Protection des infrastructures d'information critiques: réalisations et prochaines étapes: vers une cybersécurité mondiale

2011/2284(INI) - 16/05/2012 - Rapport déposé de la commission, lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport d'initiative d'Ivailo KALFIN (S&D, BG) sur la protection des infrastructures d'information critiques - Réalisations et prochaines étapes: vers une cybersécurité mondiale.

Les députés rappellent que l'internet et les technologies de l'information et de la communication (TIC) sont des moteurs essentiels d'interaction sociale, d'enrichissement culturel et de croissance économique. Un niveau adéquat de sécurité de l'information est toutefois essentiel pour une forte expansion des services basés sur l'internet. C'est la raison pour laquelle les députés proposent un projet de résolution proposant un cadre de protection à trois niveaux, national, européen et international, qui se décline comme suit :

1) Mesures de renforcement de la PIIC au niveau national et européen : les députés saluent la mise en œuvre, par les États membres, du programme européen de protection des infrastructures d'information critiques qui comprend notamment la mise en place du réseau d'alerte concernant les infrastructures critiques (CIWIN). Ce programme permettra non seulement d'améliorer la sécurité générale des citoyens, mais renforcera le sentiment de sécurité et la confiance dans les mesures prises.

Ils demandent toutefois le renforcement des mesures existantes, via :

- l'extension du champ d'application de la directive 2008/114/CE du Conseil en vue d'y inclure le secteur des TIC et les services financiers mais aussi le domaine de la santé, les systèmes d'approvisionnement en eau et en nourriture, la recherche et l'industrie nucléaires ;
- le renforcement de l'excellence européenne dans le domaine de la protection des infrastructures d'information critiques ;
- la mise à jour des normes minimales de résilience des infrastructures d'information critiques contre toute perturbation, incident ou tentatives de destruction ou d'attaque ;
- le renforcement de la coopération entre les acteurs publics et privés au niveau de l'Union en vue de développer et de mettre en œuvre des normes de sécurité et de résilience pour les infrastructures d'information critiques civiles nationales et européennes ;
- la multiplication des exercices paneuropéens de préparation aux incidents de grande envergure.

Parallèlement, les députés invitent la Commission, en coopération avec les États membres à : i) évaluer la mise en œuvre du plan d'action pour la PIIC ; ii) établir des stratégies nationales de cybersécurité ; iii) **organiser des simulations d'incidents informatiques nationales et paneuropéennes**, iv) **développer des plans d'intervention nationaux en cas d'incident informatique** et contribuer au développement d'un **plan d'intervention européen en cas d'incident informatique d'ici à la fin 2012**. Ils demandent en particulier la mise en place de plans de sûreté pour les exploitants ou de mesures équivalentes pour toutes les infrastructures d'information critiques européennes, ainsi que la désignation de correspondants pour la sécurité dans les États membres.

2) Autres activités de l'Union pour une sécurité de l'internet forte : estimant que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pouvait jouer un rôle clé, au niveau européen, dans la protection des infrastructures d'information critiques, les députés invitent cette agence à

coordonner et à mettre en œuvre annuellement les "**mois européens de la sensibilisation à la cybersécurité**" afin d'attirer particulièrement l'attention des États membres et des citoyens européens sur ce type de problème. Soutenant globalement les activités menées par cette agence, les députés invitent également l'ENISA à consulter les acteurs concernés afin de définir des mesures en matière de cybersécurité pour les propriétaires et gestionnaires de réseaux ainsi qu'à aider la Commission et les États membres à contribuer au développement et à l'adoption de régimes de certification de la sécurité de l'information, de normes de comportement et de pratiques de coopération entre les CERT (équipes d'intervention en cas d'urgence informatique) nationales et européennes et les propriétaires et gestionnaires d'infrastructures, si nécessaire, grâce à la **formulation d'exigences communes minimales neutres** sur le plan technologique.

L'ENISA est également appelée à :

- gérer de nouvelles tâches d'exécution au niveau de l'UE, en coopération avec ses homologues américains, en matière de prévention et de détection des incidents de sécurité des réseaux et de l'information (en particulier, dans le cadre de la révision du règlement instituant l'ENISA) ;
- obtenir de nouvelles responsabilités en matière de réaction aux attaques sur l'internet ;
- maintenir les exercices qu'elle a menés en 2010 et en 2011, à son ordre du jour et y associer progressivement les opérateurs privés.

Pour contrer toute attaque des infrastructures informatiques critiques, les députés proposent que les États membres mettent en place **des plans d'intervention nationaux** en matière d'incidents informatiques incluant des dispositions sur l'assistance, l'endiguement et la réparation en cas de perturbations ou d'attaques informatiques de portée régionale, nationale ou transnationale. Ils devraient en outre coordonner leurs actions entre eux et rendre leurs actions plus cohérentes.

Au plan européen, la Commission est également appelée à :

- prévoir **un plan d'urgence européen en cas d'incident informatique** incluant des mesures contraignantes en matière de coordination, au niveau de l'Union, des fonctions techniques et de pilotage des CERT nationales et gouvernementales ;
- prendre, avec les États membres, les mesures nécessaires pour protéger les infrastructures critiques contre les cyberattaques et prévoir des mécanismes pour bloquer hermétiquement l'accès à une infrastructure dès qu'une cyberattaque se profile ;
- proposer des mesures contraignantes visant à imposer des **normes minimales de sécurité et de résilience** et améliorer la coordination entre les **équipes nationales d'intervention d'urgence** en matière de sécurité informatique.

En ce qui concerne les CERT, les députés demandent que celles-ci soient fonctionnelles, dotées de capacités minimales de sécurité et de résilience basées sur les bonnes pratiques reconnues. Ils demandent en outre l'établissement **d'un service de PIIC 24 heures sur 24 et 7 jours sur 7** pour chaque État membre, ainsi que la création d'un **protocole européen commun d'urgence** applicable à tous les points de contacts nationaux.

Pour une approche commune : dans le cadre de l'approche européenne de réaction, les députés invitent la Commission à proposer une procédure conjointe de définition et de désignation d'une approche commune permettant de répondre aux menaces informatiques transfrontalières. Ils saluent dès lors l'initiative de la Commission relative à l'élaboration d'un **système européen de partage d'informations et d'alerte d'ici 2013**.

Les députés saluent le travail de consultation effectué par la Commission pour renforcer le dialogue avec les fournisseurs de services informatiques. Ils suggèrent maintenant à la Commission de lancer une **initiative publique paneuropéenne en matière d'éducation**, axée sur l'éducation et la sensibilisation des

utilisateurs finaux, privés et commerciaux, et sur les menaces potentielles sur l'internet et les appareils TIC fixes et mobiles à chaque niveau de la chaîne d'utilisation. Ils soutiennent également la création d'un programme de cours européen destiné aux experts universitaires dans le domaine de la sécurité de l'information.

Pour une stratégie européenne de cybersécurité : les députés invitent la Commission à proposer d'ici la fin 2012 une **stratégie détaillée en matière de sécurité de l'internet pour l'Union**, reposant sur une terminologie claire ayant pour objectif la création d'un cyberespace (soutenu par une infrastructure sûre et résiliente et des normes ouvertes) propice à l'innovation et à la prospérité par la libre transmission d'informations, tout en assurant une **protection forte de la vie privée et d'autres libertés civiles**. Cette stratégie devrait détailler les principes, les objectifs, les méthodes, les instruments et les politiques (internes et externes) nécessaires à la rationalisation des efforts nationaux et européens, et établir des normes minimales de résilience dans les États membres. La stratégie devrait en outre prendre comme point de référence principal les travaux réalisés dans le domaine de la protection des infrastructures d'information critiques et prévoir tant des mesures volontaristes, telles que l'introduction de normes minimales pour les mesures de sécurité que des mesures réactives, telles que des **sanctions pénales, civiles et administratives**. Les députés demandent également que la Commission présente une **proposition législative punissant davantage les cyberattaques** (harponnage, fraude en ligne, etc.).

En ce qui concerne **la coordination des mesures nationales**, les députés demandent que le mécanisme de coordination soit doté d'experts et de ressources administratives et financières suffisantes.

Ils demandent également :

- la mise en place par la Commission d’un cadre européen pour la notification des violations de la sécurité dans les secteurs critiques, notamment les secteurs de l'énergie, des transports, de l'approvisionnement en eau et en nourriture mais aussi pour les TIC et les services financiers ;
- la disponibilité de données statistiquement représentatives concernant les coûts des attaques informatiques dans l'Union, les États membres et l'industrie ;
- des mesures destinées à éviter d'entraver la croissance de l'économie européenne sur l'internet et la prévision d’incitants pour exploiter pleinement le potentiel des partenariats entre les entreprises et entre secteurs public et privé dans ce domaine.

3) Coopération internationale : les députés rappellent que la coopération internationale est l'instrument principal pour l'introduction de mesures efficaces en matière de cybersécurité. Or, à l'heure actuelle, l'Union européenne n'est pas engagée activement dans les processus de coopération internationale et dans les dialogues relatifs à la cybersécurité. Les députés appellent dès lors la Commission et le service européen pour l'action extérieure (SEAE) à entamer un dialogue constructif avec les pays dont les opinions convergent afin de développer une interprétation uniforme et des politiques visant à renforcer la résilience de l'internet et des infrastructures critiques.

Les députés demandent également :

- l’inclusion des problèmes de sécurité de l'internet dans ses relations extérieures, y compris dans les accords avec les pays tiers ;
- la coordination des actions menées par les États membres et l’UE avec les diverses institutions, organes et agences internationales afin d’éviter les doubles emplois.

Saluant la création, lors du sommet UE-États-Unis, du groupe conjoint sur la cybersécurité et la cybercriminalité ainsi que d'un programme commun et d'une feuille de route en vue d'organiser des exercices transcontinentaux communs ou synchronisés dans le domaine de la cybersécurité en 2012/2013,

les députés appellent à un **dialogue structuré entre les législateurs européens et américains** afin de discuter des problèmes liés à l'internet dans le cadre de la recherche d'une compréhension et d'une interprétation uniformes et de positions communes.

Ils invitent enfin le SEAE, la Commission et l'ENISA à défendre une position active dans les forums internationaux pertinents, notamment en coordonnant les positions des États membres afin de promouvoir les valeurs, les politiques et les objectifs essentiels de l'Union européenne en matière de sécurité et de résilience de l'internet au sein d'agences comme l'OTAN, l'ONU, la Société pour l'attribution des noms de domaine sur internet, l'OSCE, l'OCDE,…