

Doc. 11333
27 juin 2007

Comment prévenir la cybercriminalité dirigée contre les institutions publiques des Etats membres et observateurs ?

Avis¹

Commission des questions économiques et du développement

Rapporteur : M^{me} Anna LILLIEHÖÖK, Suède, Groupe du Parti populaire européen (PPE/DC)

A. Conclusions de la commission

La Commission des questions économiques et du développement apprécie l'occasion qui lui est donnée de contribuer à un débat tout à fait important et d'actualité sur la cybercriminalité. Elle partage pleinement les préoccupations de la Commission des questions juridiques et des droits de l'homme qui souligne la vulnérabilité de la société moderne face à la cybercriminalité qui est une menace pour la démocratie, les droits de l'homme et l'Etat de droit.

La Commission des questions économiques est convaincue que la cybercriminalité risque de mettre à mal les institutions de l'Etat tout comme elle peut porter atteinte au tissu socio-économique de la société. Les organismes publics et privés se trouvent devant une même nécessité, celle de renforcer la sécurité du réseau et la protection de l'infrastructure vitale. Ils doivent travailler ensemble plus activement afin de développer une coopération trans-sectorielle internationale, sur la base de partenariats entre les secteurs public et privé.

B. Amendement proposé au projet de résolution

Après l'alinéa 14.5., insérer le nouvel alinéa suivant :

« associer plus étroitement le secteur privé, notamment en instaurant des partenariats entre les secteurs public et privé en vue d'une coopération trans-sectorielle internationale plus efficace contre la cybercriminalité. »

C. Exposé des motifs par M^{me} Lilliehöök, rapporteur

Ces dernières décennies, le développement des technologies de l'information est allé de pair avec l'ouverture croissante des Etats à la libre circulation des capitaux, des biens, des personnes et des idées mais il a aussi rendu ces Etats plus vulnérables aux nouveaux problèmes mondiaux. Nos sociétés ont développé des applications informatiques complexes dans une course à la recherche d'instruments toujours plus rapides, moins coûteux et plus accessibles, sans prendre le temps de réfléchir à l'instauration des garanties nécessaires pour protéger la stabilité des réseaux et systèmes numériques. La cybercriminalité a ramené les gouvernements aux réalités en rappelant que les criminels aussi sont prompts à exploiter les nouvelles possibilités qu'offre le cyberspace où, jusqu'à une date encore récente, presque tout était permis et tout était possible.

¹ Voir le rapport présenté par la Commission des questions juridiques et des droits de l'homme (Doc. 11325).

Aujourd'hui, la Convention sur la cybercriminalité du Conseil de l'Europe est l'unique instrument international contraignant sur la cybercriminalité qui ait été approuvé non seulement par des Etats membres, mais aussi par des Etats non européens. C'est un traité ouvert, très détaillé et ambitieux qui mérite notre soutien inconditionnel et une mise en œuvre sans délai. Nous espérons que le débat de l'Assemblée sur la cybercriminalité créera la dynamique nécessaire pour accélérer l'adhésion des Etats européens et autres à cette convention afin qu'elle réalise ses pleins effets.

Nous aimerions souligner dans ce contexte certains points essentiels des conclusions des experts en cybercriminalité, représentant les secteurs public et privé, lesquels se sont réunis à Strasbourg les 11 et 12 juin 2007 pour analyser les tendances de la cybercriminalité et proposer quelques mesures concrètes nécessaires pour déjouer les nouvelles menaces. Il apparaît ainsi que :

- Les logiciels pernicioux (vicious software) évoluent rapidement et sont de plus en plus utilisés pour perpétrer des délits économiques ;
- Les cyberdélinquants tendent à s'organiser pour des délits visant à générer des profits illicites et les entreprises criminelles engendrent le développement plus avant de l'économie souterraine ;
- Aux cyberattaques irrationnelles se substituent aujourd'hui des attaques plus ciblées visant des usagers spécifiques (particuliers, groupes, organisations, entreprises, secteurs, etc.) notamment à des fins économiques criminelles ;
- Le risque de cyberattaques contre des infrastructures vitales est de mieux en mieux perçu ;
- La nouvelle génération de cybertechnologies place les services de répression en face de nouveaux défis.

A l'évidence, les secteurs privés et publics exigent tous deux de hauts niveaux de cybersécurité. Leurs moyens et leurs approches peuvent différer, mais se complètent dans une large mesure. Face à la menace de cybercriminalité et d'attaques contre l'Internet, les mesures à prendre doivent être véritablement mondiales et transsectorielles, aussi la mise en œuvre à vaste échelle et sans tarder de la Convention sur la cybercriminalité serait-elle un pas déterminant dans la bonne direction.

Une autre étape consistera à resserrer l'interaction entre les institutions publiques et privées en encourageant la coopération mondiale afin de concevoir des mesures réglementaires et techniques innovantes pour renforcer la protection des cyberréseaux et des infrastructures vitales fondamentales. Ayant lancé la Convention sur la cybercriminalité, son mécanisme de suivi et l'activité de développement des compétences des services répressifs, le Conseil de l'Europe est un cadre très utile pour le dialogue, l'échange d'informations, la coordination transfrontalière de l'action et des mesures législatives, l'organisation d'ateliers de formation et la mise en place de partenariats publics-privés pour enrayer la cybercriminalité.

Le cyberspace est resserré et interactif : toute action répréhensible peut avoir un effet retour sur les délinquants qui finissent par être eux-mêmes victimes de réseaux numériques échappant à leur contrôle. Nous souhaitons par conséquent mettre en garde contre toute indulgence, défaut de vigilance ou absence de mesures pour juguler le risque de cyberattaques malveillantes pour des raisons politiques, économiques ou autres. Enfin, lorsque nous demandons instamment aux Etats membres de ratifier la Convention sur la cybercriminalité, nous nous adressons plus particulièrement aux Etats dotés des technologies de pointe et d'expertise où nous avons observé les plus grands risques de développement de nouvelles technologies malveillantes.

* * *

Commission chargée du rapport : Commission des questions juridiques et des droits de l'homme

Commission saisie pour avis : Commission des questions économiques et du développement

Renvoi en commission : Demande de débat d'urgence, renvoi n°3365 du 25 juin 2007

Projet d'avis approuvé par la commission des questions économiques et du développement le 26 juin 2007