N° 491

SÉNAT

SESSION ORDINAIRE DE 2012-2013

Enregistré à la Présidence du Sénat le 10 avril 2013

RAPPORT

FAIT

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la proposition de résolution européenne de MM. Jacques BERTHOU et Jean-Marie BOCKEL, présentée en application de l'article 73 quinquies *du règlement, sur la proposition de directive du Parlement européen et du Conseil concernant des* **mesures** *destinées à* **assurer** *un* **niveau élevé commun** *de* **sécurité** *des* **réseaux** *et de l'***information** *dans l'***Union** *(E 8076), et sur la* **stratégie européenne** *de* **cybersécurité** : *un* **cyberespace ouvert**, **sûr** *et* **sécurisé** *(référence : JOIN(2013) 1 final),*

Par MM. Jacques BERTHOU et Jean-Marie BOCKEL,

Sénateurs

et TEXTE DE LA COMMISSION

(1) Cette commission est composée de : M. Jean-Louis Carrère, *président ;* MM. Christian Cambon, Jean-Pierre Chevènement, Robert del Picchia, Mme Josette Durrieu, MM. Jacques Gautier, Robert Hue, Jean-Claude Peyronnet, Xavier Pintat, Yves Pozzo di Borgo, Daniel Reiner, *vice-présidents ;* Mmes Leila Aïchi, Joëlle Garriaud-Maylam, MM. Gilbert Roger, André Trillard, *secrétaires ;* M. Pierre André, Mme Kalliopi Ango Ela, MM. Bertrand Auban, Jean-Michel Baylet, René Beaumont, Pierre Bernard-Reymond, Jacques Berthou, Jean Besson, Jean-Marie Bockel, Michel Boutant, Jean-Pierre Cantegrit, Luc Carvounas, Pierre Charon, Marcel-Pierre Cléach, Raymond Couderc, Jean-Pierre Demerliat, Mme Michelle Demessine, MM. André Dulait, Hubert Falco, Jean-Paul Fournier, Pierre Frogier, Jacques Gillot, Mme Nathalie Goulet, MM. Alain Gournac, Jean-Noël Guérini, Joël Guerriau, Gérard Larcher, Robert Laufoaulu, Jeanny Lorgeoux, Rachel Mazuir, Christian Namy, Alain Néri, Jean-Marc Pastor, Philippe Paul, Bernard Piras, Christian Poncelet, Roland Povinelli, Jean-Pierre Raffarin, Jean-Claude Requier, Richard Tuheiava, André Vallini, Paul Vergès.

Voir le(s) numéro(s) :

Sénat : **458** (2012-2013)

SOMMAIRE

Pages

EXPOSÉ GÉNÉRAL 5

I. QUEL RÔLE POUR L'UNION EUROPÉENNE EN MATIÈRE DE PROTECTION ET DE DÉFENSE DES SYSTÈMES D'INFORMATION ? 6

A. LA MULTIPLICATION DES ATTAQUES CONTRE LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION 6

B. L'UNION EUROPÉENNE A UN RÔLE ESSENTIEL À JOUER 8

II. LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ ET LA PROPOSITION DE DIRECTIVE SUR LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION 12

A. LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ 12

B. LA PROPOSITION DE DIRECTIVE 13

III. LA POSITION DE VOTRE COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉES 14

A. APPROUVER LES PRINCIPALES ORIENTATIONS DE LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ 14

B. SOUTENIR LA PROPOSITION DE DIRECTIVE, SOUS DEUX RÉSERVES 16

PROPOSITION DE RÉSOLUTION 19

TABLEAU COMPARATIF 22

EXAMEN EN COMMISSION 24

ANNEXE I – LES 10 PRIORITÉS DU RAPPORT D'INFORMATION SUR LA CYBERDÉFENSE DE JUILLET 2012 26

ANNEXE II – LES RECOMMANDATIONS DU RAPPORT D'INFORMATION RELATIVES À L'ACTION DE L'UNION EUROPÉENNE EN MATIÈRE DE CYBERDÉFENSE 27

EXPOSÉ GÉNÉRAL

Mesdames, Messieurs,

Depuis déjà plusieurs années, la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat a consacré plusieurs travaux au thème de la **cyberdéfense**, qui regroupe *« l'ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels »*[1].

Après un premier rapport présenté en 2008 par notre ancien collègue M. Roger Romani[2], un deuxième rapport d'information sur la cyberdéfense, présenté par M. Jean-Marie Bockel, a été adopté à l'unanimité en juillet dernier par votre commission[3].

Parmi les 10 priorités et les 50 recommandations contenues dans ce rapport, une partie d'entre elles était consacrée au rôle de l'Union européenne.

En effet, même si la cyberdéfense doit demeurer une compétence première des Etats, car elle touche à la souveraineté nationale, il semble toutefois indispensable, s'agissant d'une menace qui s'affranchit des frontières, de renforcer la coopération internationale et européenne.

Or, l'Union européenne a un grand rôle à jouer dans ce domaine puisque la plupart des normes applicables aux opérateurs de télécommunications relèvent de sa compétence.

Notre commission regrettait toutefois dans ce rapport l'absence de réelle stratégie européenne et la dispersion des acteurs européens et, parmi ses principales recommandations, figurait l'élaboration d'une véritable stratégie européenne dans ce domaine.

La communication conjointe de la Commission européenne et de la Haute représentante pour les affaires étrangères et la politique de sécurité, du 7 février dernier, répond directement à ce souhait puisqu'elle propose une stratégie européenne de cybersécurité. C'est la raison pour laquelle votre commission a souhaité s'en saisir directement, au titre de l'article 73 *quinquies* du Règlement du Sénat, de même que de la proposition de directive sur la sécurité des réseaux et des systèmes d'information de la Commission européenne, qui a été présentée le même jour.

---

[1] *Selon la définition donnée par l'Agence nationale de la sécurité des systèmes d'information.*

[2] *Rapport d'information n° 449 (2007-2008) sur la cyberdéfense, présenté par M. Roger Romani, au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, le 8 juillet 2008.*

[3] *Rapport d'information n° 681 (2011-2012) sur la cyberdéfense, présenté par M. Jean-Marie Bockel, au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, le 18 juillet 2012.*

I. QUEL RÔLE POUR L'UNION EUROPÉENNE EN MATIÈRE DE PROTECTION ET DE DÉFENSE DES SYSTÈMES D'INFORMATION ?

A. LA MULTIPLICATION DES ATTAQUES CONTRE LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

Avec le développement de l'Internet et de l'informatique dans tous les secteurs, les moyens d'information et de communication sont devenus de véritables *« centres nerveux »* de nos sociétés, sans lesquels elles ne pourraient plus fonctionner.

Or, ces dernières années, **les attaques contre les systèmes d'information et de communication se sont multipliées**, si bien qu'elles représentent aujourd'hui **l'une des principales menaces** qui pèsent sur **notre sécurité nationale**.

En effet, il ne se passe pratiquement pas une semaine sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de grands organismes publics ou privés.

Récemment, le Président Barack Obama a indiqué qu'il considérait les cyberattaques comme une menace prioritaire pour la sécurité nationale des Etats-Unis, au même rang que le terrorisme ou le programme nucléaire militaire iranien et nord-coréen.

Lors d'une audition devant le Sénat américain, le 12 mars dernier, les directeurs des services de renseignement américains ont multiplié les mises en garde au sujet des cyberattaques et du cyberespionnage, la Chine étant particulièrement montrée du doigt.

Les responsables américains disent aussi craindre un *« cyber Pearl Harbor »*, c'est-à-dire une attaque informatique massive, visant par exemple la fourniture d'électricité, d'énergie ou de transport, qui aboutirait à une paralysie complète du pays, à l'image de l'attaque informatique subie par l'Estonie en 2007, et dont la Russie pourrait être à l'origine.

Notre pays n'est pas épargné par ce phénomène, comme en témoignent les attaques informatiques dont ont fait l'objet le ministère de l'économie et des finances, à la veille de la présidence française du G8 et du G20, fin 2010, ou encore AREVA, pour ne citer que les attaques qui ont été révélées par la presse.

De manière schématique, on peut distinguer **quatre types** d'attaques informatiques :

- tout d'abord, tout ce qui relève de **la cybercriminalité**, qui regroupe par exemple l'escroquerie via Internet ou la pédopornographie sur Internet, et qui est en plein essor. Selon la Commission européenne la cybercriminalité ferait plus d'un million de victimes chaque jour dans le monde ;

- Ensuite, les attaques visant à **perturber** le fonctionnement des systèmes, par une saturation de service : c'est par exemple le cas des attaques du groupe *Anonymous* visant des sites Internet d'institutions publiques ou privées ;

- troisième type d'attaque, **le cyberespionnage**, qui se développe considérablement ;

- et, enfin, ce qui est assez nouveau, les attaques informatiques visant à **détruire** les systèmes.

On connaissait déjà, depuis juin 2010, le cas de STUXNET, ce programme informatique qui aurait été développé par les Etats-Unis et Israël et qui aurait détruit un millier de centrifugeuses de la centrale nucléaire iranienne de Natanz. Mais, en août dernier, deux attaques informatiques d'ampleur ont visé des sociétés du secteur de l'énergie au Moyen Orient, dont le premier producteur mondial de pétrole *Saudi Aramco*. 30 000 ordinateurs ont été rendus inutilisables lors d'une attaque revendiquée par un groupe terroriste.

D'une manière générale, ces attaques peuvent être menées par des pirates informatiques, des groupes d'activistes, des organisations criminelles, mais aussi par des entreprises concurrentes, voire par d'autres Etats.

Les soupçons se portent souvent vers la Chine ou la Russie, mais ils ne sont vraisemblablement pas les seuls et il est très difficile d'identifier précisément les auteurs de ces attaques.

À l'avenir, **on doit s'attendre à une croissance du nombre d'attaques informatiques**, en raison du développement du rôle de l'Internet et de l'informatique dans tous les secteurs.

D'ores et déjà, nous connaissons les téléphones portables, les ordinateurs, les tablettes, etc. Mais, demain, la plupart des objets de la vie quotidienne – de la voiture au *pacemaker*, seront également reliés à l'Internet et donc vulnérables aux attaques informatiques. Selon Cisco, plus de 50 milliards d'objets devraient être connectés à Internet l'horizon 2020 !

Par ailleurs, les risques ne pourront que s'accroître à l'avenir avec des pratiques comme le *BYOD (« Bring Your Own Device »* consistant à utiliser son ordinateur personnel pour un usage professionnel) ou encore l'informatique en nuage (*« cloud computing »*), qui consiste à utiliser des serveurs à distance, accessibles par Internet, pour traiter ou stocker de l'information.

Dans son rapport d'information, votre commission considérait donc que la cyberdéfense devrait faire l'objet d'**une véritable priorité nationale**, portée au plus haut niveau de l'Etat, et elle formulait **dix priorités**[1], assorties de **50 recommandations** concrètes, dont une partie était consacrée **au rôle de l'Union européenne**.

---

[1] *Voir la liste des dix priorités qui figure en annexe 1 au présent rapport*

B. L'UNION EUROPÉENNE A UN RÔLE ESSENTIEL À JOUER

Si la protection des systèmes d'information doit demeurer avant tout une compétence nationale, car elle touche directement à la souveraineté de chaque Etat, l'Union européenne a cependant un rôle important à jouer car une grande partie des normes applicables aux opérateurs relèvent de ses compétences.

Ces dernières années, les instances européennes ont adopté de **nombreux documents d'orientations ou de programmes** intéressant directement ou indirectement la sécurité des systèmes d'information.

On peut notamment mentionner :

- la stratégie dite *« i2010 »* (*« Une société de l'information pour la croissance et l'emploi »*), exposée dans une communication de la Commission européenne du 1er juin 2005, et qui confirme l'importance de la sécurité des réseaux ;

- la communication de la Commission du 31 mai 2006, intitulée *« Une stratégie pour une société de l'information sûre – dialogue, partenariat et responsabilisation »*, qui contient notamment une évaluation comparative des politiques nationales relatives à la sécurité des réseaux et de l'information mais qui ne propose aucune action concrète ;

- la communication de la Commission de mars 2009 relative à la *« protection des infrastructures d'information critiques »*, qui fixe des objectifs prioritaires dans le domaine de la sécurité des systèmes d'information et qui a débouché sur un plan d'action, adopté en avril 2009. Parmi les différentes mesures envisagées, la Commission européenne se donne notamment pour objectif le développement par chaque Etat membre d'un CERT opérationnel, l'organisation d'exercices de gestion de crise cyber aux niveaux national et européen ou encore la création d'un forum d'échange public-privé européen, etc. Ce plan d'action a été approuvé par le Conseil en décembre 2009 ;

- la communication de la Commission de mai 2010 intitulée *« Une stratégie numérique pour l'Europe »*, qui aborde l'ensemble des enjeux liés au développement de la société de l'information en Europe. Cette communication souligne à nouveau la nécessité d'une mise en œuvre rapide et efficace du plan d'action de l'Union européenne pour la protection des infrastructures d'information critiques ;

- une nouvelle communication de la Commission européenne relative à *« la protection des infrastructures d'information critiques »* de mars 2011, qui reprend et développe les cinq axes de la communication de mars 2009 et introduit de nouvelles propositions, telles que le développement d'un plan européen de continuité en cas de crise cyber et la création d'un groupe de travail commun Union européenne-Etats-Unis sur la cybersécurité et la cybercriminalité. Cette communication a fait l'objet de conclusions du Conseil

en mai 2011, qui soulignent notamment l'importance stratégique de l'industrie européenne des télécommunications et de l'industrie de la sécurité des réseaux et de l'information en vue de la protection durable des infrastructures d'information critiques européennes.

Il faut également relever que des initiatives ont été prises au niveau européen en matière de lutte contre la cybercriminalité, avec par exemple l'adoption, le 24 février 2005, d'une décision-cadre relative aux attaques visant les systèmes d'information et une proposition de directive.

Toutefois, cette directive n'a pas été adoptée et est moins ambitieuse que la Convention de lutte contre la cybercriminalité, dite *« Convention de Budapest »*, conclue au sein du Conseil de l'Europe, mais qui n'a pas encore été ratifiée par l'ensemble des Etats membres de l'Union européenne.

Plus récemment, en janvier dernier, un centre européen de lutte contre la cybercriminalité a été créé au sein de l'office européen de police Europol.

Une directive a aussi été adoptée le 8 décembre 2008 relative à la protection des infrastructures critiques européennes, mais ce texte, qui se limite aux secteurs de l'énergie et des transports, se contente d'appeler les Etats-membres à identifier les infrastructures critiques concernées et à prévoir des mesures en matière de sécurité, sans entrer véritablement dans le détail des mesures nécessaires.

Par ailleurs, la cyberdéfense est également un thème de travail récent de la politique de sécurité et de défense commune, notamment au sein de l'Agence européenne de défense, qui a constitué une *« Project Team »* sur ce sujet. Toutefois, les travaux de l'Union européenne dans ce domaine sont encore très embryonnaires et n'ont pas encore débouché sur des réalisations concrètes.

D'une manière générale, votre commission portait dans son rapport d'information **un regard assez critique sur l'action de l'Union européenne en matière de cybersécurité.**

Ainsi, elle relevait que *« malgré l'adoption de nombreux documents ou plans d'action,* ***l'Union européenne, et la Commission européenne en particulier, ne semblent pas encore avoir pris la mesure de l'importance des enjeux liés à la sécurité des systèmes d'information, comme d'ailleurs de nombreux pays européens ».***

Dans son rapport d'information, votre commission mentionnait **trois principales lacunes.**

Tout d'abord, **l'absence de véritable stratégie globale du cyberespace à l'échelle européenne**.

Ensuite, **une dispersion des acteurs**, ce sujet étant traité par différentes directions générales au sein de la Commission européenne et par le service européen pour l'action extérieure.

Enfin, **un manque d'efficacité**.

En particulier, le rapport soulignait que *« **l'Union européenne ne paraît pas encore en mesure d'assurer la protection de l'ensemble de ses propres réseaux et systèmes d'information ».***

L'Union européenne s'est certes dotée, le 10 juin 2011, d'un CERT (« Computer Emergency Response Team ») chargé de prévenir et de répondre aux attaques informatiques visant les réseaux ou systèmes des institutions européennes, des agences ou des autres organes qui lui sont rattachés (CERT-UE). Mais, comme le soulignait votre commission, *« cette structure, qui ne compte que dix agents, n'en est encore qu'au stade de la préfiguration et est encore très loin d'assurer une protection de l'ensemble des réseaux et systèmes de l'Union européenne ».*

Par ailleurs, *« la coordination et l'efficacité des différents outils, mécanismes et politiques, à la fois réglementaires et incitatifs, mis en place à l'échelle européenne pour encourager la prise en compte par les Etats membres des enjeux liés à la protection des systèmes d'information mériteraient d'être notablement renforcés ».*

Le rapport était particulièrement sévère concernant l'agence européenne chargée de la sécurité des réseaux et de l'information, l'**ENISA** (*European Network and Information Security Agency*)

Cette agence a été créée en 2004 avec un mandat initial d'une durée de cinq ans.

Installée à Heraklion, en Crète, **l'ENISA s'est vue assigner des missions très vastes,** que l'on peut regrouper en trois catégories :

- conseiller et assister, en tant qu'agence d'expertise technique, la Commission européenne et les États membres en matière de sécurité des systèmes d'information, notamment au travers de « guides de bonnes pratiques » ;

- soutenir les Etats membres et les institutions européennes dans le développement de capacités pour répondre aux menaces pesant sur la sécurité des systèmes d'information ;

- encourager la coopération entre les Etats membres, notamment par des exercices communs.

Cette agence européenne n'a donc pas de compétences opérationnelles mais plutôt une mission de conseil et de recommandation. Elle disposait d'environ 60 agents et d'un budget de 8,5 millions d'euros en 2012.

L'ENISA a fait l'objet d'une **évaluation externe** demandée par la Commission européenne, qui en a publié le résultat en juin 2007. Le groupe d'experts externe a conclu que **les activités de l'ENISA paraissaient « *insuffisantes pour atteindre le niveau élevé d'impact et de valeur ajouté espéré* »** et que sa visibilité était en dessous des attentes. L'évaluation a recensé divers handicaps liés à son organisation, aux ambiguïtés du mandat originel, à sa localisation éloignée, à l'effectif et à la rotation importante du

personnel, aux relations difficiles entre le conseil d'administration et la direction de l'agence. Elle a souligné un risque d'affaiblissement rapide et de perte de réputation si l'efficacité n'était pas améliorée. Le Livre blanc sur la défense et la sécurité nationale de 2008 a relevé également que « *l'efficacité de l'agence européenne ENISA devra être très notablement accrue* ».

Dans son rapport, votre commission reconnaissait toutefois que, ces derniers mois, l'agence a publié des rapports intéressants avec des recommandations concrètes, par exemple sur les systèmes de contrôle industriels et les SCADA ou encore la cybersécurité maritime.

Le mandat de l'ENISA a été prolongé jusqu'en septembre 2013 et une proposition de règlement visant à modifier et à étendre le mandat de cette agence est actuellement en discussion au niveau européen.

Votre commission soulignait également l'adoption, **en novembre 2009**, de **la directive cadre du « Paquet Télécom »** modifiant la régulation des communications électroniques en Europe[1].

Cette directive contient une disposition (article 13 *bis*) contraignant les opérateurs de télécommunications à notifier aux autorités nationales compétentes toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services. Elle introduit également l'obligation de mise en œuvre de mesures de sécurité minimales par les opérateurs, les autorités nationales étant chargées de s'assurer que les opérateurs respectent ces obligations (article 13 *ter*).

Cette directive cadre a été transposée en France par le biais de l'ordonnance du 24 août 2011, qui a modifié la loi du 6 janvier 1978 dite « informatique et libertés », en prévoyant notamment l'obligation pour les opérateurs de télécommunications de notifier à la CNIL toute faille de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

En définitive, pour votre commission, il était souhaitable que l'Union européenne s'implique plus activement sur les questions liées à la protection des systèmes d'information.

En particulier, il lui semblait indispensable que **l'Union européenne se dote d'une véritable stratégie européenne qui englobe l'ensemble des questions liées au cyberespace. L'élaboration d'une telle stratégie figurait expressément parmi les recommandations de votre commission[2].**

---

[1] *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009*

[2] *Voir les recommandations n°39 à 44 du rapport d'information n°681 (2011-2012) sur la cyberdéfense du 18 juillet 2012, qui ont été reproduites en annexe 2 au présent rapport*

II. LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ ET LA PROPOSITION DE DIRECTIVE SUR LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION

A. LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ

La Commission européenne et la Haute représentante pour les affaires étrangères et la politique de sécurité ont présenté, le 7 février dernier, une communication conjointe intitulée *« Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé »*[1].

Le fait même que cette communication ait été rédigée à la fois par les services de la Commission européenne et ceux du service européen pour l'action extérieure mérite d'être salué, car cela témoigne d'une approche globale des questions liées à la cybersécurité.

Cette stratégie distingue **cinq grands axes** de renforcement de l'action de l'Union européenne :

- le renforcement de la lutte contre la cybercriminalité ;
- la cyber-résilience ;
- le volet cyberdéfense de la politique de sécurité et de défense commune (PSDC) ;
- les ressources industrielles et technologiques ;
- et, enfin, la prise en compte de la cybersécurité dans le cadre de l'action internationale de l'Union européenne.

En ce qui concerne la sécurité des réseaux et des systèmes d'information, la Commission européenne souligne notamment :

- la nécessité de développer des capacités nationales de cybersécurité et de cyberdéfense, ainsi que du renforcement de la coopération européenne ;

- l'importance de disposer d'une industrie européenne en matière de cybersécurité et d'équipements de confiance afin d'éviter une dépendance critique à l'égard de fournisseurs extérieurs à l'Union : la Commission mentionne à plusieurs reprises le cas des « routeurs de cœur de réseaux » ;

- l'importance de la formation et de la sensibilisation. La Commission européenne prévoit ainsi la création d'un « permis de conduire » européen en matière de sécurité des systèmes d'information pour les professionnels.

Enfin, on peut relever que la Commission européenne considère qu'un cyber incident ou une cyberattaque particulièrement sérieux pourraient constituer un motif suffisant pour qu'un Etat membre invoque la « clause de solidarité », prévue à l'article 222 du traité sur le fonctionnement de l'Union européenne.

---

[1] *Join (2013) 1 final*

B. LA PROPOSITION DE DIRECTIVE

La proposition de directive sur la sécurité des réseaux et des systèmes d'information a été présentée par la Commission européenne le 7 février dernier[1], en même temps que la stratégie européenne de cybersécurité.

Cette proposition de directive comporte **trois volets**.

Le **premier volet** porte sur **le renforcement des capacités nationales des Etats membres en matière de cybersécurité**.

La proposition de directive impose l'obligation, pour tous les Etats membres, de se doter d'une autorité nationale de cybersécurité, d'élaborer une stratégie nationale en la matière et de disposer d'une structure opérationnelle d'assistance au traitement d'incidents informatiques.

Il est indiqué que *« les Etats membres veillent à ce que les autorités compétentes disposent de ressources techniques, financières et humaines suffisantes pour pouvoir s'acquitter de leurs tâches de manière efficace et efficiente »*.

Le **deuxième volet** concerne **le renforcement de la coordination européenne en matière de réponse aux incidents**.

La proposition de directive prévoit notamment :

- la création d'un réseau européen des autorités nationales de cybersécurité pour coopérer dans la lutte contre les risques et incidents touchant les réseaux et systèmes informatiques ;

- l'obligation pour ces autorités d'alerter le réseau en cas d'incidents informatiques majeurs ;

- un plan de coopération de l'Union européenne.

Le **troisième volet** porte sur l'instauration de **l'obligation,** pour les administrations publiques et plusieurs opérateurs de secteurs d'importance critique, **de notifier, sous peine de sanctions mais avec une garantie de confidentialité, les incidents informatiques significatifs à l'autorité nationale de cybersécurité**.

La Commission européenne propose ainsi d'étendre l'obligation de notification des incidents informatiques significatifs, qui ne s'applique actuellement qu'aux opérateurs de télécommunications, à l'ensemble des administrations publiques et aux opérateurs de secteurs d'importance vitale, comme l'électricité, l'énergie, les transports ou la santé.

Pour la mise en œuvre de ces différentes mesures, la proposition de directive prévoit le recours systématique à des actes délégués et d'exécution de la Commission européenne, laissant ainsi peu de marges de manœuvre aux Etats membres.

---

[1] *Com (2013) 48 final – Texte E 8076*

III. LA POSITION DE VOTRE COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉES

Dans le prolongement des travaux de votre commission sur les questions liées à la cyberdéfense et afin que le Sénat puisse se prononcer et faire connaître au gouvernement sa position sur ce sujet, vos deux co-rapporteurs ont présenté une **proposition de résolution européenne**, fondée sur l'article 88-4 de la Constitution, qui a été adoptée par la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat.

Cette proposition de résolution vise à inciter le Gouvernement à œuvrer au sein du Conseil de l'Union européenne afin que soient pris en compte les principes suivants.

A. APPROUVER LES PRINCIPALES ORIENTATIONS DE LA STRATÉGIE EUROPÉENNE DE CYBERSÉCURITÉ

Dans l'ensemble, **on peut saluer la stratégie européenne de cybersécurité, qui témoigne d'une prise de conscience de la part des institutions européennes de l'importance des enjeux de cybersécurité**.

On peut se féliciter, en particulier, de l'accent mis sur **les aspects industriels.**

Afin de garantir la souveraineté des opérations stratégiques ou la sécurité de nos infrastructures vitales, il est, en effet crucial de s'assurer de la maîtrise de certaines technologies fondamentales, dans des domaines comme la cryptologie, l'architecture matérielle et logicielle et la production de certains équipements de sécurité ou de détection. Garder cette maîtrise, c'est protéger nos entreprises, notamment face au risque d'espionnage informatique.

La France dispose certes de nombreux atouts avec de grandes entreprises – comme Thales, Cassidian, Bull, Sogeti ou encore Alcatel Lucent – et d'un tissu de PME innovantes, par exemple dans le domaine de la cryptologie ou des cartes à puces. Mais face à la concurrence américaine aujourd'hui, et demain chinoise, russe et indienne, il est indispensable pour notre pays et pour l'Europe de conserver une autonomie stratégique dans ce domaine. On pense notamment au domaine sensible des « routeurs de cœur de réseaux » ou d'une offre de *« cloud »* de confiance en Europe. On ne doit pas négliger non plus les enjeux économiques et en matière d'emplois dans ce secteur en forte croissance, qui participe à la compétitivité d'un pays.

Dans son rapport d'information, notre commission plaidait donc pour une politique industrielle volontariste, à l'échelle nationale et européenne, afin de soutenir le tissu industriel des entreprises françaises et européennes, notamment des PME, proposant des produits ou des services importants pour la sécurité informatique et plus largement du secteur de l'information et des télécommunications.

La France pourrait, si elle en a la volonté, développer une industrie complète et souveraine dans le domaine de la sécurité des systèmes d'information, à la fois dans les secteurs des matériels, des logiciels et des services.

Mais cela suppose une politique industrielle volontariste à l'échelle de l'Union européenne, notamment pour soutenir les entreprises européennes qui produisent ce type d'équipements face à la concurrence d'entreprises de pays tiers.

Selon la Commission européenne, l'Europe devrait avoir l'ambition de parvenir à une souveraineté numérique, ce qui veut dire retrouver la maîtrise de certains composants ou équipements.

De ce point de vue, **la stratégie européenne de cybersécurité témoigne d'une véritable prise de conscience de ces enjeux de la part de la Commission européenne** et répond pleinement à notre souhait.

La Commission européenne envisage notamment de soutenir les efforts de normalisation au niveau européen, un système de certification, des financements par le biais de programmes européens des efforts de recherche et développement, mais aussi la prise en compte de la sécurité informatique dans les marchés publics ou encore dans les primes d'assurance.

Un autre aspect important concerne **la formation.**

Il existe aujourd'hui dans notre pays peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à en recruter.

Dans son rapport d'information, notre commission recommandait donc de mettre l'accent sur la formation et de développer les liens avec les universités et les centres de recherche et c'est également l'une des orientations retenues par la Commission européenne.

Il paraît aussi nécessaire de renforcer **la sensibilisation** des administrations, des entreprises, des opérateurs d'importance vitale et des utilisateurs au respect des règles élémentaires de sécurité, règles que le directeur général de l'ANSSI, M. Patrick Pailloux assimile souvent à des règles d'hygiène informatique élémentaires, mais qui sont souvent considérées comme autant de contraintes par les utilisateurs.

Sur ce dernier point, la Commission propose plusieurs actions, comme par exemple l'organisation en 2014 d'un championnat européen de la cybersécurité ou des exercices de simulation de cyberincidents au niveau européen.

Votre commission vous recommande donc **d'approuver les orientations générales de cette stratégie** et **d'appeler les institutions européennes et les Etats membres à une mise en œuvre rapide de ces priorités**.

B. SOUTENIR LA PROPOSITION DE DIRECTIVE, SOUS DEUX RÉSERVES

D'une manière générale, **on peut également approuver les principales dispositions de la proposition de directive.**

Il en va en particulier de l'obligation, pour les Etats membres de l'Union, de se doter de structures chargées de la cybersécurité et d'une stratégie nationale dans ce domaine.

Face à la multiplication des attaques informatiques ces dernières années, la plupart des grands Etats membres se sont dotés de tels instruments.

Ainsi, dans le cas de la France, grâce à l'impulsion donnée par le précédent Livre blanc sur la défense et la sécurité nationale de 2008, une agence nationale de la sécurité des systèmes d'information (l'ANSSI) a été créée en 2009 et notre pays s'est doté d'une stratégie nationale dans ce domaine en 2011.

Cette agence, rattachée au Secrétaire général de la défense et de la sécurité nationale et dépendante du Premier ministre, est un service à compétence nationale. Elle comporte en son sein un centre opérationnel chargé de traiter les incidents informatiques.

Ainsi, c'est l'ANSSI qui a traité l'affaire d'espionnage informatique de Bercy découverte à la veille de la présidence française du G8 et du G20, fin 2010.

Elle compte environ 350 personnes, principalement des ingénieurs, et son budget est de l'ordre de 75 millions d'euros.

Le Royaume-Uni et l'Allemagne disposent également de tels organismes, mais avec des effectifs deux à trois fois supérieurs et une organisation parfois différente.

Cependant, tous les autres pays membres de l'Union européenne ne disposent pas encore de tels organismes ce qui illustre le fait que, pour ces pays, la cybersécurité n'est pas encore considérée comme une priorité.

La proposition de directive permettra donc un progrès.

On peut également se féliciter de l'instauration **d'une obligation de déclaration des incidents informatiques significatifs** à l'autorité nationale compétente qui serait applicable non seulement aux opérateurs de télécommunications, mais aussi aux administrations publiques et aux opérateurs critiques, tels que les entreprises de certains secteurs jugés stratégiques, comme les banques, la santé, l'énergie et les transports.

Cette obligation de déclaration répond d'ailleurs directement à l'une des recommandations qui figure dans le rapport d'information sur la cyberdéfense, qui avait été adoptée à l'unanimité par la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat.

En effet, la plupart du temps, les entreprises sont réticentes à faire part à l'Etat des attaques informatiques dont elles ont fait l'objet[1], par crainte que cela nuise à leur image, à leur réputation, voire même que cela n'entraîne une diminution du cours de leur action en bourse. Cela concerne en particulier les cas d'espionnage informatique et le vol de secrets industriels.

Or, comment l'Etat pourrait-il aider ces entreprises à mieux protéger leurs systèmes et leurs secrets, s'il n'est même pas informé des attaques informatiques dont elles font l'objet ?

L'obligation de déclaration, sous peine de sanctions, mais avec une garantie de confidentialité, constituerait donc une avancée importante, y compris dans le cas de la France.

On peut également se féliciter d'autres dispositions, comme celles de prévoir que les autorités nationales auront le pouvoir de donner des instructions contraignantes aux administrations publiques et aux opérateurs d'importance vitale ou le pouvoir de demander la réalisation d'un audit sur la sécurité de leurs réseaux et systèmes.

Qui peut sérieusement contester l'importance de mieux protéger les réseaux et systèmes d'information de secteurs d'importance stratégique, dont la perturbation pourrait avoir de graves conséquences et conduire à une paralysie générale du fonctionnement de notre pays ? On pense par exemple à la fourniture d'électricité, aux transports ou encore aux banques.

D'une manière générale, **la proposition de directive paraît donc aller dans le bon sens et votre commission vous propose d'approuver ses principales dispositions.**

On pourrait même aller un peu plus loin et prévoir notamment l'obligation pour les opérateurs d'importance vitale :

- de disposer d'une cartographie à jour de leur système d'information ;

- de mettre en place des outils de détection d'incidents et d'attaques informatiques.

En effet, l'expérience des attaques informatiques traitées par l'ANSSI montre que la plupart des administrations ou des opérateurs d'importance vitale ayant été victimes d'attaques informatiques à des fins d'espionnage ignoraient le plus souvent les attaques dont ils faisaient l'objet, parfois depuis plusieurs mois, voire des années. En outre, ils ignoraient le plus souvent où étaient situés leurs propres ordinateurs, ce qui avait pour effet de retarder l'assainissement de leurs réseaux.

La proposition de directive soulève néanmoins **deux réserves**.

La **première réserve** porte sur **la définition des modalités d'application de ces mesures**, qui serait confiée à la Commission européenne,

---

[1] *Une étude de l'ENISA du 27 août 2012 indique que la plupart des incidents ne sont pas signalés*

par exemple en ce qui concerne la définition des circonstances dans lesquelles s'appliquerait l'obligation de notifier les incidents ou la liste des opérateurs d'importance vitale concernés.

Il semble qu'il serait plus légitime, tant pour des raisons tenant à la souveraineté nationale, que d'efficacité, que **les modalités d'application soient confiées aux Etats membres**, qui, en définitive, sont les premiers responsables en matière de cybersécurité et sont mieux placés pour prendre les mesures appropriées.

La **seconde réserve** est plus fondamentale.

Elle concerne l'obligation faite aux autorités compétentes de notifier systématiquement les incidents informatiques à la Commission européenne et à l'ensemble des autres pays de l'Union européenne.

Outre sa lourdeur bureaucratique, une telle mesure paraît susceptible de soulever des difficultés au regard de la sécurité nationale, notamment dans le cas d'attaques informatiques à des fins d'espionnage.

Il faut savoir que, si les soupçons se portent le plus souvent sur la Chine ou la Russie, d'autres pays, y compris parmi nos proches alliés, sont aussi soupçonnés d'être à l'origine de telles attaques.

Or, informer la Commission européenne et l'ensemble des Etats membres de l'Union européenne de l'attaque informatique dont on fait l'objet risquerait d'alerter également – directement ou indirectement - l'auteur de cette attaque. Celui-ci pourrait alors prendre des mesures afin de se dissimuler davantage ou augmenter encore le niveau de son attaque.

*

Selon les informations recueillies par vos deux co-rapporteurs, la stratégie européenne de cybersécurité devrait être examinée par les ministres des vingt-sept Etats membres lors du Conseil « Affaires générales » de juin, puis par les chefs d'Etat et de gouvernement, lors d'un Conseil européen, et elle devrait faire l'objet de conclusions du Conseil et du Conseil européen.

Pour sa part, la proposition de directive devrait faire l'objet d'un premier échange entre les ministres lors du Conseil « transports, télécommunications et énergie » du mois de juin, et pourrait être adoptée par le Conseil et le Parlement européen d'ici la fin de l'année. Elle devrait ensuite faire l'objet de mesures de transposition dans les différents Etats membres.

*

Au bénéfice de ces observations, votre commission des Affaires étrangères, de la Défense et des Forces armées a adopté la proposition de résolution, dont le texte est reproduit ci-après.

PROPOSITION DE RÉSOLUTION

① Le Sénat,

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

③ Vu la communication conjointe de la Commission européenne et de la Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité du 7 février 2013 relative à la « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé »,

④ Vu la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (texte E 8076),

⑤ Considérant que les attaques contre les systèmes d'information et de communication constituent aujourd'hui une menace réelle et constante, pouvant déstabiliser le fonctionnement même de nos sociétés et dont le caractère transnational justifie pleinement une action au niveau européen,

⑥ Se félicite de la publication de la stratégie européenne de cybersécurité, qui témoigne d'une approche globale et cohérente de l'Union européenne des risques et des enjeux soulevés par la multiplication des attaques contre les systèmes d'information et de communication,

⑦ Appelle les institutions européennes et les Etats membres à une mise en œuvre rapide des différentes priorités de cette stratégie,

⑧ Souligne en particulier :

⑨ - l'importance de la mise en place et du développement par l'ensemble des Etats membres de capacités nationales de cybersécurité et du renforcement de la coopération européenne dans ce domaine ;

⑩ - la nécessité de disposer d'une base industrielle européenne pérenne en matière de cybersécurité et d'équipements de confiance qui suppose la mise œuvre par l'Union européenne d'une véritable politique industrielle dans ce domaine ;

⑪ - l'importance des actions de sensibilisation et de formation ;

⑫ Recommande d'inclure dans cette stratégie :

⑬ - la prise en compte de la cybersécurité dans les relations de l'Union européenne avec les pays tiers,

⑭ - le renforcement de la coopération policière et judiciaire à l'échelle européenne en matière de lutte contre la cybercriminalité,

⑮ Approuve de manière générale les dispositions de la proposition de directive, en particulier en ce qui concerne :

⑯ - la nécessité, pour chaque Etat membre, de disposer d'un organisme responsable, doté de ressources humaines et financières suffisantes, d'une stratégie nationale et d'une structure opérationnelle d'assistance au traitement d'incidents informatiques,

⑰ - l'obligation, pour les administrations publiques et les acteurs du marché, de notifier, sous peine de sanctions, les incidents graves de sécurité à l'autorité nationale compétente,

⑱ - la nécessité de prévoir dans chaque Etat membre que les autorités compétentes auront le pouvoir de donner des instructions contraignantes aux administrations publiques et aux acteurs du marché et qu'elles pourront exiger certaines informations ou la réalisation d'un audit, afin de renforcer la sécurité de leurs réseaux et systèmes,

⑲ Recommande d'inclure dans la proposition de directive :

⑳ - l'obligation pour les opérateurs d'importance vitale de mettre en place des outils de détection d'incidents et d'attaques informatiques,

㉑ - l'obligation pour les opérateurs d'importance vitale de disposer d'une cartographie à jour de leur système d'information,

㉒ Estime, toutefois, que la définition des modalités d'application de ces mesures devrait être confiée aux Etats membres et non à la Commission européenne, notamment en ce qui concerne :

㉓ - la définition des circonstances dans lesquelles s'appliquerait l'obligation de notifier les incidents ;

㉔ - la liste des secteurs d'importance critique,

㉕ Juge également qu'il ne serait pas pertinent de prévoir :

㉖ - la notification systématique des incidents par les autorités nationales à l'ensemble des Etats membres et à la Commission européenne,

㉗ Demande au gouvernement de soutenir ces deux initiatives, et notamment de favoriser une adoption rapide de la proposition de directive, et d'œuvrer au sein du Conseil afin que ces recommandations soient prises en compte lors des négociations.

TABLEAU COMPARATIF

___

Texte de la proposition de résolution initiale ___	Texte adopté par la commission ___
Proposition de résolution présentée en application de l'article 73 quinquies du règlement, relative à la stratégie européenne de cybersécurité	**Proposition de résolution présentée en application de l'article 73 quinquies du règlement, relative à la stratégie européenne de cybersécurité**
Le Sénat,	
Vu l'article 88-4 de la Constitution,	*Sans modifications*
Vu la communication conjointe de la Commission européenne et de la Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité du 7 février 2013 relative à la « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé »,	
Vu la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (texte E 8076),	
Considérant que les attaques contre les systèmes d'information et de communication constituent aujourd'hui une menace réelle et constante, pouvant déstabiliser le fonctionnement même de nos sociétés et dont le caractère transnational justifie pleinement une action au niveau européen,	
Se félicite de la publication de la stratégie européenne de cybersécurité, qui témoigne d'une approche globale et cohérente de l'Union européenne des risques et des enjeux soulevés par la multiplication des attaques contre les systèmes d'information et de communication,	
Appelle les institutions européennes et les Etats membres à une mise en œuvre rapide des différentes priorités de cette stratégie,	
Souligne en particulier : - l'importance de la mise en place et du développement par l'ensemble des Etats membres de capacités nationales de cybersécurité et du renforcement de la coopération européenne dans ce domaine ; - la nécessité de disposer d'une base industrielle européenne pérenne en matière de cybersécurité et d'équipements de confiance qui suppose la mise œuvre par l'Union européenne d'une véritable politique industrielle dans ce domaine ; - l'importance des actions de sensibilisation et de	

Texte de la proposition de résolution initiale	Texte adopté par la commission
formation ;	
Recommande d'inclure dans cette stratégie : - la prise en compte de la cybersécurité dans les relations de l'Union européenne avec les pays tiers, - le renforcement de la coopération policière et judiciaire à l'échelle européenne en matière de lutte contre la cybercriminalité,	
Approuve de manière générale les dispositions de la proposition de directive, en particulier en ce qui concerne : - la nécessité, pour chaque Etat membre, de disposer d'un organisme responsable, doté de ressources humaines et financières suffisantes, d'une stratégie nationale et d'une structure opérationnelle d'assistance au traitement d'incidents informatiques, - l'obligation, pour les administrations publiques et les acteurs du marché, de notifier, sous peine de sanctions, les incidents graves de sécurité à l'autorité nationale compétente, - la nécessité de prévoir dans chaque Etat membre que les autorités compétentes auront le pouvoir de donner des instructions contraignantes aux administrations publiques et aux acteurs du marché et qu'elles pourront exiger certaines informations ou la réalisation d'un audit, afin de renforcer la sécurité de leurs réseaux et systèmes,	
Recommande d'inclure dans la proposition de directive : - l'obligation pour les opérateurs d'importance vitale de mettre en place des outils de détection d'incidents et d'attaques informatiques, - l'obligation pour les opérateurs d'importance vitale de disposer d'une cartographie à jour de leur système d'information,	
Estime, toutefois, que la définition des modalités d'application de ces mesures devrait être confiée aux Etats membres et non à la Commission européenne, notamment en ce qui concerne : - la définition des circonstances dans lesquelles s'appliquerait l'obligation de notifier les incidents ; - la liste des secteurs d'importance critique,	
Juge également qu'il ne serait pas pertinent de prévoir : - la notification systématique des incidents par les autorités nationales à l'ensemble des Etats membres et à la Commission européenne, Demande au gouvernement de soutenir ces deux initiatives, et notamment de favoriser une adoption rapide de la proposition de directive, et d'œuvrer au sein du Conseil afin que ces recommandations soient prises en compte lors des négociations.	

EXAMEN EN COMMISSION

Lors de sa réunion du 27 mars 2013, la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat a entendu une communication de ***MM. Jacques Berthou et Jean-Marie Bockel, co-rapporteurs****.*

A l'issue de l'exposé des co-rapporteurs, un débat s'est engagé.

M. Jean-Louis Carrère, président. - Je remercie nos deux rapporteurs pour la qualité de leur travail.

Avec le rapport d'information présenté par notre ancien collègue M. Roger Romani en 2008, puis celui présenté par notre collègue Jean-Marie Bockel, et cette proposition de résolution consacrée à la stratégie européenne de cybersécurité, notre commission joue pleinement son rôle d'éclaireur sur un enjeu majeur pour notre défense et notre sécurité nationale et qui est appelé à prendre de plus en plus d'ampleur dans les années futures, compte tenu du développement d'Internet et de l'informatique dans tous les secteurs.

M. Michel Boutant. - Certains Etats sont soupçonnés d'être à l'origine d'attaques informatiques. On cite souvent la Chine et la Russie. Mais qu'en est-il de nos propres alliés ? Peut-on réellement faire confiance à nos alliés et partenaires et coopérer avec eux dans ce domaine, qu'il s'agisse de nos alliés au sein de l'OTAN ou même de nos partenaires européens ?

M. Jean-Marie Bockel, co-rapporteur. - Si les Etats que vous avez cités sont effectivement souvent soupçonnés d'être à l'origine de cyberattaques, ils ne sont pas les seuls, et de nombreux pays, y compris parmi nos alliés les plus proches, développent des capacités offensives. Pour dire les choses franchement, il n'y a pas de véritables alliés dans le cyberespace.

Dans le même temps, s'agissant d'une menace qui s'affranchit des frontières, une coopération à l'échelle européenne et internationale est indispensable et la France entretient une coopération étroite dans ce domaine, en particulier avec l'Allemagne et le Royaume-Uni.

M. Jacques Berthou, co-rapporteur. - Il est très difficile de déterminer précisément l'origine d'une attaque informatique car l'attaquant utilise généralement de nombreux ordinateurs compromis situés partout dans le monde, ce que les spécialistes désignent sous le nom de « réseaux zombies ».

Par ailleurs, les demandes d'entraide judiciaire internationale se heurtent souvent à des fins de non-recevoir de la part de certains pays. Le seul instrument international en matière de lutte contre la cybercriminalité, la convention de Budapest, conclue au sein du Conseil de l'Europe, n'a pas été signée par la Chine et la Russie, et elle n'a pas encore été ratifiée par l'ensemble de nos partenaires européens.

Au sein même de l'Union européenne, la directive sur les attaques contre les systèmes d'information n'a pas été encore adoptée définitivement et son contenu reste en deçà de la convention de Budapest, notamment en ce qui concerne l'harmonisation pénale, ce que l'on peut trouver regrettable et même paradoxal s'agissant d'un instrument communautaire.

Enfin, même si la communication de la Commission européenne prend soin d'éviter ce sujet, se pose la question de la transposition de la directive de 2006 sur la conservation des données, qui présente une grande importance en matière de lutte contre la cybercriminalité et les cyberattaques, et dont les lois de transposition ont été invalidées par plusieurs cours constitutionnelles de certains pays, comme l'Allemagne.

Sur proposition des co-rapporteurs, la commission a conclu à l'unanimité au dépôt de la proposition de résolution européenne.

* *
*

Réunie à nouveau le mercredi 10 avril 2013, la commission des affaires étrangères, de la défense et des forces armées a procédé à l'examen du présent rapport.

À l'issue de cet examen, la commission a adopté à l'unanimité le texte de la proposition de résolution.

ANNEXE I – LES 10 PRIORITÉS DU RAPPORT D'INFORMATION SUR LA CYBERDÉFENSE DE JUILLET 2012

Priorité n°1 : Faire de **la cyberdéfense** et de la **protection des systèmes d'information une priorité nationale**, portée **au plus haut niveau de l'Etat**, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. S'interroger sur la pertinence de formuler une **doctrine publique** sur **les capacités offensives** ;

Priorité n°2 : Renforcer **les effectifs, les moyens et les prérogatives** de **l'Agence nationale de sécurité des systèmes d'information**, ainsi que les effectifs et les moyens dédiés au sein **des armées, de la direction générale de l'armement et des services spécialisés**, et développer **une véritable politique des ressources humaines** ;

Priorité n°3 : Introduire des **modifications législatives** pour donner les moyens à l'ANSSI d'exercer ses missions et instituer **un pôle juridictionnel spécialisé à compétence nationale** pour réprimer les atteintes graves aux systèmes d'information ;

Priorité n°4 : Améliorer la prise en compte de **la protection des systèmes d'information dans l'action de chaque ministère**, en renforçant la sensibilisation à tous les niveaux, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse permettant de détecter les attaques, ainsi qu'en rehaussant l'autorité des fonctionnaires de sécurité des systèmes d'information ;

Priorité n°5 : Rendre **obligatoire** pour les entreprises et les opérateurs d'importance vitale **une déclaration d'incident** à l'ANSSI en cas d'attaque importante contre les systèmes d'information et encourager **les mesures de protection** par des mesures incitatives ;

Priorité n°6 : Renforcer la protection des systèmes d'information des **opérateurs d'importance vitale**, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse, en généralisant les audits, en rendant obligatoire la déclaration des processus et automates industriels connectés à Internet et en favorisant la mise en place, de manière sectorielle, de centres de détection communs ;

Priorité n°7 : Soutenir par **une politique industrielle volontariste**, à l'échelle nationale et européenne, le tissu industriel des entreprises françaises, notamment des PME, spécialisées dans la conception de certains **produits ou services importants pour la sécurité informatique** et, plus largement, du **secteur des technologies de l'information et de la communication**, et renforcer la coopération entre l'Etat et le secteur privé ;

Priorité n°8 : Encourager **la formation d'ingénieurs spécialisés** dans la protection des systèmes d'information, développer **la recherche** et les **activités de conseil**, et accentuer **la sensibilisation du public**, notamment au moyen d'une campagne de communication inspirée de la prévention routière ;

Priorité n°9 : Poursuivre **la coopération bilatérale** avec nos principaux alliés, soutenir l'action de **l'OTAN** et de **l'Union européenne**, engager **un dialogue** avec la Chine et la Russie et promouvoir l'adoption **au niveau international** de mesures de confiance ;

Priorité n°10 : Interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de **« routeurs » ou d'autres équipements de cœur de réseaux** qui présentent **un risque pour la sécurité nationale, en particulier les « routeurs » et certains équipements d'origine chinoise.**

ANNEXE II – LES RECOMMANDATIONS DU RAPPORT D'INFORMATION RELATIVES À L'ACTION DE L'UNION EUROPÉENNE EN MATIÈRE DE CYBERDÉFENSE

Recommandation n°39 : Promouvoir une véritable stratégie globale européenne en matière de protection des systèmes d'information au sein de l'Union européenne. Rendre l'action de l'UE plus « lisible ».

Recommandation n°40 : Réformer fondamentalement l'agence européenne ENISA afin d'en faire véritablement un outil de soutien réellement efficace aux Etats membres

Recommandation n°41 : Inciter l'Union européenne à assurer la protection de ses propres réseaux en renforçant le rôle du CERT des institutions de l'Union européenne, notamment auprès des organismes dépendants de l'Union européenne

Recommandation n°42 : Renforcer la coopération industrielle européenne en matière de conception de produits informatiques ou de sécurité informatique, et soutenir l'industrie européenne des technologies de l'information et de la communication afin d'en assurer la compétitivité et la pérennité, notamment grâce à des financements ou des mécanismes innovants (programme compétitivité et innovation par exemple) en priorité dans le domaine des télécommunications (routeurs et équipements cœur de réseau) mais également dans des domaines comme l'électronique (processeurs, PC), les systèmes d'exploitation ou les environnements sécurisés. Encourager la recherche au niveau européen par le biais du programme cadre de recherche et développement.

Recommandation n°43 : Développer le rôle de l'Union européenne en matière de normes juridiques afin de renforcer la protection des systèmes d'information des entreprises et des infrastructures critiques au niveau européen, notamment la protection des infrastructures critiques européennes et les infrastructures d'information (en posant notamment des garanties minimales à l'échelle européenne en matière de sécurité informatique).

Recommandation n°44 : Interdire sur le territoire national et européen le déploiement et l'utilisation de « routeurs » ou d'équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les « routeurs » ou d'autres équipements informatiques d'origine chinoise