N° 458

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 20 avril 2018

RAPPORT D´INFORMATION

FAIT

au nom de la commission des affaires européennes (1) sur la **cybersécurité** *dans l'***Union européenne***,*

Par M. René DANESI et Mme Laurence HARRIBEY,

Sénateurs

(1) Cette commission est composée de : M. Jean Bizet, *président* ; MM. Philippe Bonnecarrère, André Gattolin, Mmes Véronique Guillotin, Fabienne Keller, M. Didier Marie, Mme Colette Mélot, MM. Pierre Ouzoulias, Cyril Pellevat, André Reichardt, Simon Sutour, *vice-présidents* ; M. Benoît Huré, Mme Gisèle Jourda, MM. Pierre Médevielle, Jean-François Rapin, *secrétaires* ; MM. Pascal Allizard, Jacques Bigot, Yannick Botrel, Pierre Cuypers, René Danesi, Mme Nicole Duranton, MM. Thierry Foucaud, Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Daniel Gremillet, Mme Pascale Gruny, Laurence Harribey, MM. Claude Haut, Olivier Henno, Mmes Sophie Joissains, Claudine Kauffmann, MM. Guy-Dominique Kennel, Claude Kern, Jean-Yves Leconte, Jean-Pierre Leleux, Mme Anne-Catherine Loisier, MM. Franck Menonville, Georges Patient, Michel Raison, Claude Raynal, Mme Sylvie Robert.

SOMMAIRE

AVANT-PROPOS

Lors de son discours sur l'état de l'Union le 13 septembre 2017, Jean-Claude Juncker, le président de la Commission européenne, a déclaré : *« les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars »* ; *« Les cyberattaques ne connaissent pas de frontières; elles n'épargnent personne »*.

Force est de constater que l'Union européenne n'est pas épargnée par les attaques cyber. Son modèle démocratique, sa prospérité et, peut-être, un manque de culture de la sécurité informatique, en font une cible de choix pour les attaquants. Et la numérisation sans cesse grandissante des États, des sociétés et des économies va la rendre encore plus vulnérable. Des appareils de plus en plus connectés et des réseaux de communication électronique de plus en plus développés vont accroître le risque d'attaque cybernétique.

Si plusieurs États membres, à l'image de la France, se sont déjà saisis du phénomène et luttent avec efficacité, une augmentation du niveau de la cybersécurité en Europe est nécessaire. C'est pourquoi, le 19 septembre 2017, la Commission européenne a annoncé une série de mesures visant à renforcer la résilience de l'Union européenne dans le domaine de la cybersécurité.

Au cœur de ce paquet cybersécurité, la Commission propose un Acte européen pour la cybersécurité. Ce projet de règlement pérennise l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA, élargit ses missions et en fait l'acteur principal d'une nouvelle certification européenne de sécurité informatique.

Ces mesures ambitieuses étaient attendues, notamment par de nombreux acteurs de la cybersécurité en France. Pourtant, le résultat ne semble pas à la hauteur de l'attente et la réforme n'est pas sans soulever de questions.

Le présent rapport analyse l'état de la cybersécurité en France et en Europe et dessine les fondements d'une cybersécurité robuste, pilier de l'Europe numérique, qui seront reprises dans une proposition de résolution européenne.

I. LA PROLIFÉRATION DES CYBERMENACES OBLIGE L'EUROPE ET LA FRANCE À RENFORCER LEURS MOYENS DE RÉSILIENCE

A. UNE MENACE EN ÉVOLUTION RAPIDE ET EN AUGMENTATION CONSTANTE

1. Une menace protéiforme et de plus en plus structurée

La revue stratégique de cyberdéfense publiée le 12 février 2018 par le Secrétariat général de la défense et de la sécurité nationale dresse un constat sans équivoque des menaces cyber qui pèsent sur nos sociétés. Les dernières années ont été marquées par la croissance de la menace, tant dans ses formes que dans son intensité. Et si on connaît de mieux en mieux les cyberattaques, celles-ci présentent une grande variété.

Les attaques peuvent être massives ou ciblées et leurs effets peuvent être variables. Cela va de la disparition quasi-invisible de données à la paralysie totale d'une activité ou d'une entité visée. Quatre grandes catégories d'objectifs sont poursuivies par des attaques cyber :

- L'espionnage, transposition dans le monde numérique des activités anciennes de renseignement, qui touche peut-être plus les entreprises que les autorités publiques ;
- La cybercriminalité, qui a pour but principal le vol et l'extorsion d'argent, mais aussi de données ;
- La déstabilisation, par le biais de l'expression en ligne via des sites d'information ou de propagande et les réseaux sociaux ;
- Le sabotage informatique, c'est à dire une attaque dans le monde numérique qui vise principalement à paralyser ou détruire des infrastructures du monde physique.

On constate également qu'en un peu plus de 25 ans, la menace s'est structurée. On est passé de hackers, isolés ou en groupe, à la recherche d'un exploit comme le piratage d'une agence nationale de sécurité, à ce qu'on appelle les APT (pour *Advanced persistant threat* en anglais), c'est-à-dire des groupes d'attaquants informatiques disposant de compétences élevées, de ressources importantes et capables de conduire des attaques informatiques sophistiquées.

En outre, comme le relève la revue stratégique de cyberdéfense, *« l'implication des États transforme aussi en profondeur la nature de la menace cyber. […] Certains pays, cherchant à anonymiser leurs actions dans le cyberespace, délèguent à des entités privées le soin de les mener. »*

2. Des sociétés de plus en plus vulnérables

Les criminels ont toujours un temps d'avance sur les pouvoirs publics. Cette réalité est aussi valable dans le monde informatique. Les antivirus ne sont jamais qu'une réponse à une attaque déjà portée.

On constate aussi le manque de culture de la sécurité informatique. Hormis pour les spécialistes, la sécurisation des systèmes, produits en tous genres et infrastructures, n'est pas toujours une priorité. Pour certains, elle apparaît même comme une contrainte, voire une dépense inutile.

Pourtant, le développement de la société numérique devrait se faire sur le principe de *security by design*, c'est-à-dire de la sécurité dès la conception. À titre d'exemple, on parle beaucoup du développement des villes connectées, les *smart cities*, pour lesquelles on envisage qu'une meilleure connexion des utilisateurs de la ville et l'usage d'objets connectés permettront de mieux réguler les transports et la consommation d'énergie dans les villes. Il serait souhaitable de parler de *smart and safe cities*, des villes intelligentes et sûres. Car si les systèmes ne sont pas assez sécurisés et peuvent être détournés, les conséquences seront terribles. D'une manière générale, la transformation numérique en cours ne va faire qu'accentuer les risques informatiques qui pèsent sur nos sociétés.

L'informatique est déjà présent partout. Les objets connectés vont connaître un essor formidable dans les années qui viennent et se retrouveront dans les administrations, les entreprises, les logements individuels, les villes connectées. L'intelligence artificielle devrait permettre de gérer les grands réseaux de transport et d'énergie, en analysant des masses de données transmises en direct par le réseau internet.

Au total, il y aura une interaction permanente, via une connexion internet, entre les objets, les systèmes informatiques et l'ensemble de la société. De par la connexion, tous ces points nouveaux et connectés seront autant de point d'entrée pour une attaque. En outre, les réseaux seront de plus en plus connectés entre eux, ce qui va favoriser la propagation d'une attaque ou d'un virus à une grande échelle.

Il apparaît donc, au final, que la numérisation de la société tout entière va accroître sa vulnérabilité à la menace, au point de créer un risque systémique pour les États, les sociétés et les économies. L'Europe et la France n'échappent pas à cette analyse.

3. L'Europe et la France, cibles réelles

Les deux dernières années ont apporté la preuve de l'essor des **cyberattaques**. La Commission européenne a dressé le constat[1] qu'en 2016, il y a eu 4 000 attaques par *rançongiciel* par jour, soit une hausse de 300 % par rapport à 2015. Au total, 80 % des entreprises européennes auraient été touchées par une cyberattaque en 2016. En 2017, les virus *Wannacry* et *Notpetya* ont frappé les ordinateurs dans le monde entier avec une ampleur jamais vue auparavant. Le premier a consisté à bloquer, par chiffrement, plus de 400 000 ordinateurs dans 150 pays dans le but de demander une rançon pour la restauration des données. Le second a détruit de nombreux systèmes informatiques utilisant un logiciel comptable ukrainien, Me.Doc. L'attaque a principalement frappé l'Ukraine, dont 80 % des entreprises utilisaient ce logiciel. Au-delà, elle a touché des groupes mondiaux comme le français Saint-Gobain, l'américain FedEx ou le danois Maersk et les pertes financières totales sont estimées à plus d'un milliard d'euros. Plus grave, peut-être, des hôpitaux au Royaume-Uni ont vu leur fonctionnement affecté par l'attaque.

S'agissant des objets connectés, plusieurs exemples récents attestent de leur vulnérabilité aux attaques. La campagne « *Toyfail* » menée par l'association norvégienne de protection des consommateurs a montré que n'importe qui pouvait facilement avoir accès au microphone de la poupée connectée *Cayla* et ainsi parler avec l'enfant sans que ses parents le sachent. La campagne « *WatchOut* » menée par cette même association a également montré les nombreux défauts de sécurité affectant les montres connectées.

Pour sa part, la France est, elle aussi, touchée par le phénomène. 5 500 plaintes liées à des attaques informatiques sont déposées chaque mois et il y aurait jusqu'à 5 700 victimes sur la même période. Certes, le niveau des attaques n'est pas toujours élevé, mais ces chiffres indiquent des pratiques très répandues.

On estime que, chaque jour, c'est une collectivité territoriale qui est victime d'une attaque cyber. Ici encore, le niveau des attaques, souvent faible comme le détournement de site, doit faire relativiser l'ampleur du mouvement. Il n'en demeure pas moins que les collectivités doivent elles aussi se protéger. Outre la mise en œuvre du règlement général sur la protection des données à caractère personnel qui va les obliger à prendre un certain nombre de dispositions, assurer la sécurité de leurs installations informatiques est une charge croissante pour elles. En raison des données qu'elles gèrent, il s'agit également d'une activité sensible. C'est pourquoi, elles doivent bénéficier d'un soutien de l'État et de solutions adaptées.

---

[1] *Commission européenne, étude d'impact accompagnant la proposition de règlement sur la cybersécurité. REF*

Aperçu et comparaison du panorama actuel des menaces 2017 incluant celles de 2016.

Menaces majeures 2016	Évolution des tendances en 2016	Menaces majeures en 2017	Évolution des tendances en 2017	Changement dans le classement
1. **Programme malveillant**	⬆	**1.Programme malveillant**	➡	→
2. Attaques en provenance du web	⬆	**2. Attaques en provenance du web**	⬆	→
3. Attaques contre des applications	⬆	**3. Attaques contre des applications**	⬆	→
4. Déni de service	⬆	**4. Attaques d'hameçonnage**	⬆	↑
5. Réseaux zombies	⬆	**5. Spam**	⬆	↑
6. Attaques d'Hameçonnage	➡	**6. Déni de service**	⬆	↓
7. Spam	⬇	**7. Rançongiciel**	⬆	↑
8. Rançongiciel	➡	**8. Réseaux zombies**	⬆	↓
9. Menaces internes	➡	**9. Menaces internes**	➡	→
10. Manipulation physique/dommage /vol/ perte	⬆	**10. Manipulation physique/dommage/vol /perte**	➡	→
11. Kits d'exploits	⬆	**11. Violation de données**	⬆	↑
12. Violation de données	⬆	**12. Usurpation d'identité**	⬆	↑
13. Usurpation d'identité	⬇	**13. Fuite d'informations**	⬆	↑
14. Fuite d'informations	⬆	**14. kits d'exploits**	⬇	↓
15. Cyber espionnage	⬇	**15. cyber espionnage**	⬆	→

Légende : Tendances : ⬇ en déclin, ➡ stable, ⬆ en augmentation
Classement : ↑ monte, → ne change pas, ↓ baisse

Source : ENISA, panorama des menaces de 2017

B. LA CYBERSÉCURITÉ EN FRANCE

Face à la montée des cybermenaces et les risques qui pèsent sur sa souveraineté, la France a renforcé ses moyens d'action et développé un modèle original pour assurer la sécurité de ses systèmes d'information. Elle peut en outre s'appuyer sur une stratégie renouvelée et sur un secteur privé de pointe.

1. Le dispositif français

La France a mis en place un système de protection des systèmes d'information qui s'appuie sur une agence spécifique, l'Agence nationale de sécurité des systèmes d'information, l'ANSSI. Celle-ci a été créée par le décret n° 2009-834 du 7 juillet 2009 qui lui a donné une compétence nationale et transversale. Le modèle français se distingue du modèle anglo-saxon dans le sens où l'ANSSI n'assure que la défense et la protection de systèmes d'information, mais n'est chargée ni de l'attaque, ni du renseignement, comme la NSA (*National Security Agency*) américaine. Elle ne peut donc être suspectée d'intelligence ou de surveillance.

L'ANSSI met son expertise au service des administrations et des opérateurs d'importance vitale. Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux, notamment par le pilotage du système français de certification de cybersécurité. Elle contribue également à l'orientation de la recherche nationale et européenne en matière de sécurité des systèmes d'information. Elle est placée sous l'autorité du Secrétariat général de la défense et de la sécurité nationale, lui-même directement rattaché aux services du Premier ministre. Elle dispose de près de 800 collaborateurs.

L'ANSSI est donc au centre de l'écosystème national de cybersécurité. Elle dispose d'une vision et d'une approche transversales, et fonde son action sur la confiance qu'elle inspire aux administrations et aux différents acteurs économiques.

En outre, la numérisation croissante a obligé l'État à renforcer ses capacités pour assurer la protection du pays contre les attaques cyber. C'est particulièrement le cas en ce qui concerne le ministère des Armées, le ministère de l'Intérieur et le ministère de l'Europe et des Affaires étrangères qui ont vu leur structure évoluer en 2017.

Au ministère des Armées, un commandement de cyberdéfense (ComCyber) a été créé depuis le 1er janvier 2017. Il rassemble l'ensemble des forces de cyberdéfense des armées françaises sous une même autorité opérationnelle, permanente et interarmées. Il est chargé de trois missions principales : le cyber-renseignement, la cyber-protection, et les opérations cyber offensives. Concrètement, il s'agit d'assurer une politique cohérente du

ministère en matière d'hygiène informatique, de s'assurer que des équipes sont capables à tout moment de détecter des attaques contre les réseaux opérationnels et que la France est en capacité de neutraliser une attaque, ou de lutter contre des offensives qui menacent les intérêts français à l'extérieur.

Pour sa part, le ministère de l'Intérieur a institué par un décret du 23 janvier 2017, un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.Il élabore notamment une stratégie ministérielle de lutte contre les cybermenaces, coordonne sa mise en œuvre et pilote son évaluation et son actualisation. Il complète l'action de la sous-direction de la lutte contre la cybercriminalité, créée le 29 avril 2014. La police et la gendarmerie disposent également d'unités dédiées. À titre d'exemple, le réseau Cybergend de la Gendarmerie nationale dispose ainsi d'effectifs aux niveaux national, régional et local qu'elle prévoit de doubler d'ici à 2022.

Enfin, il convient de mentionner la création d'un poste d'ambassadeur pour le numérique le 22 novembre 2017. Il a pour mission le suivi des négociations internationales sur la cybersécurité, la gouvernance de l'internet et des réseaux, la liberté d'expression sur internet, les sujets de propriété intellectuelle liés à l'internet, le soutien à l'export des entreprises du numérique et la participation de la France au partenariat pour un gouvernement ouvert. Il est par ailleurs chargé, au titre de la lutte contre l'utilisation d'internet à des fins terroristes, de conduire un dialogue direct avec les grandes plateformes numériques américaines.

2. Une stratégie nationale globale pour la cybersécurité

Au cours des dernières années, la France a également fait évoluer sa stratégie en matière de cybersécurité. À la Stratégie nationale pour la sécurité du numérique du 16 octobre 2015, s'est ajoutée la stratégie internationale de la France pour le numérique et la revue stratégique de cyberdéfense.

La Stratégie nationale pour la sécurité du numérique fixait cinq objectifs : garantir la souveraineté nationale ; apporter une réponse forte contre les actes de cybermalveillance ; informer le grand public ; faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises ; renforcer la voix de la France à l'international. On mentionnera d'ailleurs que, pour la mise en œuvre de cette stratégie globale, le ministère de l'Intérieur a adopté en mars 2017 une stratégie de lutte contre les cybermenaces.

En décembre 2017, le ministère de l'Europe et des Affaires étrangères a publié une stratégie internationale de la France pour le numérique. Elle fixe notamment des objectifs en matière de cybersécurité pour garantir la sécurité et l'autonomie de la France dans le monde numérique : contribuer au développement d'une pensée stratégique française sur les questions de cybersécurité ; accroître avec nos partenaires la résilience de notre environnement numérique ; défendre la France et ses

alliés dans le cyberespace ; développer une cybersécurité collective à l'échelle internationale. Elle prévoit en outre deux objectifs de portée européenne : renforcer les capacités des Européens en matière de cybersécurité ; renforcer l'industrie et les services européens dans le secteur de la cybersécurité.

Le 12 février 2018, le Secrétariat général pour la défense et la sécurité nationale a publié la Revue stratégique de cyberdéfense pour permettre de développer et de structurer le dispositif national français de cyberdéfense. Portant l'affirmation d'une nouvelle ambition pour la France dans la cyberdéfense, le document évalue les menaces du monde cyber et fait de l'État le responsable de la cyberdéfense de la nation et le garant de la cybersécurité de la société française.

3. Un secteur privé en pointe

Outre l'action de l'État, il convient de souligner l'importance des acteurs privés dans le dispositif de sécurité informatique français. Si, il y a plusieurs décennies, l'innovation provenait du secteur de la défense, c'est souvent au sein des entreprises que se font aujourd'hui la recherche et le développement et c'est en leur sein que se développe l'expertise. La France dispose à la fois de grands groupes, acteurs européens et mondiaux, et d'un réseau d'entreprises plus petites, mais souvent innovantes.

Trois grandes entreprises font partie des leaders européens, voire mondiaux :

- Thalès : le spécialiste de la protection des données et du chiffrement, qui investit plus de 20 % de son chiffre d'affaire dans la recherche et le développement ; outre la sécurité et la défense, Thalès est présent dans les secteurs de l'aéronautique, de l'espace et du transport terrestre ;
- Orange : l'opérateur des télécommunications a développé depuis 2016, une branche consacrée à des activités de cybersécurité dédiées aux entreprises et est positionné parmi les premiers acteurs en Europe pour accompagner les entreprises et les administrations dans leurs stratégies de cybersécurité ;
- Atos : une des dix plus grandes entreprises du numérique à l'échelle mondiale, le groupe, figure parmi les leaders européens de l'informatique en nuage, de la cybersécurité et du super-calcul, ainsi que du paiement sécurisé en ligne pour les entreprises.

Parallèlement, des acteurs français spécialisés dans le numérique se sont réunis au sein d'associations, parmi lesquelles :

- L'Alliance pour la confiance numérique, qui a pour vocation de fédérer les principaux acteurs français et européens de la confiance numérique et de contribuer à la consolidation de la filière sécurité, que ce soit des entreprises de toute taille ou des centres de recherche ;
- Hexatrust qui rassemble des PME, des entreprises de taille intermédiaire et des start-ups travaillant dans la cybersécurité et l'informatique en nuage et très implantées en Europe.

C. L'ÉVOLUTION NÉCESSAIRE DE L'ACTION EUROPÉENNE : LE PAQUET CYBERSÉCURITÉ

1. Le constat d'une évolution nécessaire de l'action européenne

De façon assez précoce, l'Union européenne avait créé, dès 2004n une Agence chargée de la sécurité des réseaux et de l'information, l'ENISA dans son acronyme anglais. Elle lui avait fixé cinq missions : conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle ; recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents ; promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité à faire face aux menaces pesant sur la sécurité de l'information ; favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées ; suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

Élément novateur à sa création, l'ENISA n'a pas évolué depuis. Elle est restée une agence aux moyens réduits, dotée de seulement 80 salariés, et au mandat limité dans le temps, qui doit s'achever en juin 2020. Par conséquent, elle s'appuie beaucoup sur les experts de certains États membres. Elle aide les États par des formations, des recommandations ou des campagnes de sensibilisation comme le mois de la cybersécurité en Europe, elle coordonne et promeut la communauté de la sécurité des réseaux et de l'information. Sa localisation en Crète, éloignée des centres de décision, n'a pas facilité son travail. L'approche de la fin du mandat de l'ENISA a amené la Commission européenne à réfléchir au rôle futur qu'elle souhaitait lui donner.

En 2016, l'Union européenne avait pourtant fait évoluer son action en matière de cybersécurité et le rôle de l'ENISA avec l'adoption de la directive sur la sécurité des réseaux d'information, la directive SRI (ou NIS

en anglais), qui a été transposée en droit français au début de 2018. Cette directive prévoit notamment que :

- chaque État membre doit se doter d'une agence spécialisée dans la cybersécurité, à l'image de l'Agence nationale pour la sécurité des systèmes d'information en France, l'ANSSI ;
- le renforcement par chaque État de la cybersécurité d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société – les administrations, mais aussi les grandes entreprises et celles travaillant dans des secteurs sensibles. Et ces opérateurs auront l'obligation de signaler les attaques dont ils sont victimes ;
- la participation volontaire à une coopération entre États membres ;
- l'adoption de règles européennes communes en matière de cybersécurité pour certains prestataires de services numériques dans des domaines comme l'informatique en nuage pour le stockage des données, les moteurs de recherche et les places de marché en ligne.

Dans le même temps, la Commission a fait le constat d'un paysage morcelé en Europe en matière de certification de sécurité informatique. En l'absence de normes européennes, la certification s'effectue au niveau national, sur la base de normes internationales. Seuls 13 États membres ont signé un accord pour appliquer une norme internationale fondée sur des critères communs d'évaluation de la sécurité des technologies de l'information.

C'est pourquoi, de manière plus large, deux ans après son lancement en mai 2015, la Commission européenne a procédé à une révision à mi-parcours de sa stratégie pour un marché unique numérique le 10 mai 2017, dans laquelle elle estime qu'il faut renforcer la cybersécurité commune. Cette évolution a fait suite à une communication de 2016 dans laquelle la Commission annonçait déjà de nouvelles mesures pour intensifier la coopération, l'échange d'informations, et le partage de connaissance pour améliorer la résilience de l'Union en termes de cybersécurité. La Commission a annoncé que l'actualisation de la cybersécurité en Europe devait passer par trois orientations : le réexamen de la stratégie de 2013 sur la cybersécurité ; la révision du mandat l'ENISA ; la définition de mesures concernant les normes, la certification et l'étiquetage en matière de cybersécurité pour une meilleure sécurisation des systèmes.

2. La proposition de la Commission européenne : le paquet cybersécurité de septembre 2017

Signe de l'importance que la Commission européenne accorde au sujet, la cybersécurité a été évoquée par Jean-Claude Juncker dans son discours sur l'état de l'Union le 13 septembre 2017, évoqué en avant-propos. Dans la foulée, la Commission a annoncé une série de mesures surnommée « paquet cybersécurité ». Il comprend :

- Une communication chapeau intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide ;
- une proposition de règlement sur l'ENISA, aussi appelé acte pour la cybersécurité ;
- une communication et une recommandation proposant un cadre européen de réponses aux crises cyber ;
- une communication précisant certaines modalités de mise en œuvre de la directive NIS sur la sécurité des réseaux et systèmes d'information.

La Commission européenne rappelle en introduction de sa communication que « *la cybersécurité est essentielle tant pour notre prospérité que pour notre sécurité* ». Elle fait le constat que les risques se multiplient de façon exponentielle et que cette tendance s'accentue. Cela concerne la cybercriminalité, dont l'incidence sur l'économie a quintuplé entre 2013 et 2017 et pourrait encore quadrupler d'ici à 2019. Cela relève aussi de cybermenaces qui sont le fait d'acteurs étatiques qui utilisent les outils informatiques pour mener des campagnes de désinformation, propager des fausses nouvelles et interférer dans des processus démocratiques ou encore monter des cyberopérations visant des infrastructures critiques.

Comme il a été montré en première partie, au fur et à mesure que le numérique se développe et occupe une place grandissante dans nos sociétés et notre économie, le risque augmente. Il va encore augmenter avec l'internet des objets, par lequel des dizaines de milliards de dispositifs seront connectés à internet d'ici à 2020. Car ces dispositifs contrôleront les réseaux électriques, les réseaux de transport, les voitures, les usines, la finance, les hôpitaux et aussi les maisons des particuliers. Or, actuellement, la cybersécurité n'est pas une priorité dans leur conception.

Pour permettre à l'Union européenne de faire face à ces risques, la Commission propose trois axes d'action qui constituent les trois chapitres de sa communication : développer la résilience de l'UE face aux cyberattaques ; créer une cyberdissuasion européenne efficace ; renforcer la coopération internationale en matière de cybersécurité.

Les textes concernant la réponse aux crises cyber et la mise en œuvre de la directive NIS constituent surtout des lignes directrices pour une action efficace. Ils ne posent pas de difficulté.

L'Acte pour la cybersécurité est une proposition de règlement importante qui poursuit deux objectifs : un mandat pérenne et renforcé pour l'ENISA ; la création d'un cadre européen pour la certification de cybersécurité.

Lors de l'adoption de sa résolution portant avis motivé au titre du contrôle de subsidiarité[1], le Sénat s'était étonné de voir dans un même texte deux sujets aussi différents. Dans le premier cas, il s'agit de définir le rôle et le fonctionnement d'une agence européenne. Dans le second, on définit les règles qui vont s'appliquer à un processus de certification pour des produits qui seront mis sur le marché. Seul le fait que l'ENISA serait placée au centre du processus justifie que les deux aspects se trouvent dans un seul texte. Mais ce point est lui-même sujet à interrogations.

Depuis lors, le Conseil a adopté des conclusions quant au mandat qu'il entend confier à l'ENISA et le Parlement européen doit adopter sa position au cours des mois qui viennent sur la base du projet de rapport que la députée allemande Angelika Niebler a présenté le 27 mars 2018. Des discussions techniques au Conseil ont lieu chaque semaine sur la proposition de règlement dans le but qu'une orientation générale soit adoptée en juin prochain.

[1] *Résolution n° 25 (2017-2018), devenue résolution du Sénat le 6 décembre 2017 (http://www.senat.fr/dossier-legislatif/ppr17-079.html)*

II. LES CONDITIONS D'UNE CYBERSECURITÉ EUROPÉENNE ROBUSTE

L'évolution rapide des menaces cyber ainsi que l'essor des objets connectés et de l'informatique en nuage impliquent de voir l'Union européenne muscler son dispositif en matière de cybersécurité. Il s'agit, pour les Européens de mettre en place les bases d'une sécurité informatique durable qui assure la défense des démocraties, la protection des citoyens, la stabilité et le développement du marché unique numérique. La cybersécurité doit être un des piliers sur lesquels repose l'Europe numérique. Et ce pilier doit être robuste.

La proposition de règlement ENISA, surnommé Acte pour la cybersécurité, fait de cette agence le point focal de la cybersécurité en Europe. La proposition fixe cinq objectifs : développer les moyens et la préparation des États membres ; améliorer la coopération et la coordination entre les États membres et les institutions européennes ; accroitre les moyens au niveau de l'Union pour compléter les actions des États membres en cas de crise transfrontalière ; davantage sensibiliser particuliers et entreprises aux questions de cybersécurité ; accroître globalement la transparence et l'assurance de la cybersécurité ; éviter la multiplication des systèmes de certification dans l'Union, ainsi que des exigences de sécurité et des critères d'évaluation dans les différents États membres.

La question se pose de savoir ce que doit devenir l'ENISA. Agence européenne à part entière, doit-elle avoir des capacités opérationnelles propres ou venir en appui de l'action des États membres ? Est-il judicieux de lui demander d'assumer la certification européenne nouvelle, alors qu'elle n'a jusqu'à aujourd'hui aucune compétence en la matière ? Sur la base de la proposition de règlement, un juste équilibre est à trouver pour que chaque acteur puisse agir avec efficacité dans un système européen plus résilient.

A. RENFORCER L'ENISA, POUR UNE ACTION EN APPUI DE CELLE DES ETATS MEMBRES

1. Pérenniser l'ENISA et renforcer ses moyens

Comme il a été dit, le mandat de l'ENISA arrive à son terme en 2020. La numérisation des sociétés européennes, transfrontière et générale, implique que l'ENISA voit sa place confortée dans le paysage européen de la cybersécurité. Il s'agit de renforcer la sécurité informatique collective des Européens.

Il est donc tout à fait souhaitable que l'ENISA devienne une agence permanente de l'Union européenne, à l'image de celles qui existent dans d'autres secteurs. Outre un mandat permanent, la proposition prévoit que

ses objectifs et missions seraient régulièrement mis à jour. En outre, ses moyens humains, financiers et matériels seraient augmentés.

Ce dernier aspect mérite une attention particulière. L'ENISA était jusqu'à présent une agence aux moyens limités, dotée d'un effectif réduit d'environ 80 personnes, contre 570 pour l'ANSSI en 2017. C'est pourquoi elle a régulièrement recours à des experts nationaux. L'évolution proposée n'affiche pas une grande ambition puisque de 80, on passerait à 100 - 120 personnes environ. Au regard de l'élargissement envisagé pour ses missions, le renforcement de la structure de l'agence serait donc très limité.

Or, l'entrée en vigueur de la directive NIS va déjà obliger l'ENISA à remplir de nouvelles missions, notamment pour assurer des échanges entre les agences nationales, dont beaucoup sont en cours de création. C'est pourquoi, il conviendrait de ne pas trop augmenter les missions de l'ENISA et de les concentrer sur une véritable plus-value européenne. Or, dans sa proposition, la Commission européenne fait montre d'une trop grande ambition quant aux missions de l'ENISA.

En effet, dans sa proposition initiale, la Commission européenne envisageait que l'ENISA conserve ses missions concernant, d'une part, l'élaboration et la mise en œuvre de la politique de l'Union européenne en matière de cybersécurité, et, d'autre part, le soutien au renforcement des capacités (moyens et compétences) des États membres, à la coopération opérationnelle et à la gestion des crises. Mais elle prévoyait aussi que l'ENISA pourrait mener des enquêtes techniques au sein des États membres, suite à la signalisation d'un incident de cybersécurité d'ampleur européenne, sur demande de certains États membres ou de la Commission. Elle pourrait également apporter une assistance technique à certains États membres en cas de cyberattaque, grâce à une équipe d'intervention, qui serait créée.

Pour vos rapporteurs, une telle multiplication des missions de l'ENISA n'est pas justifiée, ni même souhaitable. Elle semble disproportionnée par rapport aux moyens dont elle dispose. La mise en œuvre de la directive NIS – que la France vient tout juste de transposer – devrait modifier le paysage européen de la cybersécurité avec l'émergence d'une agence nationale dans chaque État membre. Les besoins d'une mise en relation pour un partage de bonnes pratiques, d'une coopération efficace et d'une meilleure coordination dans la réponse aux crises, ainsi que le travail à venir sur la certification constituent déjà des objectifs ambitieux.

Et si vos rapporteurs partagent l'ambition plus générale d'un renforcement de la cybersécurité européenne, il convient de demeurer réaliste et de réussir chaque étape. Les États membres sont en train de mettre en œuvre la directive NIS et, pour ceux qui n'en disposaient pas encore, de se doter d'une agence nationale pour la cybersécurité. Doter l'ENISA de compétences concurrentes pourrait saper ces efforts et encourager certains à les reporter sur l'Union européenne. En l'état, cela n'est pas souhaitable, car

le niveau global de sécurité doit monter partout dans l'Union et cela passe par une action des États membres.

Il se peut que dans un futur proche, le dispositif européen de cybersécurité soit plus intégré. Toutefois, il faut ne pas vouloir aller trop vite et sauter une étape. Il importe aujourd'hui de centrer les missions de l'ENISA sur les aspects où la plus-value européenne est réelle afin de favoriser l'élévation générale du niveau de sécurité informatique.

2. Mieux articuler l'action de l'ENISA avec celle des États membres à l'avenir

La cybersécurité, parce qu'elle touche à la défense des intérêts nationaux, relève en grande partie de la souveraineté des États. Toute avancée vers une plus grande intégration européenne doit être mesurée à cette aune.

C'est la logique qui a présidé à l'adoption de la directive NIS, qui, pour améliorer la sécurité informatique en Europe, a prévu la création dans chaque État membre d'une agence dédiée et une coopération volontaire de ces agences. Ce mouvement est nécessaire et vertueux car il va permettre d'élever le niveau général de sécurité sur l'ensemble du territoire européen.

Or, comme on l'a dit ce mouvement est en cours. Et comme l'a relevé par le Sénat lors du contrôle de subsidiarité, la proposition de règlement comporte des éléments qui pourraient s'avérer contreproductifs. La Commission propose en effet de confier à l'ENISA le pouvoir de mener des enquêtes techniques au sein des États membres, suite à la signalisation d'un incident de cybersécurité d'ampleur européenne, sur demande de certains États membres ou de la Commission. Elle pourrait également apporter une assistance technique à certains États membres en cas de cyberattaque, grâce à une équipe d'intervention, qui serait créée.

Cette mesure laisse penser que l'ENISA pourrait, dans une certaine mesure, se substituer à une agence nationale faiblement dotée pour assurer une réponse en cas de cyberattaque. Pour vos rapporteurs, cela n'est ni possible, ni souhaitable. Ce n'est pas possible, car on voit mal comment l'ENISA pourrait intervenir rapidement dans n'importe quel pays d'Europe avec les moyens qui sont les siens. Ce n'est pas souhaitable, car cela pourrait saper les efforts entrepris par les États membres pour renforcer leurs moyens de protection et réduire la portée du processus en cours.

En outre, la coopération dans la sécurité informatique se fonde sur la confiance. C'est parce que les acteurs privés français ont confiance en l'ANSSI, qu'ils vont lui confier qu'ils ont, le cas échéant, été victimes d'une attaque. La confiance se gagne avec le temps. L'écosystème créé en France, mais aussi dans les pays les plus en pointe comme l'Allemagne et l'Estonie

pourrait pâtir d'un transfert de compétences vers une agence européenne qui doit encore démontrer sa valeur.

Aussi, il n'est guère certain qu'une entreprise ou une administration, victime d'une cyberattaque, informe directement une agence européenne et voit ainsi l'information se diffuser à travers tout le continent. Dans le paysage actuel, il convient donc que les agences nationales et l'ENISA travaillent ensemble à une meilleure coopération et à une meilleure coordination.

B. METTRE EN PLACE UN PROCESSUS DE CERTIFICATION DE CYBERSÉCURITÉ EXIGEANT ET SOUPLE

La certification est un processus complexe qui fait intervenir de nombreux acteurs. Le système repose sur un niveau de sécurité élevé et un processus qui garantit qu'il est respecté, comprenant trois acteurs principaux, le fournisseur de produits ou de services, le laboratoire chargé d'étudier ces derniers et l'autorité qui certifie : une autorité publique accrédite un organisme d'évaluation de la conformité– un laboratoire – pour qu'il détermine si une solution proposée par une entreprise (un service ou un produit) respecte des normes ou un cahier des charges prédéfinis, dans la plupart des cas. C'est l'intervention de l'organisme certificateur, indépendant et compétent, qui va donner sa valeur à la certification dite tierce partie. Dans certains cas, l'autorité publique peut effectuer elle-même la certification demandée.

La certification s'appuie sur des normes définies au niveau national ou international et, pour chaque type de solution, un système ou schéma s'applique. Ces derniers peuvent être proposés par les différents intervenants du secteur, publics ou privés, en fonction des besoins du marché et des évolutions technologiques. Plusieurs niveaux de certification peuvent être appliqués selon l'exigence demandée par le professionnel. Enfin, il convient de mentionner l'aspect volontaire de la démarche du professionnel qui va faire certifier son produit ou son service.

Dans le secteur de la cybersécurité, la certification a beaucoup progressé durant les dix dernières années. Pour l'ANSSI, « *la certification est l'attestation de la robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques* ». Les certificats émis par l'ANSSI attestent que les produits certifiés sont conformes à une spécification technique appelée cible de sécurité, qui peut elle-même être certifiée conforme à un cahier des charges appelé profil de protection.

En outre, 14 pays européens (13 États membres, dont la France et la Noprvège) ont mis en place un processus de certification de cybersécurité des produits et des services du numérique, sur la base de normes

internationales communément admises et mutuellement reconnues, appelé SOG-IS. La reconnaissance mutuelle des certificats par plusieurs États permet de vendre ces produits dans tous les pays signataires. Deux domaines techniques sont couverts par cet accord pour les hauts niveaux de reconnaissance, celui des « microcontrôleurs sécurisés et produits similaires » et celui des « équipements matériels avec boîtiers sécurisés ». Une véritable expertise européenne de la certification de cybersécurité, qui est un atout dans la compétition économique mondiale, s'est ainsi développée depuis une vingtaine d'années. Et, au sein de l'Union, la France figure parmi les tous meilleurs avec l'Allemagne, notamment.

1. Pour un processus de certification européen exigeant

La proposition de la Commission européenne de mettre en place une certification européenne de cybersécurité est bienvenue, car un tel système n'existe pas. Il est en effet nécessaire de disposer d'un cadre européen unique de certification de sécurité pour les produits et services des technologies de l'information et de la communication, ainsi que pour les systèmes de cybersécurité. Un tel cadre, fondé sur une démarche volontaire, permettrait d'améliorer significativement le niveau de de sécurité informatique en Europe, tout en présentant une certaine flexibilité pour s'adapter aux exigences du marché. Il serait en outre plus favorable aux entreprises qui n'auraient qu'un seul certificat à demander, au lieu de 28. Le coût et le délai d'obtention en seraient d'autant réduits. L'annexe présente l'organisation proposée par la Commission européenne.

Si la mesure était attendue et demandée par de nombreux acteurs français, vos rapporteurs ont mesuré, lors de leurs auditions, une certaine déception quant au contenu de la proposition et une inquiétude réelle et générale quant au niveau de sécurité qui pourrait en résulter.

À la lecture de la proposition, on comprend que la Commission créerait un cadre entièrement nouveau, qui ne tiendrait pas compte de l'expérience acquise en la matière par certains États membres comme la France, l'Allemagne, les Pays-Bas et le Royaume-Uni. De même, plutôt que de s'appuyer sur l'expertise développée par les États membres, le processus serait confié à l'ENISA, pour qui l'activité serait nouvelle. Enfin, les États ne joueraient qu'un rôle de conseiller dans le processus et on peine à voir quel serait le rôle de l'industrie, pourtant moteur en la matière. Enfin, le cadre semble manquer de souplesse, posant un haut niveau d'exigences pour toutes les solutions sans lien avec les contraintes et les besoins du marché.

L'ensemble combiné de ces mesures porte en lui les racines d'un affaiblissement du niveau de cybersécurité acquis par les pays les plus avancés, sous l'effet d'une dilution des normes actuellement appliquées et du risque d'une sorte de dumping, des certificats pouvant être délivrés au sein même de l'Union par des pays moins regardants.

Pour vos rapporteurs, ce n'est pas acceptable. La mise en place d'une certification unique de cybersécurité dans l'Union européenne ne doit pas conduire à son affaiblissement. L'objectif est certes de simplifier les démarches des entreprises, il est aussi d'élever le niveau général de sécurité. Pour cette raison, il convient que le futur règlement comporte certains aménagements.

En premier lieu, le règlement devrait être clarifié en ce qui concerne les compétences régaliennes des États et prévoir que la Commission ne pourra adopter des schémas de certification dans les domaines de la sécurité nationale, de la défense et en ce qui concerne certains secteurs d'importance vitale pour les États membres.

En ce qui concerne l'évaluation, le système mis en place en France et en Allemagne s'appuie sur l'indépendance entre celui qui évalue et celui qui certifie. Cette distinction doit être préservée au niveau européen.

Enfin, et surtout, la certification européenne doit partir de ce qui se fait de mieux en Europe pour l'étendre aux pays qui ne sont pas encore au même niveau. Cela implique que la norme internationale SOGIS, déjà appliquée par plusieurs États membres et fondée sur des critères communs d'évaluation de la sécurité des technologies de l'information, constitue la base d'un futur certificat européen. En outre, l'Union doit s'appuyer sur l'expertise acquise par les États membres et non transférer l'ensemble des compétences au niveau européen. Enfin, pour être efficace, l'harmonisation sur la certification doit aussi porter sur les méthodes de certification.

2. Pour un cadre de certification plus souple associant tous les acteurs

Le cadre de certification proposé par la Commission s'appuierait sur trois niveaux d'assurance :

- Un niveau d'assurance élémentaire qui accorde un degré limité de fiabilité et dont l'objectif est de réduire les incidents de cybersécurité ;
- Un niveau d'assurance substantiel, d'un niveau de fiabilité plus élevé que le précédent et dont l'objectif est de réduire substantiellement le risque d'incidents de cybersécurité ;
- Un niveau d'assurance élevé, dont l'objectif est de prévenir les incidents de cybersécurité.

Ce cadre est censé s'appliquer à toutes les situations. Or, il apparaît pour beaucoup comme trop rigide. Des solutions pourraient être envisagées pour introduire de la souplesse. Deux pistes sont possibles : soit on introduit au sein de chaque niveau des sous-niveaux pour répondre à un éventail plus large de solutions, soit on définit les niveaux d'assurance au cas par cas pour

chaque schéma de certification afin de répondre au mieux à chaque situation. Cela est également envisageable pour la période de validité des schémas, fixée de manière générale à trois ans, et qui pourrait varier en fonction du schéma considéré.

En outre, le processus est beaucoup trop centralisé et il doit mieux inclure les États membres, d'une part, et les professionnels des technologies de l'information et de la communication, d'autre part.

Ces derniers doivent pouvoir proposer des schémas de certification. En pratique, c'est ce qui se fait actuellement. Leur connaissance du secteur et leur expertise en fait des acteurs clés. Ils doivent aussi être mieux reconnus et impliqués au niveau européen. On peut également envisager que, pour le niveau élémentaire d'assurance, des mécanismes d'auto-certification et d'auto-évaluation soient mis en place pour répondre aux nécessités du marché.

Concernant les États membres, en raison du caractère particulier de la cybersécurité qui relève par certains aspects de la souveraineté nationale et de l'expertise qu'ils ont développé durant les dernières années, il n'est pas admissible qu'ils ne soient que consultés dans le processus de certification, quand bien même ils participent à la gouvernance de l'ENISA. C'est pourquoi, ils devraient pouvoir retrouver leur juste place.

Pour cela, il conviendrait qu'ils puissent, eux aussi, être en initiative de proposer un schéma de certification. En outre, ils doivent être plus présents dans le processus d'adoption, et notamment au niveau du comité chargé de valider un acte d'exécution instaurant un schéma. Par ailleurs, un mécanisme de revue par les pairs pour les plus hauts niveaux d'assurance devrait être mis en place. C'est un mécanisme exigeant, mais fécond, qui est déjà mis en œuvre par la France, l'Allemagne et le Royaume-Uni.

C. POUR UNE ACTION EUROPÉENNE PLUS AMPLE EN FAVEUR DE LA CYBERSÉCURITÉ

Les auditions menées par vos rapporteurs ont révélé qu'au-delà des propositions de la Commission européenne, trois pistes doivent être suivies pour renforcer la cybersécurité européenne : l'effort en matière de recherche doit être confirmé ; la stratégie industrielle de l'Union doit inclure la cybersécurité pour développer une industrie européenne dans le secteur ; l'accent doit être mis sur la formation en France et ailleurs en Europe pour augmenter la ressource humaine qui fait défaut aujourd'hui.

1. Maintenir l'effort de recherche

Le 5 juillet 2016, la Commission européenne a lancé un partenariat public-privé sur la cybersécurité. Son objectif est de stimuler la coopération à

un stade précoce du processus de recherche et d'innovation et de forger des solutions de cybersécurité applicables à différents secteurs, tels que l'énergie, la santé, les transports et la finance. Tandis que l'Union, via son programme pour la recherche et l'innovation Horizon 2020, doit apporter 450 millions d'euros, elle espère un apport trois fois supérieur du secteur privé d'ici à 2020.

Les acteurs du marché de la cybersécurité se sont regroupés au sein de l'organisation européenne pour la cybersécurité, l'ECSO (pour *European cybersecurity organisation*) qui a signé avec la Commission européenne. Cette organisation représente une cinquantaine de membres fondateurs représentatifs du tissu européen de l'industrie dont les entreprises françaises réunies dans l'Alliance pour la confiance numérique, des petites et moyennes entreprises, des utilisateurs, des instituts de recherche et des représentants institutionnels des États membres.

L'initiative est judicieuse. Associer tous les acteurs européens de la cybersécurité peut s'avérer fécond. C'est pourquoi, ce processus doit arriver à son terme. L'effort de l'Union européenne doit être maintenu, voire prolongé dans le prochain cadre financier pluriannuel, si de nouveaux financements s'avéraient nécessaires. Cependant, il ne sera utile que s'il débouche sur un véritable projet industriel européen.

En outre, dans sa communication de septembre 2017, la Commission a proposé la création d'un réseau des centres européens de recherche et de compétences en cybersécurité, composé des centres nationaux de cybersécurité, comme des centres de recherches publiques et des laboratoires. C'est dans le cadre de cette initiative que la Commission a lancé un appel pour un projet pilote d'un montant de 50 millions d'euros, mené dans le cadre du programme de recherche et d'innovation Horizon 2020. Chaque projet pilote devra développer une feuille de route cybersécurité prenant en compte l'ensemble de la chaîne de valeur (de la recherche à la validation), ainsi qu'une gouvernance entre les réseaux pour développer des activités de recherche.

2. Mettre en place une politique industrielle européenne

Des auditions menées, vos rapporteurs retiennent que la cybersécurité n'est encore l'affaire que de quelques entreprises très spécialisées. Si celles-ci sont souvent excellentes, le marché peine à se structurer et à grandir. Il a besoin d'un pilotage afin de faire émerger quelques grands acteurs européens susceptibles de s'intégrer dans la compétition mondiale.

Le partenariat public-privé évoqué constitue l'embryon d'une politique industrielle européenne pour la cybersécurité. Il importe désormais que l'Union transforme celui-ci en stratégie de moyen terme, avec un horizon de 10-15 ans pour, à la fois, soutenir la compétitivité européenne de ce secteur et, à la fois, assurer l'autonomie européenne en la matière et par là-même renforcer la souveraineté européenne dans le monde numérique.

C'est pourquoi, dans la lignée des positions du Sénat sur le numérique, vos rapporteurs appellent à une véritable politique industrielle européenne pour la cybersécurité ou, à défaut, à ce que la stratégie industrielle de l'Union dispose d'un volet consacré à la cybersécurité.

3. Niveau de compétence : l'urgence de la formation

Les auditions menées ont montré les difficultés que connaissent les acteurs de la cybersécurité à recruter. Tant les administrations que les acteurs privés, de petite ou grande taille, ont fait part du manque de ressource humaine qualifiée. On ne forme pas assez d'étudiants et les meilleurs, une fois diplômés, partent.

Cette réalité de terrain reflète une des faiblesses européennes identifiées par la Commission. D'une manière générale, les Européens ne sont pas assez qualifiés pour s'approprier la transformation numérique de nos sociétés. Un gros effort doit être fait par les États membres et par l'Union elle-même, bien qu'elle n'ait que des compétences réduites en la matière.

Il s'agit en premier lieu de former des ingénieurs de très haut niveau et de leur proposer ensuite des carrières attractives, tant dans le public que dans le privé. Il s'agit aussi de créer des emplois nouveaux, avec un certain niveau de qualification visant à répondre au besoin émergent de renforcer la sécurité informatique dans les entreprises, les administrations, les collectivités. Il s'agit, enfin, de développer partout la culture de la cybersécurité en renforçant les qualifications de l'ensemble des salariés.

Notre pays dispose en ce domaine d'atouts formidables : l'excellence de la formation académique, une agence de cybersécurité de référence et des entreprises de haut niveau. Des milliers d'emplois nouveaux pourraient être créés dans les années qui viennent en France et en Europe. Le Gouvernement doit se saisir au plus vite de cette question.

CONCLUSION

La multiplication et la structuration des attaques obligent les pays européens à élever leur niveau de protection et à agir ensemble, de manière coordonnée. L'Europe doit se défendre et protéger ses valeurs, ses populations et ses intérêts dans un cyberespace encore trop peu réglementé et dont les contours sont encore mal connus.

La création d'une agence européenne dédiée à la cybersécurité en 2004 était novatrice. Il a fallu attendre plus de dix ans – et malheureusement subir quelques attaques – pour qu'une réelle dynamique s'enclenche avec la directive NIS.

Une nouvelle étape vers une cybersécurité européenne était attendue. L'ambition affichée par la Commission européenne avec une proposition d'Acte européen pour la cybersécurité mérite d'être soutenue. Le monde numérique évolue trop vite pour que l'Union européenne attende.

Toutefois, cette ambition doit être matinée de réalisme et tenir compte de la situation existante. Car l'objectif est que cette nouvelle étape soit franchie avec succès, car des enjeux de moyen et de long terme pour la souveraineté numérique européenne continuent de se poser.

Le texte fort proposé par la Commission a pu raidir certains acteurs et figer quelques positions à l'ouverture des négociations. Toutefois, les auditions menées par vos rapporteurs ont montré que tous les acteurs ont à cœur de construire une cybersécurité robuste pour une Europe plus résiliente.

Bien que l'actuelle mandature européenne approche de son terme, l'espoir existe de voir adoptée la proposition de règlement avant cette issue. Par des mesures constructives inclues dans le présent rapport, et reprises dans la proposition de résolution n° 455 (2017-2018), vos rapporteurs espèrent modestement y contribuer.

EXAMEN EN COMMISSION

La commission des affaires européennes s'est réunie le jeudi 19 avril 2018 pour l'examen du présent rapport. À l'issue de la présentation faite par M. René Danesi et Mme Laurence Harribey, le débat suivant s'est engagé :

M. Jean Bizet, président. – Ce rapport doit être articulé avec la politique suivie depuis quelques années, sous l'impulsion notamment de Catherine Morin-Desailly avec laquelle nous avions rédigé un rapport, et qui a eu pour résultat l'entrée en vigueur du règlement général sur la protection des données (RGPD). Au-delà de l'aspect purement sécuritaire, l'Europe est en train d'émerger de nouveau en la matière, après avoir subi le rouleau compresseur américain. J'appelle également à la mise en place d'une politique industrielle plus nette sur le sujet.

M. Pascal Allizard. – Je partage le diagnostic du rapport. Je suis rapporteur pour la commission des affaires étrangères du programme 144 « Environnement et prospective de la politique de défense ». J'ai entendu hier matin la direction générale de la sécurité extérieure (DGSE) sur l'évolution des moyens alloués à la cyberdéfense.

La France est en retard : l'Allemagne et le Royaume-Uni sont les deux benchmarks sur lesquels les services travaillent, les Américains étant hors de notre portée. Les priorités affichées dans le projet de loi de programmation militaire vont dans le sens du renforcement et de la cohésion des différents services. En revanche, la dimension européenne n'est pas mise en avant. La DGSE sera le pivot de cette opération : c'est la plus grosse structure ; elle est dotée de moyens ; elle a une mission d'analyse, mais aussi d'interventions grâce à son service Action.

Les ressources humaines sont une véritable problématique, car les besoins sont importants, sans parler du *turn over*. Des conventions sont donc passées avec les universités. Il serait intéressant de croiser votre rapport avec les travaux menés par ailleurs au Sénat. Sur le programme 144, je travaille en binôme avec Michel Boutant. Je m'occupe davantage des problèmes industriels et mon collègue siège à la délégation parlementaire au renseignement.

M. Claude Raynal. – Au vu de l'histoire des procédures européennes, je suis dubitatif concernant la mise en place de telles agences. L'instauration d'une agence de formation, d'information, de bonnes pratiques est un point positif. Mais je me méfie : il ne faudrait pas, pour satisfaire tout le monde, que le système nous tire vers le bas. Il existe aussi un problème de rythme. En Europe, on passe souvent de rien à tout et, au lieu d'accepter de marquer des étapes, on veut immédiatement mettre en

place une réponse globalisante. Je me méfie de ce type de démarche. Respectons les étapes, mettons en route les premiers espaces et voyons. Démarrer par la formation, l'information et la mise à niveau des pays en retard : parfait, c'est indiscutablement le rôle de l'Europe. Mais n'entrons pas tout de suite dans un processus de certification, d'autant que notre modèle sera très vite dépassé.

Par ailleurs, quand des pays sont bien protégés contre la cybersécurité, c'est grâce aux budgets de la défense et non à ceux de la recherche. Cela ne favorise pas la mise en commun…

Pour finir, l'objectif ne me semble pas réaliste au vu de l'effectif et des missions.

M. René Danesi. – Si la France et l'Allemagne sont en avance sur une bonne dizaine de pays, sans parler de ceux qui en sont au point zéro, c'est grâce à la défense, aussi bien en ce qui concerne l'Anssi que le BSI allemand. Les deux agences travaillent d'ailleurs en étroite collaboration. Les difficultés viennent plutôt du Royaume-Uni et de son allié historique, la Suède. Si l'Anssi et le BSI ont éprouvé quelques inquiétudes, c'est qu'elles ont eu le sentiment que l'Union européenne voulait se substituer à elles. Certes, certains hauts responsables européens sont très obtus, mais d'autres sont très ouverts. L'Union européenne a compris que si la protection d'un frigidaire connecté pouvait relever du marché, plus on montait dans la hiérarchie, plus on s'approchait du « secret défense » et de la souveraineté des États, d'où la question de la certification. Elle a donc opéré une marche arrière assez prudente. Le rapport que Mme Niebler présentera devant le Parlement européen va dans ce sens. Les agences qui ont une réelle compétence doivent davantage être représentées au sein de l'Enisa.

Mme Laurence Harribey. – Il existe deux approches en matière de cybersécurité. Il y a ceux pour qui tout passe par le renseignement. En France, nous avons une tradition de séparation entre la notion de résilience au système et le renseignement. Nous assistons à un changement de culture : nous devons passer de la résilience à la cyber-attaque à la culture de la prévention. C'est tout le travail des agences et de la certification. Dans l'innovation technologique, le secteur privé est aujourd'hui plus en avance que le secteur militaire. À mon avis, il convient de promouvoir le modèle allemand et français plutôt que le modèle anglo-saxon.

M. René Danesi. – La présidence bulgare de l'Union européenne a la volonté de faire aboutir ce dossier et s'inscrit plutôt dans l'optique française.

À l'issue de ce débat, la proposition de résolution européenne est adoptée, à l'unanimité, dans le texte suivant :

PROPOSITION DE RÉSOLUTION EUROPÉENNE

① Le Sénat,

② Vu l'article 88-4 de la Constitution,

③ Vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite directive NIS ;

④ Vu la communication conjointe au Parlement européen et au Conseil intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide », JOIN(2017) 450 final ;

⑤ Vu la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) no 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité), COM(2017) 477 final ;

⑥ Vu sa proposition de résolution n° 25 (2017-2018), devenue résolution du Sénat le 6 décembre 2017 portant avis motivé sur la conformité au principe de subsidiarité de la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) - COM(2017) 477 final ;

⑦ Se félicite de la prise de conscience des institutions européennes sur la nécessité de doter l'Union européenne d'une cybersécurité robuste face à une menace en augmentation constante ;

⑧ Souligne que la cybersécurité est un élément indispensable au développement d'une Europe toujours plus connectée et numérisée ;

⑨ **Concernant l'Agence de l'Union européenne pour la cybersécurité (ENISA)**

⑩ Accueille favorablement la proposition de règlement sur la cybersécurité, se satisfait de voir l'ENISA pérennisée et ses moyens augmentés ; appuie l'instauration d'un cadre européen de certification de sécurité informatique ;

⑪ Estime toutefois que l'ENISA doit rester une agence d'appui au travail des agences nationales de cybersécurité et qu'elle doit se concentrer sur des missions ayant une plus-value européenne ;

⑫ **Concernant la coopération européenne dans le domaine de la cybersécurité**

⑬ Juge nécessaire que la coopération entre l'ENISA et les agences nationales, d'une part, et entre les agences nationales elles-mêmes, d'autre part, soit approfondie afin qu'un réseau de confiance s'instaure dans l'ensemble de l'Union ;

⑭ Demande que le modèle de l'Agence nationale de sécurité des systèmes d'information (ANSSI), chargée uniquement d'assurer la défense de nos installations, soit promu auprès des autres États membres pour favoriser l'émergence d'un modèle européen d'agence nationale de cybersécurité ;

⑮ **Concernant la certification européenne de cybersécurité**

⑯ Estime que la mise en place d'une certification unique de cybersécurité dans l'Union européenne doit avoir pour objectif l'élévation du niveau général de sécurité informatique ;

⑰ Considère que cette élévation ne pourra se faire que par la reprise de l'expérience et de l'expertise acquises par certains États membres dans la cybersécurité, afin de l'étendre à tous ;

⑱ Juge nécessaire que le projet de règlement sur la cybersécurité définisse plus clairement le rôle des États pour les aspects relevant de leur souveraineté et assure, dans le processus de certification, l'indépendance entre celui qui évalue et celui qui certifie ;

⑲ Soutient que pour être pleinement efficace, le cadre européen de certification doit être suffisamment souple afin de s'adapter aux besoins et nécessités de toutes les solutions de cybersécurité ;

⑳ Juge indispensable que les États membres et les industriels des technologies de l'information et de la communication soient plus présents dans le processus de certification, notamment dans l'initiative de schémas de certification ;

㉑ **Concernant les prochaines étapes nécessaires**

㉒ Relève que l'adoption du règlement européen sur la cybersécurité marque une étape importante pour la cyber-résilience européenne et appelle d'autres actions ;

㉓ Souligne que les efforts européens en matière de cybersécurité doivent aussi porter sur la recherche et le développement, en particulier dans le cadre du partenariat public-privé sur la cybersécurité ;

㉔ Juge nécessaire que cet effort de recherche soit prolongé par une véritable politique industrielle européenne dans le domaine de la cybersécurité, susceptible de renforcer la souveraineté européenne dans le monde numérique ;

㉕ Relève le manque de personnes qualifiées en cybersécurité en France et en Europe et appelle en conséquence au développement d'une filière de formation d'élite dans la cybersécurité, par une action rapide et générale ;

㉖ Invite le Gouvernement à faire valoir cette position dans les négociations au Conseil.

LISTE DES PERSONNES AUDITIONNÉES

À PARIS :

Mercredi 14 mars 2018

– *Alliance pour la confiance numérique :* **M. Alexis Caurette**, vice-président, **M. Yohann Kassianides**, secrétaire général.

Mercredi 28 mars 2018

– *SIFARIS :* **M. Jean-François Beuze**, président.

– **M. Louis Gautier**, secrétaire général de la défense et de la sécurité nationale.

– *Ministère de l'Europe et des affaires étrangères :* **M. David Martinon**, Ambassadeur pour le numérique.

– *Orange :* **M. Pierre Pétillault**, directeur-adjoint des Affaires Publiques Groupe Orange, **M. Jean-Luc Moliner**, directeur de la sécurité du groupe Orange, **M. Nicolas Arpagian**, directeur Stratégie et Affaires Publiques d'Orange Cyberdefense, **Mme Carole Gay**, Responsable des affaires institutionnelles du groupe.

Mardi 10 avril 2018

– *Ministère de l'Intérieur :* **M. Thierry Delville**, délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces ; **Mme Catherine Chambon, M. Bernard Stephane, M. Ludovic Jacquinet,** Direction générale de la Police nationale ; **M. Éric Freyssinet,** Direction générale de la Gendarmerie nationale ; **M. Patrick Guyonneau,** Direction générale de la Sécurité intérieure.

Mercredi 11 avril 2018

– *Agence nationale de la sécurité des systèmes d'information :* **M. Guillaume Poupard**, directeur général.

– *Thales :* **M. Stanislas de Maupeou**, vice-président stratégie et marketing de l'activité Systèmes d'information critiques et Cybersécurité.

À BRUXELLES, le mercredi 4 avril 2018

– *DG Connect :* **M. Khalil Rouhana**, directeur général adjoint ;

– *Cabinet du Commissaire européen chargé de l'Union de la sécurité :* **Mme Julie Ruff**, membre du cabinet en charge de la cybesécurité ;

– *Service européen d'action extérieure :* **M. François Rivasseau**, directeur pour la politique de sécurité et pour la politique spatiale.

ANNEXE

Schéma de l'élaboration et adoption d'un système européen de certification de cybersécurité proposé par la Commission

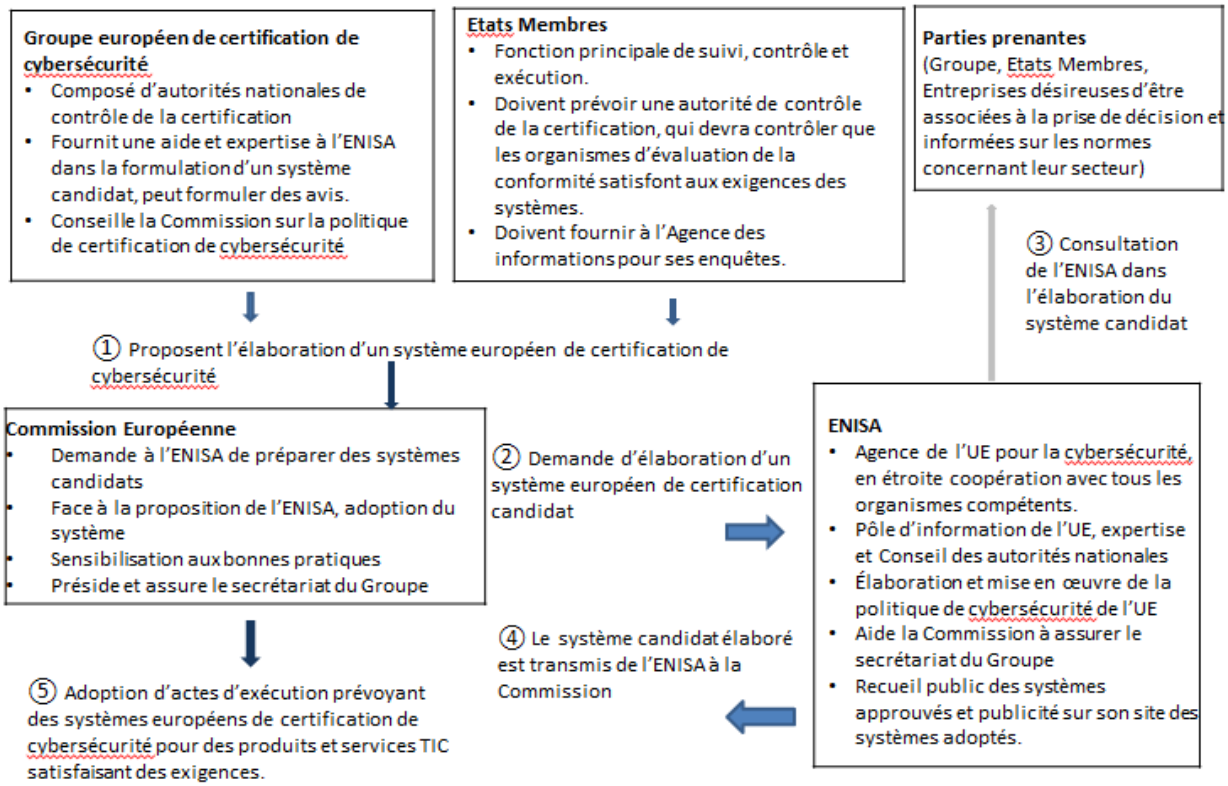

Schéma du mécanisme de certification des produits dans le Cadre Européen de cybersécurité