèle que ce rapport vise à défendre.

Le rapport présenté aujourd'hui devant notre Commission cherche donc à présenter les dernières avancées dans la législation européenne sur la cybersécurité tout en soulignant les difficultés qui pourraient survenir lors de la mise en œuvre de ces textes, difficultés inhérentes au paysage institutionnel complexe, à la sensibilité de ce sujet pour la souveraineté des États et au caractère très évolutif du secteur du numérique. Il cherche ainsi à contribuer à la diffusion d'une certaine culture autour des enjeux de cybersécurité à un moment charnière pour la vie de l'Union européenne, avec l'arrivée récente des nouveaux députés au Parlement européen et la prise de fonction prochaine de la Commission européenne. Je vous remercie.

Mme la Présidente Sabine Thillaye. M. le rapporteur, vous avez évoqué la place de la France, qui semble plutôt avancée sur ces sujets. Quels sont les États membres avec un niveau d'implication moindre ? Quels sont les plus avancés ? Par ailleurs, avons-nous une idée des zones géographiques d'où proviennent les principales menaces ?

M. Éric Bothorel, rapporteur. Nous parlions tout à l'heure de diplomatie ; je vais tenter d'être diplomate dans ma réponse. Il ne vous aura pas échappé que l'harmonisation dans l'Union européenne n'est pas encore parfaite. Il ne serait pas surprenant qu'au niveau des moyens, des outils, il y ait encore une certaine hétérogénéité. Loin de moi l'idée de désigner ici des pays, mais l'idée que la force d'une chaîne repose sur son maillon le plus faible est aujourd'hui pleinement partagée.

Cela a été rappelé : au-delà des infrastructures, ce sont les pratiques et les cultures, ainsi que la prise en compte des risques cyber par les politiques, qui

contribuent à l'effort. L'objectif est de parvenir au même niveau de prise de conscience. La certification est aussi un moyen de mettre du collaboratif et de l'échange entre les pays, en bilatéral comme en multilatéral au sein de l'Union européenne. Le nivellement doit en tout cas se faire par le haut.

M. Jean-Louis Bourlanges. Puisque vous évoquez des problèmes d'harmonisation, y aurait-il une possibilité théorique d'élever juridiquement, à travers éventuellement une révision du traité, de créer une véritable compétence d'harmonisation en la matière ? On est là face à des procédures de coopération qui marchent plus ou moins bien. Une avancée institutionnelle, même si elle n'est pas réaliste aujourd'hui, serait-elle utile ?

Mme Christine Hennion. Lorsque le RGPD a été adopté, les pays ont investi dans leurs agences et ont décuplé le nombre de leurs membres. Cela a notamment été le cas en Irlande. Dans tout ce paquet cyber, y a-t-il des textes qui pourraient amener les pays européens à se sentir contraints à investir ? Ou faut-il aller plus loin dans les textes pour qu'il y ait ce réflexe ?

M. Juhan Lepassaar, directeur exécutif de l'ENISA. Comme je l'ai dit, tous les États membres ont transposé la directive SRI. Tous les États membres ont adopté une stratégie nationale sur la cybersécurité, qui contient une partie dédiée au renforcement des capacités et des ressources. De fait, ils ont renforcé les ressources allouées, sans que ce soit suffisant.

La Commission européenne est encore en cours d'évaluation des mesures mises en place. C'est une question qui restera en suspens pour la prochaine Commission, qui entreprendra une analyse de la mise en œuvre de la directive SRI.

Il existe un groupe de coopération SRI, très efficace, et nous avons vu à partir de leurs travaux sur la 5G qu'ils produisent des résultats très intéressants. Les contributions des États membres, à travers ce réseau de coopération SRI, ont été très pertinentes. Aujourd'hui, je pense que les États membres se rendent compte que la cybersécurité est vitale pour eux. Les capacités de l'ENISA, qui reste une petite agence mais dont l'effectif a été augmenté de quasiment 50 %, montrent l'engagement de l'Union européenne en la matière.

M. Cyril Cuvillier, sous-directeur de la stratégie de l'ANSSI. Dans les expériences qui ont précédé ce schéma de certification, on avait déjà des réalisations d'une dizaine d'États membres ou plus. Ils avaient pris pour habitude de reconnaître mutuellement leurs centres de certification. Nous allons poursuivre cet effort afin d'avoir de plus en plus de centres de certification à travers l'Europe. Nous devons aussi aider des centres à monter en compétence, pour qu'ils puissent évaluer des choses de plus en plus sophistiquées. Pour moi, ce sera progressif.

Dans un second temps, je voudrais préciser qu'il ne s'agit pas, pour moi, d'un domaine qui ressort uniquement de la sphère publique. Il y a bien des domaines dans lesquels les acteurs privés développent des standards et des efforts

de certification. Nous allons voir se croiser un effort horizontal de certification générique avec des verticales sectorielles, qui témoignent d'initiatives de qualité. Il y aura un défi pour articuler cette lecture des risques pour les sociétés que fait le politique ou l'acteur public, avec la lecture de qualité que l'opérateur privé cherche à atteindre. Cela peut devenir, et nous le souhaitons, un argument de vente pour les entreprises que de savoir valoriser les efforts qu'elles font pour livrer sur le marché des services et des produits de qualité.

M. Éric Bothorel, rapporteur. Tout ce qui permettra d'adopter, à l'échelle de l'Union, un référentiel pour encadrer ces éléments de certification, à l'image de ce que l'on a fait avec le RGPD, est bienvenu. Ce sont des métiers relativement récents : entre les pratiques allemandes et françaises, par exemple, qu'il s'agisse de délais ou de gratuité, il y a des divergences. L'idée est de mettre en commun les meilleures pratiques. Il faut parvenir à garantir un niveau d'exigence suffisamment élevé pour les infrastructures, afin d'être suffisamment sereins par rapport aux menaces. À terme, en effet, si l'on peut avoir une initiative législative à l'échelon pertinent qui est celui de l'Europe, ce sera positif.

À l'issue de la discussion, la commission a *autorisé* la publication du rapport.

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR

À Paris

Organismes publics :

- Agence nationale de sécurité des systèmes d'information (ANSSI) : M. Guillaume Poupard, directeur général, Mme Anouk Teiller, chef de cabinet, Mme Aude Le Tellier, chef des Affaires politiques européennes et internationales, M. Jean-Baptiste Demaison, Conseiller innovation du Sous-directeur stratégie ;

- Ministère de l'Europe et des Affaires étrangères : M. Henri Verdier, ambassadeur au numérique ;

- Ministère des Armées, Commandement de la Cyberdéfense (COMCYBER) : Général de brigade aérienne Didier Tisseyre, officier général adjoint du commandement de la cyberdéfense, Lieutenant-colonel Cédric Méreuze, Pôle développement et stratégie, Chef de la cellule relations internationales, M. Lucas Baratin, chargé de mission.

Représentants de groupes d'intérêt et entreprises :

- CyberTaskForce : M. Jacques de La Rivière, M. Sébastien Garnault, M. Jean Larroumets, M. Guillaume Vassault-Houliere ;

- European Cyber Security Organisation (ECSO) : M. Luigi Rebuffi, secrétaire général ;

- Alliance pour la Confiance Numérique (ACN) : M. Philippe Vanier, président, M. Yoann Kassianides, directeur général ;

- Orange : Mme Carole Gay, responsable des relations institutionnelles, M. Jean-Luc Moliner, directeur de la sécurité du Groupe ;

- IBM : M. Jonathan Sage, Government affairs executive IBM Europe, en charge de la cybersécurité, Mme Diane Dufoix-Garnier, directrice des affaires publiques IBM France, Mme Solène Quéré, chargée de mission Affaires publiques IBM France ;

- Thales : M. Stanislas de Maupeou, vice-président stratégie et marketing, Mme Isabelle Caputo, vice-présidente chargée des relations institutionnelles ;

- CEIS : M. Guillaume Tissier, président, M. Bruno Denoyelle, directeur affaires publiques ;

- Syntec Numérique : M. Gérôme Billois, Mme Emilie Dumérain, déléguée juridique.

À Bruxelles :

- Représentation permanente de la France auprès de l'Union européenne : M. Fabrice Dubreuil, Représentant permanent adjoint, M. Pascal Rogard, conseiller numérique, télécommunications et postes ;
- European Union Institute for Security Studies (EUISS) : Mme Nathalie Van Raemdonck, analyste ;
- Service européen pour l'action extérieure, service du secrétaire général adjoint pour la PSDC et la réaction aux crises, M. Pawel Herczynski, directeur général ;
- Agence européenne de défense : M. Olli Ruutu, directeur général adjoint ;
- Commission européenne, direction générale "Marché intérieur, industrie, entrepreneuriat et PME", M. Pierre Delsaux, directeur général adjoint ;
- Commission européenne, direction générale des réseaux de communication, du contenu et des technologies (en visio-conférence à la Représentation permanente de la Commission européenne à Paris) : M. Khalil Rouhana, directeur général adjoint.

À Athènes :

- Ambassade de France : M. Christophe Chantepy, Ambassadeur de France, M. Olivier Dovergne, chargé de l'innovation, M. Franck Billa, attaché de sécurité intérieure ;
- ENISA : M. Udo Helmbrecht, directeur exécutif, M. Steve Purser, directeur des opérations, M. Aidan Ryan, directeur juridique,
- Division du Cybercrime, police grecque, Lieutenant-colonel de police M. Efstratios Matakoulias, directeur adjoint.

À Madrid :

- Ambassade de France : M. Jean-Michel Casa, Ambassadeur, M. Gautier Lekens, ministre-conseiller, M. Xavier Toutain, attaché de défense, M. Jean-Marc Souvira, attaché de sécurité intérieure, M. Grégory Varennes, deuxième conseiller ;
- Présidence du Gouvernement espagnol : Général Miguel Ángel Ballesteros Martin, directeur du département de la sécurité nationale ;
- Centre Cryptologique National (CCN) : M. Javier Candau, chef du département cybersécurité ;
- Centre national de Protection des infrastructures et de Cybersécurité (CNPIC) ;
- Direction générale de la garde civile : Colonel Andrès Jimenez Garcia et Colonel Antonio Doblas, unité centrale opérationnelle (département de cyberdélinquance)

- Direction générale de la Police nationale : Commissaire José Garcia Serrano, Commissaire Santiago Marotto Dominguez, Commissaire Pedro Pacheco Carrasco, Unité centrale de cyberdélinquance.