

FR

FR

FR



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le
SEC(2009) yyy

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

accompagnant la

**COMMUNICATION DE LA COMMISSION AU CONSEIL, AU PARLEMENT
EUROPÉEN, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU
COMITÉ DES RÉGIONS**

relative à la protection des infrastructures d'information critiques
*«Protéger l'Europe des cyberattaques et des perturbations de grande envergure:
améliorer l'état de préparation, la sécurité, et la résilience»*

RÉSUMÉ DE L'ANALYSE D'IMPACT

{COM(2009) }
{SEC(2009) }

RÉSUMÉ DE L'ANALYSE D'IMPACT

1. QUEL EST LE PROBLÈME?

Le secteur des TIC est essentiel pour la croissance économique et le développement sociétal de l'UE.

L'ensemble de l'économie et de la société de l'Union européenne repose désormais sur les technologies de l'information et des communications (TIC). **Le secteur des TIC est essentiel pour tous les segments de la société. Les entreprises comptent sur le secteur des TIC**, aussi bien en ce qui concerne directement l'activité de vente que pour ce qui touche à l'efficacité des processus internes. L'utilisation des TIC **se généralise également dans les secteurs public et administratif**: l'adoption des services d'administration en ligne à tous les niveaux garantit une meilleure efficacité des procédures mais accroît aussi la dépendance du secteur public à l'égard des TIC. Enfin, **les citoyens comptent de plus en plus sur les services de la société de l'information et leur utilisation des TIC dans la vie de tous les jours va croissant**: une perturbation des réseaux électroniques aurait donc une incidence négative sur ce type d'activités, et il ne faut en outre pas oublier que les données personnelles des citoyens sont de plus en plus souvent communiquées et transmises par voie électronique. Des mesures de sécurité insuffisantes pourraient causer la perte d'informations personnelles sensibles et être à l'origine d'un risque d'usurpation d'identité ou d'autres types de fraude.¹ **L'amélioration de la sécurité et de la résilience des infrastructures d'information critiques est aussi, par conséquent, absolument essentielle pour la protection des données personnelles des citoyens et pour assurer le respect de leur droit à la vie privée.**

Les systèmes et services de TIC sont, intrinsèquement, des infrastructures essentielles et ils constituent également la base d'autres infrastructures technologiques et sociétales d'importance critique. Cet état de fait a été reconnu par le livre vert sur un programme européen de protection des infrastructures critiques qui englobe dans la notion d'**infrastructures d'information critiques (IIC)** tous les systèmes d'information et de communication qui constituent intrinsèquement des infrastructures critiques ou qui sont essentiels au bon fonctionnement d'autres infrastructures critiques (télécommunications, matériels/logiciels informatiques, internet, satellites, etc.)², à l'instar de l'approche adoptée par l'OCDE³.

Au-delà des différences terminologiques existantes, **ce qui importe, c'est que la notion d'infrastructures d'information critiques conduise à une approche systémique des politiques destinées à assurer la sécurité et la continuité du fonctionnement des systèmes, services, réseaux et infrastructures de TIC** (ou, en bref, infrastructures TIC), dont **l'internet constitue un composant très important**, en raison de sa très large diffusion et du processus de convergence technologique.

¹ <http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece>

² COM(2005) 576 final

³ <http://www.oecd.org/dataoecd/1/12/40825492.pdf>

Quel est l'enjeu?

En raison de l'omniprésence des infrastructures d'information critiques, des perturbations des réseaux électroniques **pourraient avoir des répercussions sur l'ensemble de la société.**

Bien souvent, les risques dus aux attaques humaines, aux catastrophes naturelles ou aux défaillances techniques sont insuffisamment compris ou analysés. Par conséquent, le niveau de sensibilisation des intéressés n'est pas suffisant pour que des mesures de protection et des parades appropriées puissent être mises au point.

Les cyberattaques ont aujourd'hui atteint un degré de complexité sans précédent et elles sont souvent exécutées par des individus ou des groupes criminels à des fins lucratives ou pour des raisons politiques. **Les cyberattaques de grande envergure lancées contre l'Estonie, la Lituanie ou la Géorgie sont des exemples d'une tendance générale.** Le nombre très élevé de virus, de vers et d'autres types de logiciels malveillants, l'expansion des réseaux de machines zombies et l'augmentation continue du pourriel confirment la gravité du problème⁴. **Les infrastructures TIC font l'objet d'attaques en permanence** et si l'Europe ne se prépare pas, les conséquences de ces attaques seront très graves.

En raison de la dépendance élevée à l'égard des infrastructures d'information critiques, de l'interconnexion transfrontalière de ces dernières et de leur interdépendance vis-à-vis d'autres infrastructures, il faut, **pour envisager leur sécurité et leur résilience, adopter une approche systémique qui constituera une première ligne de défense** contre les défaillances et les attaques, en sus et en complément des mesures de prévention et de lutte contre les menées criminelles et terroristes visant les IIC et des procédures judiciaires qui s'y rapportent.

Nature du problème

Actuellement, **les questions de sécurité et de résilience des infrastructures d'information critiques sont essentiellement traitées au niveau national, et la coordination paneuropéenne est minime.** Le manque de coopération transfrontalière systématique **diminue considérablement l'efficacité des contre-mesures nationales.** En outre, **un faible niveau de sécurité et de résilience des infrastructures dans un pays pourrait accroître la vulnérabilité et les risques dans d'autres.**

Étant donné que les infrastructures d'information critiques ont une dimension planétaire et qu'elles sont étroitement interconnectées avec d'autres infrastructures, dont elles sont **interdépendantes**, il n'est pas possible de garantir leur sécurité et leur résilience en ayant recours à des **approches strictement nationales et non coordonnées.** En outre, **il est admis que le seul jeu des forces du marché n'incite pas suffisamment le secteur privé à investir dans la protection des infrastructures d'information critiques au niveau que demanderaient normalement les gouvernements.**

Les causes sous-jacentes du problème général exposé ci-dessus sont les suivantes:

- **Des approches disparates des politiques publiques en matière de sécurité et de résilience des IIC entre les États membres.** Il existe des différences entre les politiques des différents États membres pour ce qui est de la sécurité et de la résilience des IIC. En

⁴ COM(2006) 688 final

outre, le niveau de compétence et de préparation ne semble pas homogène, comme l'a souligné l'analyse des approches nationales exécutée par la Commission et confirmée par un rapport de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)⁵.

- **Des difficultés à adopter de nouveaux modèles de gouvernance d'envergure européenne.** L'amélioration de la sécurité et de la fiabilité des IIC pose des **problèmes particuliers en matière de gouvernance**. Les **gouvernements** sont **responsables** de la définition de leurs politiques dans le domaine des IIC, mais il est **essentiel d'obtenir la participation du secteur privé** pour garantir la **mise en œuvre** de ces politiques. On a vu apparaître, à l'échelon national, un modèle de référence qui a pris la forme de **partenariats public-privé (PPP)**. Cependant, même si tous s'accordent à reconnaître qu'il serait souhaitable que de tels PPP se constituent à l'échelon européen, concrètement, ce n'est pas encore le cas.
- **Une capacité européenne limitée en ce qui concerne l'alerte rapide et la réaction en cas d'incident.** Les consultations ont révélé des différences entre les systèmes nationaux d'alerte rapide et la réaction en cas d'incident. Dans certains États membres, la notification des incidents relatifs à la sécurité des réseaux ne fait pas partie des procédures de routine (même si cette pratique informelle existe entre opérateurs) et/ou il n'existe pas d'organisme de référence qui fasse office de centre de surveillance. La coopération et l'échange d'informations entre **organismes gouvernementaux** semblent **sous-développées** et elles sont compromises par le manque de mécanismes fiables en matière de partage et de coordination, lesquels sont **conditionnés par un bon fonctionnement de toutes les équipes d'intervention en cas d'urgence informatique (Computer Emergency Response Teams, CERT) nationales ou gouvernementales, c'est-à-dire par l'existence d'une base commune pour ce qui est des moyens**. En outre, **les exercices et simulations pratiques au niveau de l'UE**, éléments essentiels pour renforcer la sécurité et la résilience des infrastructures d'information critiques, se trouvent encore au **stade embryonnaire**.
- **La sensibilisation aux risques qui menacent la stabilité et la résilience de l'internet est faible.** L'internet, qui est par nature une infrastructure distribuée et redondante, s'est révélé jusqu'ici **plutôt solide et résilient**. Toutefois, il est légitime de **s'interroger** sur sa capacité de continuer à résister **au nombre croissant** de perturbations et de cyberattaques, au vu notamment de sa **croissance phénoménale**, de sa **complexité accrue** et de **l'apparition de nouveaux services**.

Aucun pays n'est complètement isolé. Du fait de la dimension planétaire des infrastructures d'information critiques, et plus particulièrement de l'internet, il convient d'adopter une **approche commune mondiale** en matière de sécurité et de résilience. **Seule une étroite coordination au niveau de l'UE permettra d'avoir une incidence directe au niveau international.**

2. QUELLE EST LA JUSTIFICATION D'UNE ACTION DE L'UE?

Il est possible que l'application d'approches purement nationales ne soit pas suffisante pour régler les problèmes exposés ci-dessus. Les incidences transfrontalières n'étant pas négligeables, de nombreuses menaces pour la sécurité des réseaux et de l'information sont des

⁵ http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

sources potentielles d'externalités négatives transfrontalières qui ne peuvent pas être traitées efficacement au niveau national et qui risquent de provoquer des perturbations dans d'autres pays.

Une approche visant à renforcer la sécurité et la résilience des IIC qui soit intégrée au niveau de l'UE représenterait un complément utile et un apport de valeur ajoutée européenne pour les programmes nationaux de protection des IIC ainsi que pour les systèmes de coopération existant entre les États membres. Étant donné qu'ils sont confrontés à de nombreux problèmes et difficultés identiques, une approche commune serait bénéfique pour tous.

Il ressort des débats qui ont eu lieu au lendemain des événements survenus en Estonie qu'il est possible de limiter les conséquences d'attaques de ce type en prenant des **mesures préventives** – telles que des échanges d'information plus structurés à l'échelon européen - et en **coordonnant les actions** au moment de la crise. La Commission, dans le total respect du **principe de subsidiarité**, est idéalement placée pour assurer la coordination de ces efforts, en coopération étroite avec les États membres et d'autres organisations internationales.

En outre, les préoccupations nationales dans le domaine de la sécurité, même si elles jouent un rôle non négligeable dans la définition des politiques et obligations dans le domaine de la sécurité des réseaux et de l'information, peuvent conduire à une fragmentation réglementaire et nuire à la compétitivité de l'Union européenne dans son ensemble, ainsi qu'à la capacité de création de richesse du marché unique européen.

En 2006, la Commission a annoncé⁶ son intention de mettre au point, dans le cadre du programme européen de protection des infrastructures critiques (EPCIP)⁷ une politique sectorielle pour les TIC destinée à *«améliorer la sécurité et la résilience des réseaux et des systèmes d'information»*. Cette annonce a été favorablement accueillie par le Conseil européen en 2007⁸.

Cette initiative prendrait dûment en considération la dimension internationale et se fonderait notamment sur des principes reconnus tels que ceux qui ont été affirmés par le G8 dans le domaine de la protection des infrastructures d'information critiques, sur la résolution 58/199 de l'Assemblée générale de l'ONU sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et sur la recommandation du conseil de l'OCDE sur la protection des infrastructures d'information critiques.

Enfin, il faut souligner que l'initiative proposée tient compte, sans faire double emploi, des activités de l'OTAN en ce qui concerne la sécurité des réseaux, qui sont plutôt axées sur les aspects militaires - à savoir la politique commune en matière de cyberdéfense et les activités de l'autorité de gestion de la cyberdéfense (CDMA) ainsi que des travaux du centre d'excellence pour la cyberdéfense (CCD-COE).

⁶ COM(2006)251.

⁷ COM(2006)786.

⁸ Résolution du Conseil 2007/C 68/01.

3. QUELS SONT LES OBJECTIFS?

L'objectif de cette initiative politique consiste à **améliorer le niveau de préparation et de réaction dans toute l'Europe** en ce qui concerne les risques et menaces décrits, en évitant une approche fragmentée menée individuellement par les États membres. Les actions porteraient essentiellement sur la définition de processus communs souples permettant de faire face aux menaces identifiées comme à celles qui sont encore inconnues. Les parties intéressées des secteurs public et privé s'emploieraient à garantir que des **mesures de prévention, de détection, d'action en cas d'urgence et de récupération** sont mises en place, **de manière adéquate et cohérente**, afin de parvenir à un **niveau de sécurité et de résilience approprié pour les infrastructures d'information critiques et de garantir la continuité des services**. L'amélioration de la sécurité et de la résilience aurait aussi une **incidence positive sur la protection des données personnelles et de la vie privée des citoyens de l'UE**.

L'objectif général de cette proposition, qui consiste à **renforcer la sécurité et la résilience des infrastructures d'information critiques pour constituer une première ligne de défense**, peut être atteint en menant des actions reposant sur les quatre axes suivants:

- (1) combler les lacunes existantes dans les politiques nationales en matière de sécurité et de résilience des IIC;
- (2) renforcer la gouvernance européenne en ce qui concerne la sécurité et la résilience des IIC;
- (3) renforcer la capacité européenne en ce qui concerne la réaction opérationnelle en cas d'incident;
- (4) améliorer la sécurité et la résilience de l'internet.

4. QUELLES SONT LES OPTIONS STRATEGIQUES?

Option stratégique 1: Statu quo

Il ne serait pas viable de ne pas proposer d'autre action. Sans action horizontale à l'échelon de l'UE, les États membres continueraient à agir individuellement ou dans un cadre bilatéral ou multilatéral restreint. Il y aurait donc un **risque lié à l'évolution des différentes approches nationales**, qui pourraient se révéler incompatibles. En outre, la coopération transfrontalière s'établirait en fonction des besoins et pourrait se montrer inefficace face à la complexité et à l'ampleur des cyberattaques.

Étant donné que les États membres continueraient à travailler sur ces problèmes à des rythmes différents, les parties intéressées **pourraient s'abstenir d'investir dans la sécurité et la résilience** car la multitude de normes et d'obligations diminuerait leur compétitivité. La nature transfrontalière du problème accentuerait les différences dans le domaine de la sécurité, de la résilience et de la préparation dans les différents pays d'Europe. La vulnérabilité des IIC en Europe resterait élevée et pourrait même s'accroître, malgré les efforts fournis individuellement.

Option stratégique 2: Cadre non contraignant

La Commission **fournirait un cadre de coordination et de coopération** qui prendrait la forme d'une communication et d'un plan d'action auxquels participeraient les États membres, le secteur privé et la société civile. La communication pourrait être approuvée par le Conseil de l'UE et le Parlement européen pourrait aussi décider de contribuer au débat.

L'initiative serait axée sur les objectifs mentionnés ci-dessus et elle proposerait plus particulièrement de:

(1) **promouvoir la cohérence entre les politiques nationales en matière de sécurité et de résilience des IIC en**

- identifiant des exemples de pratiques de politique publique qui peuvent servir de modèle et des points communs;
- établissant un forum européen permettant aux États membres d'échanger des informations et de bonnes pratiques politiques sur la sécurité et la résilience des IIC.

(2) **renforcer la gouvernance européenne en ce qui concerne la sécurité et la résilience des IIC en:**

- lançant un **Partenariat public privé européen pour la résilience (EP3R)** qui encouragera la coopération entre le secteur public et le secteur privé sur des objectifs liés à la sécurité et à la résilience, sur les exigences de base et sur l'adoption de bonnes mesures et pratiques politiques.

(3) **renforcer la capacité européenne en ce qui concerne la réaction opérationnelle en cas d'incident en:**

- établissant des CERT nationales ou gouvernementales⁹ en bon état de fonctionnement qui constitueront un élément clé de la capacité nationale en matière de préparation, de partage d'informations, de coordination et de réaction;
- trouvant un accord sur un niveau minimum de capacités et de services pour les équipes d'intervention en cas d'urgence informatique (CERT) nationales ou gouvernementales;
- encourageant la coopération européenne entre les CERT nationales/gouvernementales; en facilitant les contacts et la coopération entre les capacités nationales de réaction; en organisant des exercices paneuropéens et/ou régionaux sur des incidents de grande envergure simulés;
- assurant la promotion de plans nationaux en cas d'urgence portant sur la réaction en cas d'incident affectant la sécurité des réseaux et sur la récupération après défaillance grave;
- finançant des exercices européens portant sur des simulations d'incidents de grande envergure affectant la sécurité des réseaux;

⁹ Équipes d'intervention en cas d'urgence informatique (CERT)

- soutenant le développement et le déploiement d'un système européen de partage d'information et d'alerte (SEPIA) qui répondra d'une manière équitable et efficace aux besoins des citoyens et des PME.

(4) **améliorer la sécurité et la résilience de l'internet en:**

- définissant des priorités communautaires concernant la stabilité et la résilience à long terme de l'internet;
- parvenant à un accord sur un ensemble de principes européens, puis internationaux, pour ce qui est de la stabilité et de la résilience de l'internet.

Option stratégique 3: un cadre contraignant

La plupart des problèmes décrits ci-dessus pourraient être réglés par l'adoption d'un certain nombre de mesures contraignantes qui pourraient prendre la forme d'une directive, d'un règlement ou d'une décision, le cas échéant.

La Commission peut proposer des mesures contraignantes visant à:

- (1) **définir une base commune permettant l'harmonisation des politiques nationales.** Ces mesures peuvent être axées sur une sécurité et une résilience accrues des IIC qui sortent du cadre de la législation de marché déjà proposée;
- (2) **définir le rôle et la responsabilité des parties intéressées des secteurs public et privé** dans le domaine de la sécurité et de la résilience des infrastructures d'information critiques;
- (3) **améliorer la préparation opérationnelle**, grâce à:
 - (a) un ensemble minimal de normes relatives à des fonctions et services de niveau harmonisé pour les CERT nationales ou gouvernementales;
 - (b) un cadre pour la planification en cas d'urgence à l'échelon national, dans l'optique du développement de plans d'urgence de dimension communautaire.

5. QUE RESSORT-IL DE LA COMPARAISON DES OPTIONS?

L'option du «statu quo» ne **présente aucun avantage manifeste** en ce qui concerne l'amélioration de la sécurité et de la résilience des IIC en Europe. Il reste donc à choisir entre un cadre contraignant et un cadre non-contraignant. Actuellement, le «cadre contraignant» ne semble pas constituer une option viable pour les raisons suivantes:

- la **réalité politique** des États souverains, que toute politique de sécurité des réseaux et de l'information au niveau communautaire doit prendre en considération;
- la nécessité de tenir compte d'une responsabilité opérationnelle largement décentralisée dans le secteur privé;

- le manque d'expérience cumulée dans les domaines du partage d'informations et de la coopération sur les politiques en matière d'infrastructures d'information critiques entre les secteurs public et privé.

En outre, la **pièdre qualité des données** actuellement disponibles sur les incidents liés à la sécurité – en raison d'asymétries des informations et de préoccupations de sécurité nationale – nuit à la possibilité de définir des mesures réglementaires dans une perspective économique et de politique publique cohérente. Elle pose également **un problème en ce qui concerne le principe de proportionnalité**, étant donné qu'il est impossible de proposer des actions proportionnées lorsque l'ampleur exacte du problème n'est pas réellement connue.

En dernier lieu, en raison de la longueur du processus d'adoption, le calendrier d'une approche contraignante serait incompatible avec la nécessité d'une action rapide de la part de tous les intéressés.

L'analyse d'impact conclut que, pour le court et moyen terme, c'est l'option stratégique n° 2 qui serait préférable, avec un lancement immédiat des actions proposées et, en temps opportun, un examen des résultats, notamment de ceux du débat public concernant le renforcement et la modernisation de la politique de la sécurité des réseaux et de l'information dans l'UE. Ces éléments constitueraient la base d'une évaluation des besoins et des options relatifs à d'éventuelles mesures contraignantes dans l'avenir.

Il pourrait alors être possible de recommander la mise en œuvre d'actions du type de celles qui sont décrites dans le cadre de l'option stratégique n° 3.