N° 458

SÉNAT

SESSION ORDINAIRE DE 2012-2013

Enregistré à la Présidence du Sénat le 27 mars 2013

PROPOSITION DE RÉSOLUTION EUROPÉENNE

présentée, en application de l'article 73 quinquies *du règlement, au nom de la commission des affaires étrangères, de la défense et des forces armées, 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 (E8076), dont cette commission s'est saisie, 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

(Envoyée à la commission des affaires étrangères, de la défense et des forces armées.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Avec le développement d'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 la fraude bancaire 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 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 ver 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 informatiques 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 d'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. Plus de 50 milliards d'objets devraient être connectés !

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 les 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 notre 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 de la Commission européenne, 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. LA STRATEGIE EUROPEENNE DE CYBERSECURITE

La communication contient **quatre grands axes** de renforcement de l'action de l'Union européenne : la lutte contre la cybercriminalité, la cyberésilience, la cyberdéfense et l'action internationale de l'Union.

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 du renforcement de la coopération européenne ;

- l'importance des relations avec le secteur privé et 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 ;

- l'importance de la formation et de la sensibilisation.

Au total, **on peut saluer cette stratégie européenne 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 ».

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.

Notre rapport 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 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 l'élaboration de normes dans ce domaine, 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'assurances.

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.

Le rapport d'information recommandait donc de mettre l'accent sur la formation et 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**.

II. 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, 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.

Le **deuxième volet** porte sur l'instauration de **l'obligation,** pour plusieurs secteurs d'importance critique, **de notifier les incidents informatiques significatifs à l'autorité nationale de cybersécurité** ;

Le **troisième 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 ;

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

Que faut-il penser de cette proposition de directive ?

D'une manière générale, **on peut approuver ses principales dispositions.**

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, 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 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, par crainte que cela nuise à leur image, à leur réputation, voire même que cela n'entraine 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 au transport de l'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, 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 de notifier systématiquement les incidents informatiques, non seulement à l'autorité nationale, mais aussi 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.

Sous ces deux réserves, la commission des Affaires étrangère, de la Défense et des Forces armées du Sénat approuve la proposition de directive présentée par la Commission européenne, et, afin que le Sénat fasse connaître sa position au gouvernement sur ce sujet, a conclu au dépôt de **la proposition de résolution** qui suit :

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 ;

- l'importance des actions de sensibilisation et de 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 :

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.