COMMISSION EUROPÉENNE

Bruxelles, le 31.3.2011
COM(2011) 163 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

«Réalisations et prochaines étapes: vers une cybersécurité mondiale»

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

«Réalisations et prochaines étapes: vers une cybersécurité mondiale»

1. INTRODUCTION

La Commission a publié, le 30 mars 2009, une communication 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] exposant un plan d'action (le plan d'action PIIC) destiné à renforcer la sécurité et la résilience des infrastructures essentielles des technologies de l'information et des communications (TIC). Cette communication avait pour objectif de stimuler et de soutenir la mise en place, au niveau européen comme au niveau national, d'un état de préparation, de mesures de sécurité et d'une capacité de résilience d'un niveau élevé. Cette approche a reçu, pour l'essentiel, le soutien du Conseil en 2009[2].

Le plan d'action pour la protection des infrastructures d'information critiques s'articule autour des cinq axes suivants: la préparation et la prévention, la détection et la réaction, l'atténuation et la récupération, la coopération internationale et les critères concernant les infrastructures critiques européennes dans le secteur des TIC. Il indique les tâches à accomplir, au titre de chacun de ces axes, par la Commission, les États membres et/ou les entreprises, avec le soutien de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

La stratégie numérique pour l'Europe[3], adoptée en mai 2010, ainsi que les conclusions du Conseil la concernant[4] soulignent bien que la confiance et la sécurité sont des conditions préalables fondamentales pour favoriser une adoption généralisée des TIC et, partant, la réalisation des objectifs de la stratégie Europe 2020 en ce qui concerne la «croissance intelligente»[5]. La stratégie numérique insiste sur la nécessité, pour toutes les parties prenantes, d'unir leurs forces dans un effort global pour renforcer la sécurité et la résilience des infrastructures TIC en centrant leur action sur la prévention, la préparation et la sensibilisation et de mettre en place des mécanismes efficaces et coordonnés propres à répondre à de nouvelles formes de cyberattaques et de cybercriminalité de plus en plus perfectionnées. Cette approche permet de garantir que des mesures de prévention et de réaction seront adoptées pour faire face au problème.

---

1 COM(2009) 149.

2 Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information (JO C 321 du 29.12.2009, p. 1).

3 COM(2010) 245.

4 Conclusions du Conseil du 31 mai 2010 concernant la stratégie numérique pour l'Europe (10130/10).

5 COM(2010)2020 et conclusions du Conseil européen des 25 et 26 mars 2010 (EUCO 7/10).

Les mesures suivantes, annoncées dans la stratégie numérique, ont été adoptées ces derniers mois: la Commission a adopté en septembre 2010 une proposition de directive relative aux attaques visant les systèmes d'information[6]. Elle vise à intensifier la lutte contre la cybercriminalité en rapprochant les règles pénales des États membres et en améliorant la coopération entre les autorités judiciaires et les autres autorités compétentes. Elle comporte aussi des dispositions permettant de s'attaquer à de nouveaux types de cyberattaques, notamment celles lancées à partir de réseaux zombies. Pour compléter ce texte, la Commission a présenté en parallèle une proposition[7] relative à un nouveau mandat visant à renforcer et à moderniser l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) afin d'accroître la confiance et d'améliorer la sécurité des réseaux. Le renforcement et la modernisation de l'ENISA aideraient également l'UE, les États membres et les partenaires privés à développer leur aptitude à prévenir, détecter et combattre les problèmes de cybersécurité, et amélioreraient leur état de préparation face à ces défis.

Enfin, la stratégie numérique, le plan d'action mettant en œuvre le programme de Stockholm[8] et la stratégie de sécurité intérieure de l'UE en action[9] reflètent tous l'attachement de la Commission à la mise en place d'un environnement numérique permettant au potentiel économique et social de chaque Européen de s'exprimer sans restrictions.

La présente communication récapitule les résultats obtenus depuis l'adoption du plan d'action PIIC en 2009. Elle décrit les prochaines étapes prévues pour chaque action, au niveau européen comme au niveau international. Elle s'intéresse également à la dimension mondiale des problèmes posés et à l'importance d'un renforcement de la coopération entre les États membres et le secteur privé aux niveaux national, européen et international, de manière à résoudre les questions d'interdépendance sur le plan mondial.

2. UN SCENARIO EN EVOLUTION

Aussi bien l'analyse d'impact accompagnant le plan d'action PIIC[10] qu'un grand nombre d'analyses et d'études de parties prenantes des secteurs privé et public soulignent non seulement la dépendance sociale, économique et politique de l'Europe à l'égard des TIC mais également l'augmentation constante de la quantité, de l'étendue, de la sophistication et de l'incidence potentielle des menaces, qu'elles soient naturelles ou dues à l'homme.

Des menaces nouvelles et d'une plus grande sophistication technologique sont apparues. Leur dimension géopolitique planétaire commence à se préciser petit à petit. Nous nous trouvons face à une tendance qui consiste à utiliser les TIC pour parvenir à l'hégémonie politique, économique et militaire, notamment en ayant recours à des moyens offensifs. La «cyberguerre» ou le «cyberterrorisme» sont des phénomènes parfois évoqués dans ce contexte.

En outre, comme l'ont montré les récents événements survenus dans le sud de la Méditerranée, certains régimes sont prêts, à des fins politiques, à perturber ou à couper arbitrairement l'accès de leur population à des moyens de communications électroniques tels

---

6 COM(2010) 517 final.
7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.

que l'internet et les communications mobiles, et ils ont la capacité de le faire. Ces interventions nationales unilatérales peuvent avoir de graves répercussions dans d'autres parties du monde[11].

Pour mieux comprendre ces menaces de différentes natures, il peut être judicieux de les classer, selon leur finalité, dans les différentes catégories suivantes:

– finalité d'**exploitation**, comme dans le cas des «menaces persistantes avancées»[12] à des fins d'espionnage économique et politique (GhostNet, par exemple[13]), du vol d'identité, des récentes attaques contre le système d'échange des droits d'émission[14] ou contre des systèmes informatiques gouvernementaux[15];

– finalité de **perturbation,** comme les attaques par déni de service distribué ou le pollupostage par l'intermédiaire de réseaux zombies (tels que le réseau Conficker qui compte 7 millions de machines et le réseau Mariposa en Espagne, avec 12,7 millions de machines[16]), Stuxnet[17] et la coupure des moyens de communication;

– finalité de **destruction.** Ce scénario ne s'est pas encore concrétisé mais, compte tenu de l'utilisation de plus en plus généralisée des TIC dans les infrastructures critiques (réseaux électriques et systèmes d'alimentation en eau intelligents, par exemple), il ne peut pas être exclu à l'avenir[18].

3. L'UNION EUROPEENNE DANS UN CONTEXTE MONDIAL

Les problèmes qui se posent ne concernent pas exclusivement l'Union européenne (UE), et cette dernière ne pourra pas non plus y faire face seule. L'omniprésence des TIC et de l'internet permet de rendre la communication, la coordination et la coopération entre parties intéressées plus efficace et plus économique et favorise le développement d'un écosystème de l'innovation dynamique dans tous les secteurs. Cependant, des menaces peuvent provenir aujourd'hui de n'importe quel endroit du monde et, parce que le monde entier est interconnecté, toucher n'importe quelle partie du monde.

Pour résoudre les problèmes qui nous attendent, une approche purement européenne ne suffit pas. L'objectif consistant à mettre en place une approche cohérente et coopérative au sein de

---

11 Communication conjointe «Un partenariat pour la démocratie et une prospérité partagée avec le sud de la Méditerranée», COM(2011)200 du 8.3.2011.

12 Par exemple, des attaques continues et coordonnées contre des organismes gouvernementaux et des administrations publiques. Ce phénomène devient maintenant préoccupant pour le secteur privé (voir le rapport «RSA 2011 cybercrime trends report».

13 Voir les rapports du projet «Information Warfare Monitor» intitulés «Tracking GhostNet: investigating a Cyber Espionage Network» (2009) et «Shadows in the Cloud: Investigating Cyber Espionage 2.0» (2010).

14 Voir les questions et réponses données à l'adresse suivante: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Telles que les attaques récentes contre des services du gouvernement français.

16 Voir le projet OCDE/IFP sur les futurs chocs mondiaux, rapport «Reducing systemic cyber-security risks» du 14 janvier 2011, à l'adresse suivante http://www.oecd.org/dataoecd/3/42/46894657.pdf (en anglais).

17 Voir http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis

18 Voir le rapport «Global Risks 2011» du Forum économique mondial.

l'UE n'a rien perdu de son importance, mais il doit s'inscrire dans une stratégie de coordination mondiale étendue à des partenaires essentiels, qu'il s'agisse de nations ou d'organisations internationales concernées par ces questions.

Nous devons œuvrer en faveur d'une compréhension globale des risques inhérents à l'utilisation massive et généralisée des TIC par toutes les composantes de la société. Qui plus est, il nous faut concevoir des stratégies permettant de gérer ces risques de manière efficace et appropriée, par la prévention, la parade, l'atténuation et la réaction. La stratégie numérique en appelle à la «*coopération des acteurs concernés* [qui] *doit s'organiser au niveau mondial pour réellement permettre de lutter contre les atteintes à la sécurité et en limiter le risque*» et fixe un objectif consistant à «*travailler avec les acteurs concernés dans le monde, notamment pour améliorer la* ***gestion mondiale des risques*** *dans l'environnement numérique et physique, et mener des actions ciblées, coordonnées au niveau international, contre la criminalité informatique et les atteintes à la sécurité.*»

4. MISE EN ŒUVRE DU PLAN D'ACTION PIIC DE L'UE: POINTS SAILLANTS

Le rapport complet concernant les résultats déjà obtenus dans le cadre du plan d'action PIIC et les prochaines étapes prévues figure à l'annexe. En ce qui concerne l'état actuel de la situation, les points saillants sont exposés ci-après.

4.1. Préparation et prévention

- Le **Forum européen des États membres** a accompli des progrès significatifs dans la promotion des débats et des échanges entre autorités compétentes en ce qui concerne les bonnes pratiques en matière de sécurité et de résilience des infrastructures TIC**.** Les États membres considèrent ce Forum comme une plateforme importante pour le dialogue et l'échange de bonnes pratiques[19]. Ses futures activités continueront à bénéficier du soutien de l'ENISA et porteront sur la coopération entre les équipes d'intervention en cas d'urgence informatique (CERT) nationales/gouvernementales, la définition de mesures incitatives, de nature économique et réglementaire, en faveur de la sécurité et de la résilience (dans le respect des règles applicables dans le domaine de la concurrence et des aides d'État), l'évaluation de la situation de la cybersécurité en Europe, l'organisation d'exercices paneuropéens ainsi que l'examen des priorités à aborder dans un cadre international en matière de sécurité et de résilience.

- Le **Partenariat public-privé européen pour la résilience** (EP3R) constitue un cadre européen souple de gouvernance pour la résilience des infrastructures TIC. Il a pour but d'encourager la coopération entre le secteur public et le secteur privé sur des questions stratégiques de politique de l'UE en matière de sécurité et de résilience. L'ENISA a fait office de facilitateur pour les activités de l'EP3R et, conformément à la proposition de la Commission de 2010 relative à la modernisation de l'ENISA, elle fournira un cadre durable à long terme pour l'EP3R. L'EP3R constituera aussi une plateforme de portée mondiale pour les questions relatives à la politique publique, à l'économie et aux marchés à examiner

[19] Dans sa réponse au cinquième rapport de la commission sur l'Union européenne de la Chambre de Lords concernant le plan d'action PIIC, le gouvernement britannique déclare que le Forum européen des États membres est une initiative couronnée de succès, qui répond à un réel besoin en fournissant aux décideurs un cadre au sein duquel échanger leurs expériences.

sous l'angle de la sécurité et de la résilience, notamment pour renforcer la gestion mondiale des risques dans le domaine des infrastructures TIC.

- La **base minimale de capacités et de services**[20] et les **recommandations stratégiques** qui lui sont associées[21], permettant aux CERT nationales/gouvernementales de fonctionner efficacement et d'être la cheville ouvrière du dispositif national de préparation, d'échange d'informations, de coordination et de réaction ont été élaborées. Il va désormais être possible d'établir sur cette base, avec le soutien de l'ENISA, un réseau de CERT nationales/gouvernementales opérationnelles dans tous les États membres d'ici à 2012. Ce réseau sera la pierre angulaire d'un système européen de partage d'informations et d'alerte (SEPIA) pour les particuliers et les PME qui doit être mis en place à l'aide de ressources et de moyens nationaux d'ici à la fin de 2013.

4.2. Détection et réaction

- L'ENISA a établi une feuille de route à haut niveau pour promouvoir le développement, d'ici à 2013, d'un système européen de partage d'informations et d'alerte (**SEPIA)**[22]**,** reposant sur la mise en œuvre de *services de base* au niveau des CERT nationales/gouvernementales et de *services d'interopérabilité* en vue de l'intégration des systèmes nationaux de partage d'informations et d'alerte dans le SEPIA. Il sera essentiel, dans le cadre de cette activité, d'assurer un niveau approprié de protection des données personnelles.

4.3. Atténuation et récupération

- Jusqu'à présent, seuls 12 États membres ont organisé 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[23]. L'ENISA a publié un guide de **bonne pratique pour les exercices nationaux**[24], ainsi que des **recommandations** sur le développement de stratégies nationales[25] afin de soutenir les activités des États membres, qui devraient être intensifiées.

- Le premier **exercice paneuropéen portant sur des incidents de grande envergure affectant la sécurité des réseaux** (Cyber Europe 2010) a eu lieu le 4 novembre 2010 avec la participation de tous les États membres, dont 19 ont participé activement à l'exercice, et de la Suisse, la Norvège et l'Islande. Il serait sans nul doute avantageux que les futurs exercices paneuropéens disposent d'un cadre commun fondé sur les plans d'urgence nationaux et fonctionnant en interaction avec eux, qui fournirait les mécanismes et procédures de base pour les communications et la coopération entre États membres.

---

20 Voir: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs

21 Voir http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Source: ENISA.

24 Voir: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport

25 Voir: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

4.4. Coopération internationale

- **Des principes et lignes directrices européens pour la stabilité et la résilience de l'internet**[26] ont été élaborés après avoir fait l'objet d'un examen dans le cadre du Forum européen des États membres. La Commission va examiner ces principes et les promouvoir auprès des principaux intéressés, notamment le secteur privé (par l'intermédiaire de l'EP3R), dans un cadre bilatéral avec des partenaires internationaux majeurs, notamment les États-Unis, ainsi que dans un cadre multilatéral. Elle mènera ces activités, dans la limite de ses compétences, dans des enceintes telles que le G8, l'OCDE, l'OTAN (en particulier sur la base de son nouveau concept stratégique adopté en novembre 2010 et des activités du centre d'excellence pour la cyberdéfense en coopération), l'UIT (dans le cadre du renforcement des capacités dans le domaine de la cybersécurité), l'OSCE (par l'intermédiaire de son forum pour la coopération en matière de sécurité), l'ASEAN, Meridian[27], etc. L'objectif est de transformer ces principes et lignes directrices en un cadre commun propice à un engagement collectif international sur la résilience et la stabilité à long terme de l'internet.

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

- Les discussions techniques au sein du Forum européen des États membres ont débouché sur une **première version des critères spécifiques au secteur des TIC** pour recenser les infrastructures européennes critiques, portant plus particulièrement sur les **communications fixes et mobiles et l'internet.** Les discussions techniques, qui vont se poursuivre, bénéficieront de l'apport des consultations sur la première version des critères, lancées avec le secteur privé au niveau national et européen (par l'intermédiaire de l'EP3R). La Commission examinera aussi avec les États membres les éléments spécifiques au secteur des TIC à prendre en considération pour le réexamen de la directive concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection[28] en 2012.

5. PROCHAINES ETAPES

Des résultats positifs, tels que la reconnaissance de la nécessité d'adopter une approche coopérative de la sécurité des réseaux et de l'information associant l'ensemble des parties prenantes, ont déjà été obtenus dans le cadre de la mise en œuvre du plan PIIC. Cette mise en œuvre respecte aussi, dans les grandes lignes, le calendrier et les étapes fixés en 2009. Cependant, il ne faut pas verser dans le triomphalisme car il reste beaucoup à faire, aux niveaux national et européen, pour que les efforts déployés soient efficaces.

Il est aussi très important d'inscrire ces efforts dans une stratégie de coordination mondiale et, par conséquent, de leur donner une dimension internationale, avec tous les partenaires concernés, pour se rapprocher d'autres régions, pays ou organisations confrontés à des problèmes similaires, et de créer des partenariats pour mettre en commun les approches suivies et les activités qui y sont associées et éviter la duplication des efforts.

---

[26] Voir http://ec.europa.eu/information_society/policy/nis/index_en.htm

[27] L'initiative Meridian vise à fournir aux gouvernements du monde entier un cadre au sein duquel ils peuvent discuter des moyens de coopérer au niveau des politiques en matière de protection des infrastructures d'information critiques (PIIC). Voir http://meridianprocess.org/

[28] Directive 2008/114/CE du Conseil

Il nous faut promouvoir une culture mondiale de la gestion des risques. Elle devra être axée sur la promotion d'actions coordonnées visant à prévenir, détecter et atténuer toutes les formes de perturbations, naturelles ou liées à l'homme, et à y apporter une réponse, et à poursuivre en justice les cyberdélinquants. À cet effet, il faudra mener des actions ciblées pour lutter contre les menaces pesant sur la sécurité et combattre la criminalité informatique.

À cette fin, la **Commission compte**:

- **promouvoir des principes pour la résilience et la stabilité de l'internet**. Il convient d'établir, en concertation avec d'autres pays, des organisations internationales et, le cas échéant, des organismes privés d'envergure mondiale, des principes internationaux pour la résilience et la stabilité de l'internet. Il faudrait, pour ce faire, utiliser des forums et des mécanismes existants, tels que ceux qui sont associés à la gouvernance de l'internet. Ces principes devraient constituer le cadre dans lequel devraient s'inscrire les activités de toutes les parties prenantes en matière de stabilité et de résilience de l'internet. Les principes et lignes directrices européens devraient, à cet égard, jouer un rôle fondateur;

- **constituer des partenariats stratégiques de dimension internationale.** Il convient de tirer parti des efforts entrepris dans des domaines critiques, tels que la gestion des incidents informatiques, pour créer des partenariats stratégiques, avec notamment des exercices et des mesures de coopération entre CERT. L'engagement du secteur privé, dont les activités ont une dimension mondiale, revêt une importance primordiale. La création, lors du sommet UE-États-Unis de novembre 2010, d'un groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité, constitue un grand pas dans cette direction. Les travaux de ce groupe porteront sur la gestion des incidents informatiques, les partenariats public-privé, la sensibilisation et la criminalité informatique. Le groupe peut aussi envisager un rapprochement avec d'autres pays ou régions confrontés à des problèmes similaires, en vue, selon le cas, de mettre en commun les approches suivies et les activités qui y sont associées ou d'éviter la duplication des efforts. Il convient de continuer à développer les actions entreprises et la coordination dans les enceintes internationales, notamment dans le cadre du G8. En Europe, le principal facteur de succès sera une bonne coordination entre toutes les institutions de l'UE, les organismes concernés (notamment l'ENISA et Europol) et les États membres;

- **renforcer la confiance dans l'informatique en nuage.** Il faut absolument intensifier les discussions sur les meilleures stratégies de gouvernance pour les technologies émergentes ayant une incidence mondiale, telles que l'informatique en nuage. Ces discussions devraient porter sur une gouvernance appropriée dans le cadre de la protection des données personnelles sans pour autant être limitées à cet aspect. La confiance est essentielle pour qu'il soit possible d'exploiter pleinement les avantages de cette technologie[29].

La sécurité est une responsabilité partagée par tous, par conséquent tous les États membres doivent veiller à ce que les mesures qu'ils adoptent et les efforts qu'ils déploient contribuent collectivement à une approche européenne coordonnée visant à prévenir, détecter et atténuer

[29] Voir par exemple les rapports de l'ENISA intitulés «Cloud Computing Information Assurance Framework» (2009), à l'adresse http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) et «Security and resilience in governmental clouds» (2011), à l'adresse http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

toutes les formes de perturbations et attaques informatiques et à y apporter une réponse. À cet égard, **les États membres devraient s'engager à**:

- **améliorer l'état de préparation de l'UE en mettant en place un réseau de CERT nationales/gouvernementales opérationnelles d'ici à 2012.** Pour leur part, les institutions de l'UE créeront aussi une CERT à leur niveau d'ici à 2012. Tous les efforts déployés dans ce cadre devraient s'appuyer sur la base minimale de capacités et de services et sur les recommandations stratégiques qui lui sont associées, établies par l'ENISA, qui continuera à apporter son soutien à ces initiatives. Ces activités permettront également de promouvoir la mise en place d'un système européen de partage d'informations et d'alerte (SEPIA) pour le grand public d'ici à 2013;

- **établir un plan d'urgence européen en cas d'incident informatique d'ici à 2012 et organiser des exercices paneuropéens réguliers dans le domaine de la cybersécurité .** Ces exercices revêtent une importance non négligeable pour une stratégie cohérente relative à un plan d'urgence européen en cas d'incident informatique et à la récupération après incident, au niveau national comme au niveau européen. Les futurs exercices paneuropéens devraient être lancés sur la base d'un plan d'urgence européen en cas d'incident qui soit fondé sur les plans d'urgence nationaux et fonctionne en interaction avec eux. Ce plan devrait fournir les mécanismes et procédures de base pour la communication entre États membres ainsi qu'un appui pour définir l'envergure des futurs exercices paneuropéens et les organiser. L'ENISA collaborera avec les États membres afin que ce plan d'urgence européen en cas d'incident informatique soit établi d'ici à 2012. Pour cette même date, tous les États membres devraient mettre en place des plans d'urgence nationaux et des exercices réguliers de réaction et récupération;

- **déployer des efforts coordonnés au niveau européen dans le cadre de forums internationaux et amorcer des dialogues sur l'amélioration de la sécurité et de la résilience de l'internet.** Les États membres devaient coopérer entre eux et avec la Commission pour promouvoir l'adoption d'une approche fondée sur des principes ou des normes qui soit applicable à la stabilité et à la résilience mondiales de l'internet. Son objectif serait de promouvoir la prévention et la préparation à tous les niveaux et auprès de toutes les parties prenantes, ce qui rééquilibrerait les discussions actuelles, beaucoup plus axées sur les aspects militaires ou de sécurité nationale.

6. CONCLUSION

L'expérience montre qu'appliquer des approches strictement nationales ou régionales pour s'attaquer aux problèmes de sécurité et de résilience ne suffit pas. La coopération européenne s'est développée de manière notable depuis 2009 et les résultats obtenus sont encourageants, notamment dans le cadre de l'exercice Cyber Europe 2010. L'Europe doit toutefois persévérer dans ses efforts visant à mettre en place une approche cohérente et coopérative dans l'ensemble de l'UE. Une fois modernisée, l'ENISA devrait apporter un soutien accru aux États membres, aux institutions de l'UE et au secteur privé dans cette entreprise à long terme.

Pour être couronnés de succès, les efforts européens doivent s'inscrire dans une approche coordonnée au niveau mondial. À cet effet, la Commission va promouvoir un dialogue sur la cybersécurité dans toutes les enceintes internationales appropriées.

Une conférence ministérielle sur la PIIC, organisée par la présidence hongroise de l'UE, se tiendra les 14 et 15 avril 2011. Cette réunion sera une excellente occasion de renforcer la volonté de coordination et de coopération entre les États membres aux niveaux européen et international.

ANNEXE

Plan d'action PIIC: présentation détaillée des réalisations et prochaines étapes

Les résultats des activités exécutées dans le cadre du plan d'action PIIC correspondent en gros au calendrier et aux étapes fixés par la Commission en 2009. Dans les paragraphes suivants, les «réalisations» et les «prochaines étapes» sont décrites pour tous les axes. La description de la situation tient compte du fait que certaines activités ont été poussées plus avant dans le cadre de la stratégie numérique et de la stratégie de sécurité intérieure de l'UE en action.

1. Préparation et prévention

Base commune de capacités et de services en vue d'une coopération paneuropéenne

Réalisations

– En 2009, l'ENISA et le réseau européen d'équipes d'intervention en cas d'urgence informatique (CERT) ont établi et approuvé une base minimale de capacités et de services que les CERT nationales/gouvernementales doivent posséder pour pouvoir soutenir efficacement la coopération paneuropéenne. Un consensus a pu être trouvé sur une liste d'exigences «essentielles» dans les domaines du fonctionnement, des capacités techniques, du mandat et de la coopération[30].

– En 2010, l'ENISA a collaboré avec le réseau des CERT en Europe pour transformer les exigences à finalité opérationnelle précitées en un ensemble de recommandations stratégiques[31] qui permettront aux CERT nationales/gouvernementales d'être la cheville ouvrière des dispositifs nationaux de préparation, d'échange d'informations, de coordination et de réaction.

– Aujourd'hui, 20 États membres[32] ont créé des CERT nationales/gouvernementales et pratiquement tous les autres prévoient d'en mettre en place. Conformément à l'annonce faite dans les communications sur la stratégie numérique et la stratégie de sécurité intérieure de l'UE en action, la Commission a proposé des mesures pour créer une CERT pour les institutions de l'UE d'ici à 2012.

Prochaines étapes

– L'ENISA continuera à soutenir les États membres qui n'ont pas encore créé de CERT nationale/gouvernementale satisfaisant aux exigences de base approuvées susmentionnées, afin de garantir que l'objectif d'avoir des CERT nationales/gouvernementales opérationnelles dans tous les États membres d'ici à la fin de 2011 sera atteint. Une fois cette étape franchie, la mise en place d'un réseau opérationnel de CERT au niveau national **d'ici à 2012** pourra être envisagé, conformément à la stratégie numérique.

– L'ENISA étudiera, en coopération avec les CERT nationales/gouvernementales, la possibilité d'étendre les «capacités de base» et les éventuelles modalités de cette extension,

---

30 Voir: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs

31 Voir http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Source: ENISA.

dont l'objectif serait d'adapter la capacité des CERT à garantir la résilience et la stabilité des infrastructures TIC essentielles et à devenir la pierre angulaire d'un système européen de partage d'informations et d'alerte (SEPIA) pour les particuliers et les PME. Ce système doit être mis en place à l'aide de ressources et de moyens nationaux **d'ici à 2013,** conformément à la communication sur la stratégie de sécurité intérieure de l'UE en action.

Partenariat public-privé européen pour la résilience (EP3R).

Réalisations

– En 2009 a été lancé le partenariat public-privé européen pour la résilience (EP3R), qui constitue un cadre européen de gouvernance pour la résilience des infrastructures TIC. Il a pour but d'encourager la coopération entre le secteur public et le secteur privé sur des objectifs en matière de sécurité et de résilience, des exigences de base, et des pratiques et mesures appropriées. Comme l'indique la communication sur la stratégie de sécurité intérieure de l'UE en action, l'EP3R devrait également «*s'associer à des partenaires internationaux en vue de renforcer la gestion des risques informatiques au niveau mondial*». L'ENISA a facilité les activités de l'EP3R.

– Des parties prenantes des secteurs privé et public ont été consultées pour définir les objectifs, les principes et la structure de l'EP3R et déterminer quelles mesures pourraient être utilisées pour inciter les intéressés à prendre une part active aux travaux[33]. La proposition relative à la modernisation de l'ENISA recense les domaines d'action prioritaires pour l'EP3R[34].

– Parallèlement à la conception de la structure de l'EP3R, trois groupes de travail ont été créés à la fin de 2010 pour se pencher sur (a) les principaux atouts, ressources et fonctions permettant la fourniture sûre et continue des communications électroniques entre les pays; (b) les exigences de base en matière de sécurité et de résilience des communications électroniques; (c) les besoins en matière de coordination et de coopération et les mécanismes de préparation et de réaction à des perturbations de grande envergure affectant les communications électroniques.

– En 2010, la proposition de la Commission relative à la modernisation de l'ENISA prévoyait de fournir un cadre durable à long terme à l'EP3R en préconisant que l'ENISA «[favorise] *la coopération entre parties prenantes publiques et privées au niveau de l'Union, notamment en promouvant le partage d'informations et la sensibilisation et en accompagnant leurs efforts pour mettre au point et adopter des normes en matière de gestion des risques et de sécurité des produits, réseaux et services électroniques*».

Prochaines étapes

– En 2011, l'EP3R continuera à renforcer la coopération entre le secteur public et le secteur privé pour améliorer la sécurité et la résilience au moyen de mesures et d'instruments novateurs et pour déterminer les responsabilités des parties prenantes. Les groupes de travail de l'EP3R livreront leurs premiers résultats en tirant parti du rôle de facilitateur et du soutien de l'ENISA. Les futures activités porteront aussi sur les problèmes que posent

[33] Voir http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

[34] COM(2010) 521.

les réseaux intelligents en ce qui concerne la cybersécurité, sur la base des travaux préparatoires exécutés par la Commission et l'ENISA.

– L'EP3R constituera une plateforme de portée mondiale pour les questions relatives à la politique publique, à l'économie et aux marchés qui ont trait à la sécurité et à la résilience. La Commission compte tirer parti de l'EP3R pour soutenir les activités du groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité afin de fournir un environnement cohérent pour la coopération entre le secteur public et le secteur privé, dans le respect des règles applicables dans le domaine de la concurrence et des aides d'État.

– À long terme, et conformément à la proposition relative à un nouveau règlement sur l'ENISA, il est envisagé de faire de l'EP3R une activité essentielle d'une ENISA modernisée.

Forum européen des États membres

Réalisations

– Un Forum européen des États membres a été créé en 2009 pour favoriser les débats et les échanges entre autorités publiques concernées en matière de bonnes pratiques, en vue de partager des priorités et des objectifs stratégiques dans le domaine de la sécurité et de la résilience des infrastructures TIC, en tirant directement parti des travaux effectués et du soutien apporté par l'ENISA. Ce Forum, dont les membres se réunissent tous les trimestres, bénéficie depuis la mi-2010 du soutien d'un portail web spécialisé géré par l'ENISA.

– Il a accompli des progrès significatifs en ce qui concerne: (a) la définition des critères relatifs à l'identification des infrastructures TIC européennes critiques dans le cadre de la directive concernant le recensement et la désignation des infrastructures critiques européennes[35]; (b) le recensement des priorités, principes et lignes directrices européens pour la stabilité et la résilience de l'internet; (c) l'échange de bonnes pratiques, notamment pour les exercices dans le domaine de la cybersécurité.

– Les États membres considèrent ce Forum comme une plateforme importante pour le dialogue et l'échange de bonnes pratiques[36].

Prochaines étapes

– En 2011, le Forum clôturera les discussions techniques sur les critères relatifs à l'identification des infrastructures TIC européennes critiques et fournira des orientations et priorités à long terme en ce qui concerne les exercices paneuropéens portant sur des incidents de grande envergure affectant la sécurité des réseaux et des informations.

– Il participera davantage aux débats sur les priorités de portée internationale en matière de sécurité et de résilience, notamment en lien avec les activités du groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité.

---

35 Directive 2008/114/CE du Conseil.

36 Dans sa réponse au cinquième rapport de la commission sur l'Union européenne de la Chambre de Lords concernant le plan d'action PIIC, le gouvernement britannique déclare que le Forum européen des États membres est une initiative couronnée de succès et qu'elle répondait à un réel besoin en fournissant aux décideurs un cadre au sein duquel échanger leurs expériences.

– Parmi les domaines sur lesquels porteront en priorité les futures activités du Forum, qui bénéficieront du soutien direct de l'ENISA, on peut citer[37]: l'élaboration de méthodes permettant d'établir une coopération efficace entre les CERT nationales/gouvernementales; l'utilisation d'exigences minimales dans les marchés publics pour renforcer la cybersécurité; la définition de mesures incitatives, de nature économique et réglementaire, en faveur de la sécurité et de la résilience (dans le respect des règles applicables dans le domaine de la concurrence et des aides d'État) et l'évaluation de l'état actuel de cybersécurité en Europe.

2. Détection et réaction

Système européen de partage d'informations et d'alerte (SEPIA)

Réalisations

– Deux projets prototypes (FISHAS et NEISAS) ont été financés par la Commission et livrent actuellement leurs résultats finaux.

– En s'appuyant sur son rapport de faisabilité de 2007[38] et sur l'analyse de projets pertinents aux niveaux national et européen, l'ENISA a élaboré une feuille de route à haut niveau pour promouvoir le développement, d'ici à 2013, d'un système européen de partage d'informations et d'alerte (SEPIA)[39].

Prochaines étapes

– En 2011, l'ENISA assistera les États membres pour la mise en œuvre d'une feuille de route SEPIA en développant les «services de base» dont les États membres ont besoin pour mettre en place leurs systèmes nationaux de partage d'informations et d'alerte (SPIA) fondés sur les capacités de leurs CERT nationales/gouvernementales.

– En 2012, l'ENISA développera les «services d'interopérabilité» permettant l'intégration de tous les systèmes nationaux de partage d'informations et d'alerte dans le SEPIA. Elle apportera également une assistance aux États membres pour la phase de test de ces services qui consistera à intégrer progressivement les systèmes nationaux.

– Dans le courant de 2011-2012, l'ENISA engagera les CERT nationales/gouvernementales à intégrer la fonction SPIA dans leurs services.

37 COM(2010) 251.

38 Voir http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

3. Atténuation et récupération

Planification en cas d'urgence et exercices à l'échelon national

Réalisations

– À la fin de 2010, 12 États membres avaient élaboré un plan national en cas d'urgence et/ou organisé 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[40].

– En se fondant sur l'expérience acquise au niveau national et international, l'ENISA a élaboré un guide de bonne pratique pour les exercices nationaux [41]: elle a organisé, avec les États membres et des CERT du monde entier, des manifestations consacrées aux exercices nationaux; et, plus récemment, elle a publié des recommandations sur le développement des stratégies nationales qui attribuent aux CERT/CSIRT nationales ou gouvernementales un rôle essentiel dans la conduite d'exercices de planification d'urgence et de test à l'échelon national, avec la participation de parties intéressées des secteurs public et privé[42].

Prochaines étapes

– L'ENISA continuera à soutenir les efforts déployés par les États membres pour 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.

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

Réalisations

– Le premier exercice paneuropéen portant sur des incidents de grande envergure affectant la sécurité des réseaux (*Cyber Europe 2010*) a eu lieu le 4 novembre 2010 avec la participation de tous les États membres, dont 19 ont été acteurs de l'exercice, et de la Suisse, la Norvège et l'Islande. Il a été organisé et évalué[43] par l'ENISA et huit États membres ont joué un rôle actif dans l'équipe de planification. Il a également bénéficié de l'assistance technologique du Centre commun de recherche (JRC).Prochaines étapes

– En 2011, les États membres se consacreront à l'examen de l'objectif et de l'envergure du prochain exercice paneuropéen dans le domaine de la cybersécurité, qui est prévu pour 2012. L'éventualité d'une approche par étapes, avec des exercices plus approfondis, faisant intervenir un plus petit nombre d'États membres et à laquelle participeraient éventuellement des acteurs internationaux, sera envisagée. L'ENISA continuera à soutenir ce processus.

---

40 Voir http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 Voir http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 Voir http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations..

43 Voir http://www.enisa.europa.eu/.

– La Commission apporte un soutien financier au projet EuroCybex, qui concerne l'organisation d'un exercice de simulation pendant le deuxième semestre de 2011.

– Les exercices dans le domaine de la cybersécurité sont un élément important de toute stratégie cohérente relative à un plan d'urgence européen en cas d'incident informatique, au niveau national comme au niveau européen. Les futurs exercices paneuropéens devraient, par conséquent, être lancés sur la base d'un plan d'urgence européen en cas d'incident informatique qui soit fondé sur les plans d'urgence nationaux et fonctionne en interaction avec eux. Ce plan devrait fournir les mécanismes et procédures de base pour la communication entre États membres ainsi qu'un appui pour définir l'envergure des futurs exercices paneuropéens et les organiser. L'ENISA collaborera avec les États membres afin que ce plan d'urgence européen en cas d'incident informatique soit élaboré d'ici à 2012. Pour cette même date, tous les États membres doivent mettre en place des plans d'urgence nationaux et des exercices réguliers de réaction et récupération. Le Forum européen des États membres se chargera de coordonner les travaux nécessaires pour obtenir ces résultats.

Renforcement de la coopération entre les CERT nationales/gouvernementales.

Réalisations

– La coopération entre les CERT nationales/gouvernementales s'est intensifiée. Les travaux de l'ENISA sur la base minimale de capacités des CERT nationales/gouvernementales, les exercices des CERT et les exercices nationaux et sur la gestion des incidents dans le domaine de la cybersécurité ont permis de stimuler et de soutenir le renforcement de la coopération paneuropéenne entre les CERT nationales/gouvernementales.

Prochaines étapes

– L'ENISA continuera à soutenir la coopération entre les CERT nationales/gouvernementales. À cette fin, elle procédera, en 2011, à une analyse des exigences et donnera des orientations quant au choix d'un canal sûr et approprié pour la communication avec les CERT, y compris une feuille de route pour la mise en œuvre et le développement futur. L'ENISA analysera aussi les lacunes opérationnelles au niveau européen et fera rapport sur les possibilités de renforcer la collaboration transnationale entre CERT et parties intéressées, notamment pour la coordination de la réaction en cas d'incident.

– Dans la communication sur la stratégie numérique, il est demandé aux États membres de mettre en place un réseau opérationnel de CERT au niveau national **d'ici à 2012.**

4. Coopération internationale

Stabilité et résilience de l'internet.

Réalisations

– Des principes et lignes directrices européens pour la résilience et la stabilité de l'internet[44] ont été établis sur la base des travaux réalisés dans le cadre du Forum européen des États membres.

Prochaines étapes

– En 2011, la Commission va: promouvoir et examiner ces principes, aussi bien dans le cadre de la coopération bilatérale avec des partenaires internationaux, comme les États-Unis, que dans des dialogues multilatéraux au sein du G8, de l'OCDE, de l'initiative Meridian et de l'UIT; engager une consultation avec les parties intéressées, notamment le secteur privé, aux niveaux européen (par l'intermédiaire de l'EP3R) et international (dans le cadre du forum de gouvernance de l'internet et d'autres enceintes appropriées); et promouvoir des débats avec des acteurs/organisations majeurs de l'internet.

– En 2012, les partenaires internationaux s'emploieront à transformer ces principes et lignes directrices en un cadre commun propice à un engagement collectif international sur la résilience et la stabilité à long terme de l'internet.

Exercices de dimension mondiale portant sur l'atténuation des conséquences des incidents informatiques de grande envergure et sur la récupération.

Réalisations

– Sept États membres[45] ont participé à l'exercice américain dans le domaine de la cybersécurité Cyber Storm III en tant que partenaires internationaux. La Commission et l'ENISA y ont pris part à titre d'observateurs.

Prochaines étapes

– En 2011, la Commission élaborera avec les États-Unis, sous l'égide du groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité, un programme commun et une feuille de route en vue d'organiser des exercices transcontinentaux communs ou synchronisés dans le domaine de la cybersécurité en 2012/2013. Un rapprochement avec d'autres pays ou régions confrontés à des problèmes similaires afin de mettre en commun les approches suivies et les activités qui y sont associées sera aussi envisagé.

[44] Voir http://ec.europa.eu/information_society/policy/nis/index_en.htm

[45] L'Allemagne, la France, la Hongrie, l'Italie, les Pays-Bas, le Royaume-Uni et la Suède.

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

Critères sectoriels pour le recensement des infrastructures critiques européennes dans le secteur des TIC

Réalisations

– Les discussions techniques sur les critères spécifiques au secteur des TIC au sein du Forum européen des États membres ont débouché sur une première version de ces critères pour les communications fixes et mobiles et l'internet.

Prochaines étapes

– Ces discussions sur les critères sectoriels se poursuivront au sein du Forum et devraient prendre fin à la fin de 2011. En parallèle, des consultations avec le secteur privé sur la première version des critères sectoriels sont prévues par certains États membres et au niveau européen (par l'intermédiaire de l'EP3R).

– La Commission examinera aussi avec les États membres les éléments spécifiques au secteur des TIC à prendre en considération pour le réexamen de la directive 2008/114/CE concernant le recensement et la désignation des infrastructures européennes critiques en 2012.