Annexe 1 – Plan d'action PIIC dans Communication COM(2009)149 final

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 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:

- 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.

5.5. 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.