COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 30.3.2009
COM(2009) 149 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, 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»

{SEC(2009) 399}
{SEC(2009) 400}

(présentée par la Commission)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, 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»

1. INTRODUCTION

Les technologies de l'information et des communications sont de plus en plus étroitement liées à notre quotidien. Certains systèmes, services, réseaux et infrastructures de TIC (ou, en bref, les infrastructures TIC) constituent une partie essentielle de l'économie et de la société européennes, soit parce qu'ils fournissent des biens et services d'importance capitale, soit parce qu'ils servent de base à d'autres infrastructures critiques. Ils sont généralement considérés comme des infrastructures d'information critiques (IIC)[1] car leur perturbation ou leur destruction aurait de graves incidences sur les fonctions vitales de la société. Au nombre de ces perturbations, on peut citer, à titre d'exemple récent, les cyberattaques de grande envergure qu'a subies l'Estonie en 2007 et la rupture de câbles transcontinentaux en 2008.

Le Forum économique mondial a estimé, en 2008, que la probabilité d'une défaillance grave des IIC dans les dix prochaines années était de 10 à 20 %, et que son coût économique potentiel, sur le plan mondial, avoisinerait 250 milliards de dollars[2].

La présente communication est consacrée à la prévention, à l'état de préparation et à la sensibilisation, et elle établit un programme d'actions à entreprendre immédiatement pour renforcer la sécurité et la résilience des IIC . L'axe choisi se situe dans la ligne du débat engagé à la demande du Conseil et du Parlement européen en ce qui concerne les défis et les priorités de la politique relative à la sécurité des réseaux et de l'information et aux instruments les mieux adaptés au niveau de l'UE pour faire face à la situation. Les actions proposées viennent également compléter les mesures de prévention et de lutte contre les menées criminelles et terroristes visant les IIC et les procédures judiciaires qui s'y rapportent, et elles s'inscrivent dans le cadre des efforts de recherche actuels et futurs de l'UE dans le domaine de la sécurité des réseaux et de l'information comme dans celui de nombreuses initiatives internationales sur le même sujet.

2. CONTEXTE POLITIQUE

La présente communication a pour but de développer la politique européenne destinée à améliorer la sécurité de la société de l'information et à renforcer la confiance qu'elle inspire aux citoyens. En 2005 déjà, la Commission[3] avait souligné qu'il était urgent de coordonner les

---

1 Une définition des IIC a été proposée dans le document COM (2005) 576 final.
2 Global Risks 2008
3 COM(2005)229.

efforts visant à renforcer la confiance des parties intéressées dans les services et communications électroniques. À cette fin, une stratégie pour une société de l'information sûre[4] a été adoptée en 2006. Ses principaux éléments, notamment la sécurité et la résilience des infrastructures TIC, ont été approuvés dans la résolution du Conseil 2007/068/01. Cependant, les parties intéressées ne semblent pas suffisamment adhérer à ces principes ni en favoriser la mise en œuvre. Cette stratégie renforce également le rôle, sur les plans tactique et opérationnel, de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), créée en 2004 aux fins d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne.

En 2008, le mandat de l'ENISA a été prolongé sans modifications jusqu'en mars 2012[5]. Dans le même temps, le Conseil et le Parlement européen appelaient à «*poursuivre les discussions concernant l'Agence [et] concernant l'orientation générale que doivent suivre les efforts européens visant à accroître la sécurité des réseaux et de l'information*.» Pour favoriser ces discussions, la Commission a lancé en novembre dernier une consultation publique en ligne[6] dont l'analyse sera disponible sous peu.

Les activités prévues dans la présente communication sont menées dans le cadre du programme européen de protection des infrastructures critiques (EPCIP)[7] et en parallèle avec ce dernier. L'un des éléments essentiels de l'EPCIP est la directive concernant le recensement et la désignation des infrastructures critiques européennes[8], qui cite le secteur des technologies de l'information et des communications parmi les secteurs prioritaires à inclure dans son champ d'application[9]. Le réseau d'alerte concernant les infrastructures critiques (CIWIN)[10] constitue un autre volet important du programme.

Sur le plan réglementaire, la proposition de la Commission concernant la réforme du cadre réglementaire pour les réseaux et services de communications électroniques[11] contient de nouvelles dispositions relatives à la sécurité et à l'intégrité, notamment en ce qui concerne le renforcement des obligations imposées aux opérateurs quant aux mesures nécessaires pour se prémunir des risques identifiés, garantir la continuité des services fournis et notifier les atteintes à la sécurité[12]. Cette approche va dans le sens de l'objectif général consistant à améliorer la sécurité et la résilience des IIC. Le Parlement européen et le Conseil se sont montrés très favorables à ces dispositions.

Les actions proposées dans la présente communication complètent des mesures existantes et en projet dans le domaine de la police et de la coopération judiciaire pour la prévention et la lutte contre les activités criminelles et terroristes visant les infrastructures TIC ainsi que pour les procédures judiciaires qui s'y rapportent, comme le prévoit notamment la décision-cadre

---

4 COM(2006)251.
5 Règlement (CE) n° 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 final
8 Directive 2008/114/CE
9 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/gena/104618.pdf
10 COM(2008) 676 final.
11 COM(2007) 697, COM(2007) 698 et COM(2007) 699.
12 Article 13 de la directive «Cadre».

du Conseil relative aux attaques visant les systèmes d'information[13] qui sera prochainement modifiée[14].

Cette initiative tient compte des activités de l'OTAN en ce qui concerne la politique commune sur la cyberdéfense, à savoir l'autorité de gestion de la cyberdéfense (CDMA) et le centre d'excellence pour la cyberdéfense.

Enfin, elle prend dûment en considération les événements survenus sur la scène politique internationale, et notamment les principes affirmés par le G8 sur la protection des infrastructures d'information critiques[15], 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 la recommandation du conseil de l'OCDE sur la protection des infrastructures d'information critiques.

3. QUEL EST L'ENJEU?

3.1. Les infrastructures d'information critiques ont une importance vitale pour la croissance économique et le développement sociétal de l'UE.

Les récents rapports sur l'innovation et la croissance économique mettent en évidence le rôle économique et sociétal du secteur des TIC et des infrastructures TIC. Il s'agit notamment de la communication sur l'examen à mi-parcours de l'initiative i2010[16], du rapport du groupe Aho[17] et des rapports économiques annuels de l'Union européenne[18]. L'OCDE souligne l'importance que revêtent les technologies de. l'information et des communications lorsqu'il s'agit «*d'améliorer notre capacité à stimuler les performances économiques et le bien-être social, et de renforcer la capacité des sociétés à améliorer la qualité de vie des citoyens dans le monde entier*.»[19].Elle recommande en outre des politiques qui renforcent la confiance dans l'infrastructure internet.
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. Les TIC constituent une composante cruciale de l'innovation et on leur doit près de 40 % des gains de productivité[20]. L'utilisation des TIC est également généralisée dans les secteurs public et administratif: l'adoption des services publics en ligne à tous les niveaux, ainsi que de nouvelles applications telles que des solutions innovantes dans le domaine de la santé, de l'énergie et de la participation politique accroissent la dépendance du secteur public à l'égard des TIC. Enfin, les citoyens comptent sur les TIC et les utilisent de plus en plus dans leur vie de tous les jours: une amélioration de la sécurité des infrastructures d'information critiques les inciterait donc à faire davantage confiance aux TIC, principalement grâce à une meilleure protection des données personnelles et de la vie privée.

---

13 2005/222/JAI.
14 COM(2008)712.
15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
16 COM(2008) 199 final.
17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
18 EU Economy 2007 Review http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
19 http://www.oecd.org/dataoecd/1/12/40825492.pdf
20 http://epp.eurostat.ec.europa.eu/ - Science and Technology/Information Society

3.2. Les risques qui menacent les infrastructures d'information critiques

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

Les cyberattaques ont aujourd'hui atteint un degré de complexité sans précédent. Les simples «expériences» sont désormais devenues des activités très élaborées exécutées à des fins lucratives ou pour des raisons politiques. Les cyberattaques de grande envergure lancées récemment contre l'Estonie, la Lituanie ou la Géorgie sont les exemples les plus médiatisés 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 continuelle du pourriel confirment la gravité du problème[21].

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, ainsi que de leur vulnérabilité et des menaces auxquelles elles sont exposées, il faut, pour envisager la sécurité et la résilience de ces infrastructures, adopter une approche systémique qui constituera une première ligne de défense contre les défaillances et les attaques.

3.3. Sécurité et résilience des infrastructures d'information critiques pour renforcer la confiance dans la société de l'information

Afin de garantir que les infrastructures des TIC sont exploitées au maximum, ce qui permettrait de réaliser pleinement le potentiel économique et social de la société de l'information, les parties intéressées doivent pouvoir leur faire vraiment confiance. Le degré de confiance qu'elles inspirent dépend de différents éléments, dont le plus important est l'existence d'un niveau élevé de sécurité et de résilience. La diversité, l'ouverture, l'interopérabilité, la facilité d'utilisation, la transparence, l'obligation de rendre des comptes et l'auditabilité des différents composants, de même que la concurrence, sont les principaux moteurs du développement de la sécurité et ils stimulent la généralisation de produits, processus et services propres à l'améliorer. Comme l'a déjà souligné la Commission[22], il s'agit là d'une responsabilité partagée: en effet, aucune des parties prenantes n'a les moyens d'assurer la sécurité et la résilience de toutes les infrastructures des TIC et d'assumer l'ensemble des responsabilités qui en découlent.

La prise en charge de ces responsabilités exige une culture et une approche de la gestion de risques qui permette de réagir aux menaces identifiées et d'anticiper celles qui sont encore inconnues, sans que la réaction soit disproportionnée et empêche l'apparition de services et applications innovants.

3.4. Les défis que doit relever l'Europe

En complément de toutes les activités liées à la mise en œuvre de la directive concernant le recensement et la désignation des infrastructures d'information critiques, et notamment la définition de critères spécifiques au secteur des TIC, il faudra surmonter un certain nombre

---

21 COM(2006) 688 final

22 COM(2006) 251 final

d'obstacles plus importants pour renforcer la sécurité et la résilience des infrastructures d'information critiques.

3.4.1. Des approches nationales disparates et non coordonnées

Même si les obstacles et les problèmes auxquels il faut faire face ont des points communs, on observe, d'un État membre à l'autre, des divergences aussi bien en ce qui concerne les mesures et les régimes permettant de garantir la sécurité et la résilience des infrastructures d'information critiques que le niveau de compétence et de préparation.

L'application d'approches purement nationales risquerait d'être à l'origine d'une fragmentation et d'un manque d'efficacité à l'échelle de l'Europe. Les différences entre approches nationales et le manque de coopération transfrontalière diminuent considérablement l'efficacité des contre-mesures nationales, notamment parce que, du fait du caractère interconnecté des infrastructures d'information critiques, un faible niveau de sécurité et de résilience des infrastructures dans un pays pourrait accroître la vulnérabilité et les risques dans d'autres.

Pour remédier à cela, il faut entreprendre, à l'échelon européen, une action destinée à apporter une valeur ajoutée aux politiques et programmes nationaux grâce à une sensibilisation plus poussée aux problèmes et à une meilleure compréhension de ces derniers et en favorisant l'adoption de priorités et d'objectifs politiques communs, en renforçant la coopération entre États membres et en intégrant les politiques nationales pour leur donner une dimension européenne et mondiale.

3.4.2. Nécessité de disposer d'un nouveau modèle européen de gouvernance pour les infrastructures d'information critiques

L'amélioration de la sécurité et de la résilience des infrastructures d'information critiques pose des problèmes particuliers en matière de gouvernance. Bien que les États membres restent, en dernier ressort, responsables de la définition de leurs politiques dans le domaine des infrastructures d'information critiques, la mise en œuvre de ces politiques dépend de l'engagement du secteur privé, qui possède ou contrôle un grand nombre de ces infrastructures. Par ailleurs, les marchés ne fournissent pas toujours au secteur privé d'incitations suffisantes pour susciter des investissements dans la protection des infrastructures d'information critiques au niveau que demanderaient normalement les gouvernements.

Pour remédier à ce problème de gouvernance, 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. Un cadre de gouvernance multipartite d'envergure européenne, qui pourrait prévoir un renforcement du rôle de l'ENISA, permettrait de stimuler l'engagement du secteur privé dans la définition d'objectifs stratégiques de politique publique ainsi que de mesures et priorités opérationnelles. L'existence d'un tel cadre permettrait de rapprocher les décisions en matière de politique prises à l'échelon national de la réalité opérationnelle sur le terrain.

3.4.3. Une capacité européenne limitée en ce qui concerne l'alerte rapide et la réaction en cas d'incident

Les mécanismes de gouvernance ne se révéleront véritablement efficaces que si tous les participants disposent d'informations à partir desquelles ils peuvent agir. Cette condition est particulièrement importante pour les gouvernements qui sont, en dernier ressort, responsables de la sécurité et du bien-être des citoyens.

Toutefois, les processus et les pratiques en matière de surveillance et de notification des incidents dans le domaine de la sécurité des réseaux varient considérablement selon les États membres. Ainsi, certains d'entre eux n'ont pas d'organisme de référence qui fasse office de centre de surveillance. En outre, en ce qui concerne les incidents de sécurité, la coopération entre États membres et le partage d'informations fiables et pouvant donner lieu à des actions ne semblent pas suffisamment développés, puisqu'ils restent soit informels, soit limités à des échanges bilatéraux ou multilatéraux restreints. Par ailleurs, la simulation d'incidents et l'organisation d'exercices destinés à tester les capacités de réaction revêtent une importance stratégique pour le renforcement de la sécurité des infrastructures d'information critiques et l'amélioration de leur résilience, notamment lorsqu'elles sont axées sur des stratégies et processus flexibles permettant de faire face au caractère imprévisible des éventuelles crises. Dans l'UE, les exercices dans le domaine de la cybersécurité se trouvent encore au stade embryonnaire. Les exercices transfrontaliers sont très limités. Les événements récents[23] ont bien montré que l'entraide constitue un élément essentiel pour apporter une réponse appropriée aux menaces et attaques de grande envergure contre les infrastructures d'information critiques.

Pour disposer d'une solide capacité européenne en ce qui concerne l'alerte rapide et la réaction en cas d'incident, il faut pouvoir compter sur des équipes d'intervention en cas d'urgence informatique (Computer Emergency Response Teams, CERT) nationales ou gouvernementales qui fonctionnent bien, c'est-à-dire avoir une base commune pour ce qui est des moyens. Ces organismes doivent, au niveau national, catalyser les intérêts des parties prenantes et les capacités d'action touchant à la politique publique (notamment en ce qui concerne les systèmes de partage d'information et d'alerte destinés aux citoyens et aux PME) et œuvrer pour une coopération et des échanges d'information transfrontaliers efficaces, éventuellement en mettant à contribution des organismes existants tels que l'EGC (Groupe des CERT gouvernementales européennes)[24].

3.4.4. Coopération internationale

Parmi les infrastructures d'information critiques, l'internet a acquis une importance telle qu'il convient d'accorder une attention particulière à sa résilience et à sa stabilité. L'internet, qui est par nature une infrastructure distribuée et redondante, a fait les preuves de sa robustesse. Cependant, sa croissance phénoménale a accru sa complexité physique et logique et a permis l'apparition d'utilisations et services nouveaux. Il est donc légitime de s'interroger sur la capacité de l'internet à résister aux perturbations et aux cyberattaques en augmentation croissante.

Les divergences de vues en ce qui concerne le caractère critique des éléments qui constituent l'internet expliquent en partie la diversité des positions gouvernementales exprimées dans les

---

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

[24] http://www.egc-group.org/

enceintes internationales et les perceptions souvent contradictoires de l'importance de la question. Cette situation pourrait nuire à une prévention appropriée des menaces liées à l'internet, mais aussi à l'état de préparation à ces menaces et à la faculté de récupération après un incident. Par exemple, il conviendrait que les conséquences de la transition de l'IPv4 vers l'IPv6 soient également évaluées sous l'angle de la sécurité.

L'internet est un réseau des réseaux mondial et hautement décentralisé, dont les centres de contrôle ne correspondent pas toujours aux frontières nationales. Pour garantir sa résilience et sa stabilité, il faut donc adopter une approche spécifique et ciblée articulée autour de deux mesures convergentes. Premièrement, il convient de parvenir à un consensus sur les priorités européennes en matière de résilience et de stabilité de l'internet, aussi bien pour ce qui est de la politique publique que pour ce qui touche au déploiement opérationnel. Deuxièmement, il fait inciter la communauté mondiale à définir un ensemble de principes conformes aux valeurs européennes essentielles pour la stabilité et la résilience de l'internet, dans le cadre de notre dialogue stratégique et de la coopération avec les pays tiers et les organisations internationales. Ces activités se fonderont sur la reconnaissance de l'importance essentielle que revêt la stabilité de l'internet par le sommet mondial sur la société de l'information[25].

4. LA VOIE A SUIVRE: RENFORCER LA COOPERATION ET LA COORDINATION DANS L'UE

En raison de la dimension communautaire et internationale du problème, une approche visant à renforcer la sécurité et la résilience des infrastructures d'information critiques qui soit intégrée au niveau de l'UE représenterait un complément et un apport de valeur ajoutée pour les programmes nationaux ainsi que pour les systèmes de coopération bilatérale et multilatérale existant entre les États membres.

Il ressort des débats sur les possibilités d'action publique 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 et en coordonnant les actions au moment de la crise. Des échanges d'information plus structurés, associés à de bonnes pratiques communes à toute l'UE faciliteraient considérablement la lutte contre les menaces transfrontalières.

Il est nécessaire de renforcer les instruments de coopération existants, tels que l'ENISA et, si nécessaire, de créer de nouveaux outils. L'adoption d'une approche multipartite et multiniveaux à l'échelon européen, qui compléterait les responsabilités nationales tout en les respectant pleinement, se révèle indispensable.

Il faut aussi comprendre parfaitement l'environnement et les contraintes. Ainsi, la nature décentralisée de l'internet, dont les nœuds de bordure peuvent servir de vecteurs d'attaque, comme dans le cas des réseaux de machines zombies, est préoccupante. Cependant, ce caractère décentralisé constitue un élément essentiel de la stabilité et de la résilience du réseau et il peut permettre une récupération beaucoup plus rapide que des procédures descendantes excessivement formalisées. Il faut donc analyser au cas par cas et avec circonspection les politiques publiques et les procédures opérationnelles à instaurer.

---

[25] **Agenda de Tunis pour la société de l'information:** http://www.itu.int/wsis/documents/doc_multi.asp?lang=fr&id=2267|0

L'échéance est également importante. En effet, il est manifestement nécessaire d'agir dès maintenant et de mettre en place rapidement les éléments nécessaires à la constitution d'un cadre qui nous permettra de faire face aux problèmes actuels et qui s'inscrira dans la future stratégie pour la sécurité des réseaux et de l'information.

L'action proposée pour faire face à ces problèmes s'articule autour des cinq axes suivants:

(1) Préparation et prévention: garantir un état de préparation à tous les niveaux;

(2) Détection et réaction: fournir des mécanismes d'alerte rapide adéquats;

(3) Atténuation et récupération: renforcer les mécanismes de défense des infrastructures d'information critiques dans l'UE;

(4) Coopération internationale: promouvoir les priorités de l'UE sur le plan international;

(5) Critères pour le secteur des TIC: soutenir la mise en œuvre de la directive concernant le recensement et la désignation des infrastructures d'information critiques[26].

5. LE PLAN D'ACTION

5.1. Préparation et prévention

Base commune de capacités et de services en vue d'une coopération paneuropéenne. La Commission invite les États membres et les parties concernées à:

- définir, avec l'appui de l'ENISA, un niveau minimum de capacités et de services pour les équipes d'intervention en cas d'urgence informatique (CERT) nationales ou gouvernementales et les opérations de réaction en cas d'incident, pour soutenir la coopération paneuropéenne;
- veiller à ce que les CERT nationales ou gouvernementales constituent un élément clé de la capacité nationale en matière de préparation, de partage d'information de coordination et de réaction.

Objectif: fin 2010 pour la définition commune de normes minimales, fin 2011 pour la mise en place de CERT nationales ou gouvernementales qui fonctionnent bien dans tous les États membres.

Partenariat public privé européen pour la résilience (EP3R). La Commission

- 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. Ce partenariat sera axé, en priorité, sur la dimension européenne envisagée sous les angles stratégique (bonnes pratiques politiques, par exemple) et tactique

[26] Directive 2008/114/CE du Conseil.

ou opérationnel (déploiement industriel). Il sera fondé sur des initiatives nationales existantes et sur les activités opérationnelles de l'ENISA et il les complétera.

Objectif: fin 2009 pour une feuille de route et un plan concernant le partenariat EP3R, mi-2010 pour l'établissement du partenariat, fin 2010 pour les premiers résultats.

Forum européen pour le partage d'information entre États membres. La Commission

- établira un forum européen permettant aux États membres d'échanger des informations et de bonnes pratiques politiques sur la sécurité et la résilience des infrastructures d'information critiques. Ce forum tirera parti des résultats des activités des autres organismes et en particulier de l'ENISA.

Objectif: fin 2009 pour le lancement du forum; fin 2010 pour les premiers résultats

5.2. Détection et réaction

Système européen de partage d'information et d'alerte (SEPIA) La Commission soutient:

le développement et le déploiement d'un système européen de partage d'information et d'alerte destiné aux citoyens et aux PME et fondé sur des systèmes nationaux et privés de partage d'information et d'alerte. La Commission soutient financièrement deux projets de prototypes complémentaires[27]. L'ENISA est invitée à faire l'inventaire des résultats de ces projets et d'autres initiatives nationales et à établir une feuille de route afin de promouvoir le développement et le déploiement du SEPIA.

Objectif: fin 2010 pour mener à bien les projets de prototypes, fin 2010 pour la feuille de route relative à un système européen.

5.3. Atténuation et récupération

Planification en cas d'urgence et exercices à l'échelon national. La Commission invite les États Membres à:

- élaborer des plans nationaux en cas d'urgence et organiser régulièrement 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, afin de renforcer la coordination paneuropéenne. Les CERT/CSIRT nationales ou gouvernementales pourraient être chargées d'organiser des exercices de planification d'urgence et de test à l'échelon national, avec la participation de parties intéressées des secteurs public et privé. L'ENISA est invitée à participer pour soutenir l'échange de bonnes pratiques entre États membres.

Objectif: fin 2010 pour l'organisation d'au moins un exercice à l'échelon national dans chaque État membre.

Exercices paneuropéens portant sur des incidents de grande envergure affectant la sécurité des réseaux. La Commission:

[27] Dans le cadre du projet européen «*Prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité*»
http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

- soutiendra financièrement le développement d'exercices paneuropéens portant sur des incidents affectant la sécurité d'internet[28], qui pourront également constituer la base opérationnelle d'une participation paneuropéenne à des exercices internationaux sur des incidents affectant la sécurité des réseaux, tels que le «Cyber Storm» aux Etats-Unis.

Objectif: fin 2010 pour la conception et le lancement du premier exercice paneuropéen, fin 2010 pour une participation paneuropéenne à des exercices internationaux.

Renforcement de la coopération entre les CERT nationales/gouvernementales. La Commission invite les États Membres à:

- renforcer la coopération entre les CERT nationales/gouvernementales, le cas échéant en mettant à contribution et en développant des mécanismes de coopération existants tels que l'EGC (Groupe des CERT gouvernementales européennes)[29]. L'ENISA est invitée à s'employer activement à stimuler et à soutenir la coopération paneuropéenne entre CERT nationales/gouvernementales, qui devrait déboucher sur une meilleure préparation, sur une capacité européenne de réaction en cas d'incident renforcée et sur des exercices paneuropéens (et/ou régionaux).

Objectif: fin 2010 pour le doublement du nombre d'organismes nationaux participant à l'ECG; fin 2010 pour le développement par l'ENISA de matériel de référence destiné à soutenir la coopération paneuropéenne.

5.4. Coopération internationale

Stabilité et résilience de l'internet. Trois activités complémentaires sont envisagées:

- Priorités européennes concernant la stabilité et la résilience à long terme de l'internet. La Commission animera un débat de dimension européenne auquel prendront part toutes les parties intéressées des secteurs public et privé, pour définir les priorités de l'UE en ce qui concerne la stabilité et la résilience à long terme de l'internet.

Objectif: fin 2010 pour les priorités de l'UE sur les composants et problèmes critiques de l'internet.

- Principes et lignes directrices pour la stabilité et la résilience de l'internet (échelon européen). La Commission s'engagera, en collaboration avec les États membres, dans un travail de définition de lignes directrices pour la stabilité et la résilience de l'internet, qui portera notamment sur des mesures correctrices régionales, des accords d'assistance mutuelle, des stratégies coordonnées de récupération et de continuité, la répartition géographique des ressources internet critiques, l'introduction de mesures de protection technologiques dans l'architecture et les protocoles de l'internet, et la reproduction et la diversité des services et des données. La Commission finance déjà une task force pour la résilience DNS qui, avec d'autres projets pertinents, permettra de parvenir à un consensus[30].

[28] Supra 27.
[29] Supra 24.
[30] Supra 27.

Objectif: fin 2009 pour une feuille de route européenne relative à des principes et lignes directrices pour la stabilité et la résilience de l'internet; fin 2010 pour un accord sur un avant-projet de principes et lignes directrices.

- Principes et lignes directrices pour la stabilité et la résilience de l'internet (niveau mondial). La Commission collaborera avec les États membres à l'élaboration d'une feuille de route destinée à promouvoir les principes et lignes directrices au niveau mondial. Une coopération stratégique sera mise en place avec les pays tiers, notamment dans le cadre de dialogues sur la société de l'information, en vue de progresser vers un consensus mondial[31].

Objectif: début 2010 pour une feuille de route européenne concernant la coopération internationale en matière de principes et lignes directrices pour la stabilité et la résilience de l'internet; fin 2010 pour un avant-projet de principes et lignes directrices internationalement reconnus à examiner avec les pays tiers et dans les enceintes concernées, et notamment le forum de gouvernance de l'internet.

Exercices de dimension mondiale portant sur l'atténuation des conséquences des incidents internet de grande envergure et sur la récupération. La Commission invite les parties intéressées, en Europe, à:

- réfléchir à un moyen pratique de donner une dimension mondiale aux exercices menés dans le cadre de l'activité «atténuation et récupération», en se fondant sur les plans et ressources d'urgence régionaux.

Objectif: fin 2010: proposition de la Commission relative à un cadre et à une feuille de route pour soutenir l'engagement et la participation de l'Europe aux exercices de dimension mondiale portant sur l'atténuation des conséquences et sur la récupération après des incidents internet de grande envergure.

5.5. Critères pour les infrastructures critiques européennes dans le secteur des TIC

Critères spécifiques au secteur des TIC En se fondant sur la première activité déjà menée à bien en 2008, la Commission:

- continuera à élaborer, en coopération avec les États membres et toutes les parties concernées, les critères relatifs à l'identification des infrastructures critiques européennes dans le secteur des TIC. À cet effet, des informations pertinentes seront tirées d'une étude spécifique en cours de lancement[32].

Objectif: première moitié de 2010: définition par la Commission des critères pour les infrastructures critiques européennes dans le secteur des TIC.

6. CONCLUSIONS

La sécurité et la résilience des infrastructures d'information critiques constituent une première ligne de défense contre les défaillances et les attaques. Il est essentiel de les renforcer dans

[31] COM(2008) 588 final.
[32] Supra 27.

l'ensemble de l'UE pour pouvoir exploiter pleinement tous les avantages qu'offre la société de l'information. Pour atteindre cet objectif ambitieux, un plan d'action visant à renforcer la coopération sur les plans tactique et opérationnel au niveau européen est proposé. Le succès des actions prévues dépend de leur capacité à tirer parti des activités des secteurs public et privé tout en leur étant bénéfique et repose sur l'engagement et la participation pleine et entière des États membres, des institutions européennes et des parties intéressées.

À cet effet, une conférence ministérielle sera organisée les 27 et 28 avril 2009. Son objectif sera l'examen des initiatives proposées avec les États membres et l'officialisation de leur engagement dans le débat sur une politique européenne de la sécurité des réseaux modernisée et renforcée.

Enfin, le renforcement de la sécurité et de la résilience des infrastructures d'information critiques est un objectif à long terme et la stratégie et les mesures adoptées dans ce domaine doivent faire l'objet d'évaluations régulières. Par conséquent, étant donné que cet objectif est conforme à l'esprit du débat d'ordre général sur l'avenir de la politique de sécurité des réseaux et de l'information dans l'UE après 2012, la Commission lancera, vers la fin 2010, un exercice d'inventaire destiné à évaluer la première phase des actions et à recenser et proposer d'autres mesures, le cas échéant.