Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 05/12/2013

Le Conseil a fait **le point des travaux** sur un projet de directive qui vise à assurer un niveau commun élevé de sécurité des réseaux de communication dans toute l'UE.

Les délégations reconnaissent qu'il faut prendre des mesures pour lutter contre les cyberattaques, mais **divergent quant au meilleur moyen d'assurer la sécurité des réseaux** dans toute l'UE :

- certaines délégations sont favorables à une **approche souple**, avec des règles contraignantes au niveau de l'UE limitées aux infrastructures critiques et aux exigences de base et complétées par des mesures facultatives et volontaires ;
- d'autres délégations ainsi que la Commission estiment que seules des **mesures juridiquement contraignantes** permettraient d'atteindre les niveaux de sécurité nécessaires à l'échelle de l'UE.

En ce qui concerne les **modalités pratiques**, de nouvelles discussions sont nécessaires sur plusieurs questions :

Stratégie et organisme compétent en matière de sécurité des réseaux (**SRI**) : toute perturbation importante survenant dans un État membre étant susceptible d'avoir des répercussions dans d'autres États membres, les délégations sont en mesure de soutenir le principe d'une entité de coordination au niveau national.

Toutefois, les États membres ayant déjà adopté des stratégies en matière de SRI portent un regard critique sur le chapitre II de la proposition, consacré aux **cadres nationaux des réseaux de l'information** : ces États souhaitent s'assurer que les exigences auxquelles les États membres devront satisfaire seront compatibles avec la pratique nationale en vigueur et n'iront pas au-delà.

Certaines délégations souhaitent obtenir des éclaircissements sur les termes «risques» ou «menaces» et se demandent à quoi correspondent exactement ces exigences et si elles devraient ne concerner que le secteur privé ou bien également le secteur public.

Autorité compétente et description de ses tâches : de nombreuses questions doivent encore être précisées, comme par exemple celle de savoir si l'autorité doit assumer des tâches opérationnelles, ce à quoi de nombreux États membres sont opposés, de même que la question de la répartition des responsabilités avec les équipes d'intervention en cas d'urgence informatique (CERT) nationales.

Gestion des risques et notification d'incidents : de nombreuses délégations ont demandé :

- si, outre les «opérateurs d'infrastructures critiques», la proposition devrait également couvrir les fournisseurs de services de la société de l'information ;
- que les États membres puissent déterminer avec plus de souplesse les secteurs qui constituent des infrastructures critiques nationales. Certaines délégations souhaitent limiter les exigences proposées au seul secteur privé ; d'autres demandent que les exigences relatives à la notification en cas d'atteinte à la sécurité soient volontaires ;
- dans quelle mesure les États membres pourraient en fait «garantir» que les parties sécurisent leurs réseaux et notifient les incidents.

Des préoccupations ont également été exprimées sur les conséquences que les notifications peuvent avoir sur la vie privée et la confidentialité de l'information.

Réseau de coopération : les discussions doivent se poursuivre sur les tâches du réseau de coopération, bien que de nombreuses délégations estiment qu'il ne devrait pas assumer de tâches opérationnelles.

Un certain nombre de questions demandent à être précisées, comme par exemple :

- qui présidera le réseau de coopération, quels en seront les coûts et quelles seront les relations et la répartition des responsabilités dans le cadre de la coopération entre les CERTS nationales, l'ENISA et Europol ;
- la question du partage d'informations au sein du réseau, que devrait selon certaines délégations, s'effectuer sur une base volontaire ;
- la nécessité du «système sécurisé d'échange d'informations» proposé et dédié ;
- le mécanisme d'alerte rapide proposé, notamment la question de savoir quelles informations seront échangées et à quel moment, et quelles seront les conséquences éventuelles pour l'incident ou le risque ;
- la question du moment et des conditions dans lesquelles une intervention coordonnée est nécessaire.

Selon la présidence, le principal défi consistera à convenir d'une approche assurant **un juste équilibre entre les règles contraignantes au niveau de l'UE et des mesures facultatives et volontaires**, qui devront toutes conduire à des niveaux similaires de préparation en matière de SRI entre les États membres et permettre à l'UE de répondre de manière efficace aux défis en matière de SRI.