1°) Que pensez-vous de la nouvelle stratégie et de la nouvelle directive de l'Union européenne ? En quoi ces documents peuvent-ils changer/accélérer les choses ?

Jean-Marie BOCKEL : D'une manière générale, on peut saluer cette stratégie européenne, qui témoigne d'une véritable prise de conscience de la part des institutions européennes de l'importance des enjeux de cybersécurité. Je pense notamment à l'accent mis sur la lutte contre la cybercriminalité, sur la cyberésilience et la cyberdéfense, sur les aspects industriels, sur la recherche, la formation et la sensibilisation ou encore concernant le rôle international de l'Union européenne.

Dans notre proposition de résolution, nous recommandons 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.

Nous portons également un regard très positif sur la proposition de directive sur la sécurité des réseaux et des systèmes d'information. 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.

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.

De ce point de vue, la stratégie européenne et la proposition de directive constitueront donc un progrès et permettront d'accélérer la prise de conscience des enjeux liés à la cyberdéfense au niveau européen.

2°) Quelles sont les mesures concrètes que vous soutenez particulièrement ?

La proposition de directive sur la sécurité des réseaux et des systèmes d'information 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 s'agit là d'un aspect essentiel et qui représentera un progrès car de nombreux Etats membres ne sont pas encore suffisamment sensibilisés à la menace représentée par les attaques contre les systèmes d'information et de communication.

- 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, avec notamment la création d'un réseau européen des autorités nationales de cybersécurité et l'obligation pour ces autorités d'alerter le réseau en cas d'incidents informatiques majeurs.

L'une des principales avancées, qui figurait d'ailleurs dans mon rapport, est selon moi la création 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.

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, voire même que cela n'entraîne une diminution du cours de leur action en bourse. 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, constitue donc pour moi une avancée importante, y compris pour notre pays.

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 distribution de l'électricité, aux transports ou encore aux banques.

Cette proposition de directive soulève cependant 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 me 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.

Dans notre proposition de résolution européenne, nous recommandons donc au gouvernement d'œuvrer au sein du Conseil en vue d'une adoption rapide de cette directive, tout en tenant compte de ces deux réserves dans les négociations avec nos partenaires européens.

3°) Cette nouvelle stratégie européenne et ces textes juridiques vous semblent-ils suffisants ou l'UE doit-elle être plus ambitieuse sur certains points ?

La proposition de directive prévoit plusieurs mesures pour renforcer la protection et la défense des systèmes d'information des administrations et des secteurs d'importance vitale, comme l'énergie, les transports ou la santé.

On pourrait aller encore 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 et 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.

Ainsi, nous recommandons d'inclure ces différents aspects dans le texte de la directive européenne.

Par ailleurs, l'Europe devrait être plus ambitieuse sur les aspects industriels, qui revêtent une importance majeure.

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 et nos emplois, notamment face au risque d'espionnage informatique.

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.

Dans mon rapport, je plaidais 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.

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.

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.

Mais encore, l'Union européenne pourrait s'impliquer sur de nombreux autres aspects de la cybersécurité. Outre les aspects industriels, il y a aussi tout ce qui relève de la lutte contre la cybercriminalité, à l'image de la pédopornographie sur Internet ou la fraude bancaire, qui sont en plein essor, puisque la cybercriminalité ferait plus d'un million de victimes chaque jour dans le monde, d'après la Commission européenne.

Je pense également à la prise en compte de la cybersécurité dans les relations extérieures de l'Union européenne, qui mériterait d'être renforcée, notamment dans les relations commerciales de l'Union européenne avec de grands partenaires, comme la Chine ou la Russie. Il est urgent d'agir car sinon cela risque d'être trop tard.

Source : SENAT

Télécharger la proposition de résolution