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

2011/2284(INI) - 31/03/2011 - Document de base non législatif

OBJECTIF : présenter un 1er bilan du plan d'action sur la protection des infrastructures d'information critiques et proposer un cadre d'action renouvelé pour les années à venir dans ce domaine.

CONTEXTE : la Commission a publié, le 30 mars 2009, une communication relative à la protection des infrastructures d'information critiques exposant un plan d'action (le plan d'action PIIC) destiné à renforcer la sécurité et la résilience des infrastructures essentielles des technologies de l'information et des communications (TIC). Cette communication avait pour objectif de stimuler et de soutenir la mise en place, au niveau européen comme au niveau national, d'un plan de préparation, de mesures de sécurité et d'une capacité de résilience d'un niveau élevé. Ce plan d'action s'articulait autour des 5 axes suivants: la préparation et la prévention, la détection et la réaction, l'atténuation et la récupération, la coopération internationale et les critères concernant les infrastructures critiques européennes dans le secteur des TIC.

Parallèlement, la stratégie numérique pour l'Europe, adoptée en mai 2010, insiste sur la nécessité, pour toutes les parties prenantes, d'unir leurs forces dans un effort global pour renforcer la sécurité et la résilience des infrastructures TIC en centrant leur action sur la prévention, la préparation et la sensibilisation et de mettre en place des mécanismes efficaces et coordonnés propres à répondre à de nouvelles formes de cyberattaques et de cybercriminalité de plus en plus perfectionnées.

Pour compléter ce texte, la Commission a présenté en parallèle une proposition relative à un nouveau mandat visant à renforcer et à moderniser l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) afin d'accroître la confiance et améliorer la sécurité des réseaux, mais aussi prévenir, détecter et combattre les problèmes de cybersécurité.

La présente communication récapitule les résultats obtenus depuis l'adoption du plan d'action PIIC en 2009 et décrit les prochaines étapes prévues pour chaque action, au niveau européen comme au niveau international. Elle s'intéresse également à la dimension mondiale des problèmes posés et à l'importance d'un renforcement de la coopération entre les États membres et le secteur privé aux niveaux national, européen et international, de manière à résoudre les questions d'interdépendance sur le plan mondial.

CONTENU : la communication identifie tout d'abord les risques potentiels qui peuvent atteindre gravement la sécurité des grands réseaux informatiques :

1. **des risques d'exploitation**, comme dans le cas des «menaces persistantes avancées» à des fins d'espionnage économique et politique (GhostNet, par exemple), ou le vol d'identité,…
2. **des risques de perturbation**, comme les attaques par déni de service distribué ou le pollupostage par l'intermédiaire de réseaux zombies (tels que le réseau Conficker qui compte 7 millions de machines) ;
3. **des risques de destruction** non encore réellement identifiés à ce jour mais à prendre en compte.

Pour contrer ces risques, la Commission a mis en œuvre pas mal d'actions dont les points saillants peuvent se résumer comme suit :

1) Préparation et prévention :

- création d'un Forum où les États membres peuvent échanger des bonnes pratiques dans le domaine des infrastructures d'information critiques ;
- création d'un partenariat public-privé européen pour la résilience (EP3R) en vue d'encourager la coopération public/privé sur des questions stratégiques de politique de l'UE en matière de sécurité et de résilience ;
- création d'un réseau de CERT rassemblant tous les États membres d'ici à 2012 qui servira de pierre angulaire à un futur système européen de partage d'informations et d'alerte (SEPIA) pour les particuliers et les PME.

2) Détection et réaction : l'ENISA a établi une feuille de route à haut niveau pour promouvoir le développement, d'ici à 2013, d'un système européen de partage d'informations et d'alerte (SEPIA).

3) Atténuation et récupération : jusqu'à présent, seuls 12 États membres ont organisé des exercices portant sur la réaction en cas d'incident de grande envergure affectant la sécurité des réseaux et sur la récupération après défaillance grave. Le 1er exercice paneuropéen portant sur des incidents de grande envergure affectant la sécurité des réseaux (Cyber Europe 2010) a eu lieu le 4 novembre 2010 avec la participation de tous les États membres et de la Suisse, la Norvège et l'Islande. L'objectif est maintenant de créer des exercices paneuropéens disposant d'un cadre commun.

4) Coopération internationale : la Commission va examiner les principes existants et les promouvoir auprès des principaux intéressés, notamment le secteur privé (par l'intermédiaire de l'EP3R), dans un cadre bilatéral avec des partenaires internationaux majeurs, notamment les États-Unis, ainsi que dans un cadre multilatéral. Elle mènera ces activités, dans la limite de ses compétences, dans des enceintes telles que le G8, l'OCDE, l'OTAN, etc.

5) Critères pour les infrastructures critiques européennes dans le secteur des TIC : les discussions techniques au sein du Forum européen des États membres ont débouché sur une première version des critères spécifiques au secteur des TIC pour recenser les infrastructures européennes critiques, portant plus particulièrement sur les communications fixes et mobiles et l'internet. La Commission examinera aussi avec les États membres les éléments spécifiques au secteur des TIC à prendre en considération pour le réexamen de la directive concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection en 2012.

Prochaines étapes : face aux défis qui se posent au niveau mondial, la Commission compte :

- **promouvoir des principes pour la résilience et la stabilité de l'internet**. Il convient d'établir, en concertation avec d'autres pays, des organisations internationales et, le cas échéant, des organismes privés d'envergure mondiale, des principes internationaux pour la résilience et la stabilité de l' internet. Ces principes devraient constituer le cadre dans lequel devraient s'inscrire les activités de toutes les parties prenantes en matière de stabilité et de résilience de l'internet ;
- constituer des partenariats stratégiques de dimension internationale. Il convient de tirer parti des efforts entrepris dans des domaines critiques, tels que la **gestion des incidents informatiques**, pour créer des partenariats stratégiques, avec notamment des exercices et des mesures de coopération avec le CERT. La création d'un groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité, constitue un grand pas dans cette direction. Les travaux de ce groupe porteront sur la gestion des incidents informatiques, les partenariats public-privé, la sensibilisation et la criminalité informatique. En Europe, le principal facteur de succès sera une bonne coordination entre toutes les institutions de l'UE, les organismes concernés (notamment l'ENISA et Europol) et les États membres;
- renforcer la **confiance dans l'informatique en nuage** car cette technologie est essentielle pour qu' il soit possible d'exploiter pleinement les avantages de cette technologie.

Les États membres sont également appelés à :

- améliorer l'état de préparation de l'UE en mettant en place un réseau de CERT nationales /gouvernementales opérationnelles d'ici à 2012. Ces activités permettront de promouvoir la mise en place d'un système européen de partage d'informations et d'alerte (SEPIA) pour le grand public d'ici à 2013;
- **établir un plan d'urgence européen en cas d'incident informatique d'ici à 2012** et organiser des exercices paneuropéens réguliers dans le domaine de la cybersécurité. Les futurs exercices paneuropéens devraient être lancés sur la base d'un plan d'urgence européen en cas d'incident qui soit fondé sur les plans d'urgence nationaux et fonctionne en interaction avec eux. Ce plan devrait fournir les mécanismes et procédures de base pour la communication entre États membres ainsi qu' un appui pour définir l'envergure des futurs exercices paneuropéens et les organiser. L'ENISA collaborera avec les États membres afin que ce plan d'urgence européen en cas d'incident informatique soit établi d'ici à 2012 ;
- déployer des efforts coordonnés au niveau européen dans le cadre de forums internationaux et amorcer des dialogues sur **l'amélioration de la sécurité et de la résilience de l'internet**. Les États membres devaient coopérer entre eux et avec la Commission pour promouvoir l'adoption d'une approche fondée sur des principes ou des normes, applicable à la stabilité et à la résilience mondiales de l'internet.

Á noter qu'une annexe à la communication présente un état des lieux précis de toutes les actions menées dans le cadre du Plan d'action PIIC ainsi que des prochaines étapes dans le cadre de ce dernier.