Informations de base

2011/2284(INI) INI - Procédure d'initiative	Procédure terminée
Protection des infrastructures d'information critiques: réalisations et prochaines étapes: vers une cybersécurité mondiale **Subject** 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ITRE Industrie, recherche et énergie	KALFIN Ivailo (S&D)	07/06/2011
	Rapporteur(e) fictif/fictive VAN NISTELROOIJ Lambert (PPE) CREUTZMANN Jürgen (ALDE) ANDERSDOTTER Amelia (Verts/ALE) TOŠENOVSKÝ Evžen (ECR) ZUBER Inês Cristina (GUE/NGL) TZAVELA Niki (EFD)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	La commission a décidé de ne pas donner d'avis.	
LIBE Libertés civiles, justice et affaires intérieures	HANKISS Ágnes (PPE)	23/11/2011

Commission européenne

DG de la Commission	Commissaire
Réseaux de communication, contenu et technologies	KROES Neelie

Evénements clés

Date	Evénement	Référence	Résumé
31/03/2011	Publication du document de base non-législatif	COM(2011)0163	Résumé
17/11/2011	Annonce en plénière de la saisine de la commission		
08/05/2012	Vote en commission		
16/05/2012	Dépôt du rapport de la commission	A7-0167/2012	Résumé
11/06/2012	Débat en plénière		
12/06/2012	Décision du Parlement	T7-0237/2012	Résumé
12/06/2012	Résultat du vote au parlement		
12/06/2012	Fin de la procédure au Parlement		

Informations techniques

Référence de la procédure	2011/2284(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d'initiative
Base juridique	Règlement du Parlement EP 55
État de la procédure	Procédure terminée
Dossier de la commission	ITRE/7/06163

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE474.017	07/02/2012	
Amendements déposés en commission		PE483.516	06/03/2012	
Avis de la commission	LIBE	PE480.619	22/03/2012	
Rapport déposé de la commission, lecture unique		A7-0167/2012	16/05/2012	Résumé
Texte adopté du Parlement, lecture unique		T7-0237/2012	12/06/2012	Résumé

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base non législatif	COM(2011)0163	31/03/2011	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2012)626	30/10/2012	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	PT_PARLIAMENT	COM(2011)0163	10/05/2012	

Protection des infrastructures d'information critiques: réalisations et prochaines étapes: vers une cybersécurité mondiale

2011/2284(INI) - 31/03/2011 - Document de base non législatif

OBJECTIF : présenter un 1er bilan du plan d'action sur la protection des infrastructures d'information critiques et proposer un cadre d'action renouvelé pour les années à venir dans ce domaine.

CONTEXTE : la Commission a publié, le 30 mars 2009, une communication relative à la protection des infrastructures d'information critiques 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 plan de préparation, de mesures de sécurité et d'une capacité de résilience d'un niveau élevé. Ce plan d'action s'articulait autour des 5 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.

Parallèlement, la stratégie numérique pour l'Europe, adoptée en mai 2010, 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.

Pour compléter ce texte, la Commission a présenté en parallèle une proposition 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 améliorer la sécurité des réseaux, mais aussi prévenir, détecter et combattre les problèmes de cybersécurité.

La présente communication récapitule les résultats obtenus depuis l'adoption du plan d'action PIIC en 2009 et 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.

CONTENU : la communication identifie tout d'abord les risques potentiels qui peuvent atteindre gravement la sécurité des grands réseaux informatiques :

1. **des risques d'exploitation**, comme dans le cas des «menaces persistantes avancées» à des fins d'espionnage économique et politique (GhostNet, par exemple), ou le vol d'identité,…
2. **des risques 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) ;
3. **des risques de destruction** non encore réellement identifiés à ce jour mais à prendre en compte.

Pour contrer ces risques, la Commission a mis en œuvre pas mal d'actions dont les points saillants peuvent se résumer comme suit :

1) Préparation et prévention :

- création d'un Forum où les États membres peuvent échanger des bonnes pratiques dans le domaine des infrastructures d'information critiques ;
- création d'un partenariat public-privé européen pour la résilience (EP3R) en vue d'encourager la coopération public/privé sur des questions stratégiques de politique de l'UE en matière de sécurité et de résilience ;
- création d'un réseau de CERT rassemblant tous les États membres d'ici à 2012 qui servira de pierre angulaire à un futur système européen de partage d'informations et d'alerte (SEPIA) pour les particuliers et les PME.

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).

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. Le 1er 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 et de la Suisse, la Norvège et l'Islande. L'objectif est maintenant de créer des exercices paneuropéens disposant d'un cadre commun.

4) Coopération internationale : la Commission va examiner les principes existants 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, etc.

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. 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 en 2012.

Prochaines étapes : face aux défis qui se posent au niveau mondial, 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. 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 ;
- 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 avec le CERT. La création 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. 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** car cette technologie est essentielle pour qu'il soit possible d'exploiter pleinement les avantages de cette technologie.

Les États membres sont également appelés à :

- améliorer l'état de préparation de l'UE en mettant en place un réseau de CERT nationales/gouvernementales opérationnelles d'ici à 2012. Ces activités permettront 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. 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 ;
- 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, applicable à la stabilité et à la résilience mondiales de l'internet.

Á noter qu'une annexe à la communication présente un état des lieux précis de toutes les actions menées dans le cadre du Plan d'action PIIC ainsi que des prochaines étapes dans le cadre de ce dernier.

Protection des infrastructures d'information critiques: réalisations et prochaines étapes: vers une cybersécurité mondiale

2011/2284(INI) - 16/05/2012 - Rapport déposé de la commission, lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport d'initiative d'Ivailo KALFIN (S&D, BG) sur la protection des infrastructures d'information critiques - Réalisations et prochaines étapes: vers une cybersécurité mondiale.

Les députés rappellent que l'internet et les technologies de l'information et de la communication (TIC) sont des moteurs essentiels d'interaction sociale, d'enrichissement culturel et de croissance économique. Un niveau adéquat de sécurité de l'information est toutefois essentiel pour une forte expansion des services basés sur l'internet. C'est la raison pour laquelle les députés proposent un projet de résolution proposant un cadre de protection à trois niveaux, national, européen et international, qui se décline comme suit :

1) Mesures de renforcement de la PIIC au niveau national et européen : les députés saluent la mise en œuvre, par les États membres, du programme européen de protection des infrastructures d'information critiques qui comprend notamment la mise en place du réseau d'alerte concernant les infrastructures critiques (CIWIN). Ce programme permettra non seulement d'améliorer la sécurité générale des citoyens, mais renforcera le sentiment de sécurité et la confiance dans les mesures prises.

Ils demandent toutefois le renforcement des mesures existantes, via :

- l'extension du champ d'application de la directive 2008/114/CE du Conseil en vue d'y inclure le secteur des TIC et les services financiers mais aussi le domaine de la santé, les systèmes d'approvisionnement en eau et en nourriture, la recherche et l'industrie nucléaires ;
- le renforcement de l'excellence européenne dans le domaine de la protection des infrastructures d'information critiques ;

- la mise à jour des normes minimales de résilience des infrastructures d'information critiques contre toute perturbation, incident ou tentatives de destruction ou d'attaque ;
- le renforcement de la coopération entre les acteurs publics et privés au niveau de l'Union en vue de développer et de mettre en œuvre des normes de sécurité et de résilience pour les infrastructures d'information critiques civiles nationales et européennes ;
- la multiplication des exercices paneuropéens de préparation aux incidents de grande envergure.

Parallèlement, les députés invitent la Commission, en coopération avec les États membres à : i) évaluer la mise en œuvre du plan d'action pour la PIIC ; ii) établir des stratégies nationales de cybersécurité ; iii) **organiser des simulations d'incidents informatiques nationales et paneuropéennes**, iv) **développer des plans d'intervention nationaux en cas d'incident informatique** et contribuer au développement d'un **plan d'intervention européen en cas d'incident informatique d'ici à la fin 2012**. Ils demandent en particulier la mise en place de plans de sûreté pour les exploitants ou de mesures équivalentes pour toutes les infrastructures d'information critiques européennes, ainsi que la désignation de correspondants pour la sécurité dans les États membres.

2) Autres activités de l'Union pour une sécurité de l'internet forte : estimant que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pouvait jouer un rôle clé, au niveau européen, dans la protection des infrastructures d'information critiques, les députés invitent cette agence à coordonner et à mettre en œuvre annuellement les **"mois européens de la sensibilisation à la cybersécurité**" afin d'attirer particulièrement l'attention des États membres et des citoyens européens sur ce type de problème. Soutenant globalement les activités menées par cette agence, les députés invitent également l'ENISA à consulter les acteurs concernés afin de définir des mesures en matière de cybersécurité pour les propriétaires et gestionnaires de réseaux ainsi qu'à aider la Commission et les États membres à contribuer au développement et à l'adoption de régimes de certification de la sécurité de l'information, de normes de comportement et de pratiques de coopération entre les CERT (équipes d'intervention en cas d'urgence informatique) nationales et européennes et les propriétaires et gestionnaires d'infrastructures, si nécessaire, grâce à la **formulation d'exigences communes minimales neutres** sur le plan technologique.

L'ENISA est également appelée à :

- gérer de nouvelles tâches d'exécution au niveau de l'UE, en coopération avec ses homologues américains, en matière de prévention et de détection des incidents de sécurité des réseaux et de l'information (en particulier, dans le cadre de la révision du règlement instituant l'ENISA) ;
- obtenir de nouvelles responsabilités en matière de réaction aux attaques sur l'internet ;
- maintenir les exercices qu'elle a menés en 2010 et en 2011, à son ordre du jour et y associer progressivement les opérateurs privés.

Pour contrer toute attaque des infrastructures informatiques critiques, les députés proposent que les États membres mettent en place **des plans d'intervention nationaux** en matière d'incidents informatiques incluant des dispositions sur l'assistance, l'endiguement et la réparation en cas de perturbations ou d'attaques informatiques de portée régionale, nationale ou transnationale. Ils devraient en outre coordonner leurs actions entre eux et rendre leurs actions plus cohérentes.

Au plan européen, la Commission est également appelée à :

- prévoir **un plan d'urgence européen en cas d'incident informatique** incluant des mesures contraignantes en matière de coordination, au niveau de l'Union, des fonctions techniques et de pilotage des CERT nationales et gouvernementales ;
- prendre, avec les États membres, les mesures nécessaires pour protéger les infrastructures critiques contre les cyberattaques et prévoir des mécanismes pour bloquer hermétiquement l'accès à une infrastructure dès qu'une cyberattaque se profile ;
- proposer des mesures contraignantes visant à imposer des **normes minimales de sécurité et de résilience** et améliorer la coordination entre les **équipes nationales d'intervention d'urgence** en matière de sécurité informatique.

En ce qui concerne les CERT, les députés demandent que celles-ci soient fonctionnelles, dotées de capacités minimales de sécurité et de résilience basées sur les bonnes pratiques reconnues. Ils demandent en outre l'établissement **d'un service de PIIC 24 heures sur 24 et 7 jours sur 7** pour chaque État membre, ainsi que la création d'un **protocole européen commun d'urgence** applicable à tous les points de contacts nationaux.

Pour une approche commune : dans le cadre de l'approche européenne de réaction, les députés invitent la Commission à proposer une procédure conjointe de définition et de désignation d'une approche commune permettant de répondre aux menaces informatiques transfrontalières. Ils saluent dès lors l'initiative de la Commission relative à l'élaboration d'un **système européen de partage d'informations et d'alerte d'ici 2013**.

Les députés saluent le travail de consultation effectué par la Commission pour renforcer le dialogue avec les fournisseurs de services informatiques. Ils suggèrent maintenant à la Commission de lancer une **initiative publique paneuropéenne en matière d'éducation**, axée sur l'éducation et la sensibilisation des utilisateurs finaux, privés et commerciaux, et sur les menaces potentielles sur l'internet et les appareils TIC fixes et mobiles à chaque niveau de la chaîne d'utilisation. Ils soutiennent également la création d'un programme de cours européen destiné aux experts universitaires dans le domaine de la sécurité de l'information.

Pour une stratégie européenne de cybersécurité : les députés invitent la Commission à proposer d'ici la fin 2012 une **stratégie détaillée en matière de sécurité de l'internet pour l'Union**, reposant sur une terminologie claire ayant pour objectif la création d'un cyberespace (soutenu par une infrastructure sûre et résiliente et des normes ouvertes) propice à l'innovation et à la prospérité par la libre transmission d'informations, tout en assurant une **protection forte de la vie privée et d'autres libertés civiles**. Cette stratégie devrait détailler les principes, les objectifs, les méthodes, les instruments et les politiques (internes et externes) nécessaires à la rationalisation des efforts nationaux et européens, et établir des normes minimales de résilience dans les États membres. La stratégie devrait en outre prendre comme point de référence principal les travaux réalisés dans le domaine de la protection des infrastructures d'information critiques et prévoir tant des mesures volontaristes, telles que l'introduction de normes minimales pour les mesures de sécurité que des mesures réactives, telles que des **sanctions pénales, civiles et administratives**. Les députés demandent également que la Commission présente une **proposition législative punissant davantage les cyberattaques** (harponnage, fraude en ligne, etc.).

En ce qui concerne **la coordination des mesures nationales**, les députés demandent que le mécanisme de coordination soit doté d'experts et de ressources administratives et financières suffisantes.

Ils demandent également :

- la mise en place par la Commission d'un cadre européen pour la notification des violations de la sécurité dans les secteurs critiques, notamment les secteurs de l'énergie, des transports, de l'approvisionnement en eau et en nourriture mais aussi pour les TIC et les services financiers ;
- la disponibilité de données statistiquement représentatives concernant les coûts des attaques informatiques dans l'Union, les États membres et l'industrie ;
- des mesures destinées à éviter d'entraver la croissance de l'économie européenne sur l'internet et la prévision d'incitants pour exploiter pleinement le potentiel des partenariats entre les entreprises et entre secteurs public et privé dans ce domaine.

3) Coopération internationale : les députés rappellent que la coopération internationale est l'instrument principal pour l'introduction de mesures efficaces en matière de cybersécurité. Or, à l'heure actuelle, l'Union européenne n'est pas engagée activement dans les processus de coopération internationale et dans les dialogues relatifs à la cybersécurité. Les députés appellent dès lors la Commission et le service européen pour l'action extérieure (SEAE) à entamer un dialogue constructif avec les pays dont les opinions convergent afin de développer une interprétation uniforme et des politiques visant à renforcer la résilience de l'internet et des infrastructures critiques.

Les députés demandent également :

- l'inclusion des problèmes de sécurité de l'internet dans ses relations extérieures, y compris dans les accords avec les pays tiers ;
- la coordination des actions menées par les États membres et l'UE avec les diverses institutions, organes et agences internationales afin d'éviter les doubles emplois.

Saluant la création, lors du sommet UE-États-Unis, du groupe conjoint sur la cybersécurité et la cybercriminalité ainsi que d'un programme commun et d'une feuille de route en vue d'organiser des exercices transcontinentaux communs ou synchronisés dans le domaine de la cybersécurité en 2012 /2013, les députés appellent à un **dialogue structuré entre les législateurs européens et américains** afin de discuter des problèmes liés à l'internet dans le cadre de la recherche d'une compréhension et d'une interprétation uniformes et de positions communes.

Ils invitent enfin le SEAE, la Commission et l'ENISA à défendre une position active dans les forums internationaux pertinents, notamment en coordonnant les positions des États membres afin de promouvoir les valeurs, les politiques et les objectifs essentiels de l'Union européenne en matière de sécurité et de résilience de l'internet au sein d'agences comme l'OTAN, l'ONU, la Société pour l'attribution des noms de domaine sur internet, l'OSCE, l'OCDE,…

Protection des infrastructures d'information critiques: réalisations et prochaines étapes: vers une cybersécurité mondiale

2011/2284(INI) - 12/06/2012 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 573 voix pour, 90 voix contre et 26 abstentions, une résolution sur la protection des infrastructures d'information critiques - Réalisations et prochaines étapes: vers une cybersécurité mondiale.

Le Parlement considère que les technologies de l'information et de la communication (TIC) ne peuvent pleinement favoriser l'économie et la société que si les utilisateurs ont confiance en leur sécurité et leur résilience, et si la législation en vigueur en matière notamment de confidentialité des données et de droits de propriété intellectuelle est appliquée efficacement dans l'environnement internet. Il rappelle que l'internet et les TIC sont des moteurs essentiels d'interaction sociale, d'enrichissement culturel et de croissance économique. Un niveau adéquat de sécurité de l'information est toutefois essentiel pour une forte expansion des services basés sur l'internet. C'est la raison pour laquelle la résolution propose un cadre de protection à trois niveaux, national, européen et international, qui se décline comme suit :

1) Mesures de renforcement de la PIIC au niveau national et européen : le Parlement salue la mise en œuvre, par les États membres, du programme européen de protection des infrastructures d'information critiques qui comprend notamment la mise en place du réseau d'alerte concernant les infrastructures critiques (CIWIN). Ce programme permettra non seulement d'améliorer la sécurité générale des citoyens, mais renforcera le sentiment de sécurité et la confiance dans les mesures prises.

Il demande toutefois le renforcement des mesures existantes, via :

- l'extension du champ d'application de la directive 2008/114/CE du Conseil en vue d'y inclure le secteur des TIC et les services financiers mais aussi le domaine de la santé, les systèmes d'approvisionnement en eau et en nourriture, la recherche et l'industrie nucléaires;
- le renforcement de l'excellence européenne dans le domaine de la protection des infrastructures d'information critiques ;
- la mise à jour des normes minimales de résilience des infrastructures d'information critiques contre toute perturbation, incident ou tentatives de destruction ou d'attaque ;
- le renforcement de la coopération entre les acteurs publics et privés au niveau de l'Union en vue de développer et de mettre en œuvre des normes de sécurité et de résilience pour les infrastructures d'information critiques civiles nationales et européennes.

Parallèlement, le Parlement invite la Commission, en coopération avec les États membres à : i) évaluer la mise en œuvre du plan d'action pour la PIIC ; ii) établir des stratégies nationales de cybersécurité ; iii) **organiser des simulations d'incidents informatiques nationales et paneuropéennes**, iv) **développer des plans d'intervention nationaux en cas d'incident informatique** et contribuer au développement d'un **plan d'intervention européen en cas d'incident informatique d'ici à la fin 2012**. Il demande en particulier la mise en place de plans de sûreté pour les exploitants ou de mesures équivalentes pour toutes les infrastructures d'information critiques européennes, ainsi que la désignation de correspondants pour la sécurité dans les États membres.

2) Autres activités de l'Union pour une sécurité de l'internet forte : estimant que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pouvait jouer un rôle clé, au niveau européen, dans la protection des infrastructures d'information critiques, le Parlement invite cette agence à coordonner et à mettre en œuvre annuellement les **"mois européens de la sensibilisation à la cybersécurité**" afin d'attirer particulièrement l'attention des États membres et des citoyens européens sur ce type de problème. Soutenant globalement les activités menées par cette agence, le Parlement invite également l'ENISA à consulter les acteurs concernés afin de définir des mesures en matière de cybersécurité pour les propriétaires et gestionnaires de réseaux ainsi qu'à aider la Commission et les États membres à contribuer au développement et à l'adoption de régimes de certification de la sécurité de l'information, de normes de comportement et de pratiques de coopération entre les CERT (équipes d'intervention en cas d'urgence informatique) nationales et européennes et les propriétaires et gestionnaires d'infrastructures, si nécessaire, grâce à la **formulation d'exigences communes minimales neutres** sur le plan technologique.

L'ENISA est également appelée à :

- **gérer de nouvelles tâches d'exécution au niveau de l'UE**, en coopération avec ses homologues américains, en matière de prévention et de détection des incidents de sécurité des réseaux et de l'information (en particulier, dans le cadre de la révision du règlement instituant l'ENISA) ;
- se voir attribuer des responsabilités supplémentaires en matière de réaction aux attaques sur l'internet dans la mesure où elle apporte une valeur ajoutée claire aux mécanismes de réaction nationaux existants ;
- maintenir les exercices qu'elle a menés en 2010 et en 2011, à son ordre du jour et y associer progressivement les opérateurs privés.

Pour contrer toute attaque des infrastructures informatiques critiques, le Parlement propose que les États membres mettent en place **des plans d'intervention nationaux** en matière d'incidents informatiques incluant des dispositions sur l'assistance, l'endiguement et la réparation en cas de perturbations ou d'attaques informatiques de portée régionale, nationale ou transnationale. Il devrait en outre coordonner leurs actions entre eux et rendre leurs actions plus cohérentes.

Réaction européenne aux cybertattaques : le Parlement constate que les données disponibles relatives à la cybercriminalité des services répressifs (couvrant les cyberattaques, mais aussi d'autres types de délits en ligne) indiquent de fortes hausses dans différents pays européens. Toutefois, les données statistiques des services répressifs et de la CERT (équipe d'intervention d'urgence en matière de sécurité informatique) concernant les cyberattaques **restent rares** et devraient être mieux collectées à l'avenir, ce qui permettra de meilleures réponses des services répressifs dans l'UE et une meilleure définition des réponses législatives face aux menaces informatiques en perpétuelle évolution. Le Parlement appelle dès lors la Commission à :

- prévoir **un plan d'urgence européen en cas d'incident informatique** incluant des mesures contraignantes en matière de coordination, au niveau de l'Union, des fonctions techniques et de pilotage des CERT nationales et gouvernementales ;
- prendre, avec les États membres, les mesures nécessaires pour protéger les infrastructures critiques contre les cyberattaques et prévoir des mécanismes pour bloquer hermétiquement l'accès à une infrastructure dès qu'une cyberattaque se profile ;
- proposer des mesures contraignantes visant à imposer des **normes minimales de sécurité et de résilience** et améliorer la coordination entre les **équipes nationales d'intervention d'urgence** en matière de sécurité informatique.

En ce qui concerne les CERT, le Parlement demande que celles-ci soient fonctionnelles, dotées de capacités minimales de sécurité et de résilience basées sur les bonnes pratiques reconnues. Il demande en outre l'établissement **d'un service de PIIC 24 heures sur 24 et 7 jours sur 7** pour chaque État membre, ainsi que la création d'un **protocole européen commun d'urgence** applicable à tous les points de contacts nationaux.

Pour une approche commune : dans le cadre de l'approche européenne de réaction, le Parlement invite la Commission à proposer une procédure conjointe de définition et de désignation d'une approche commune permettant de répondre aux menaces informatiques transfrontalières. Il salue dès lors l'initiative de la Commission relative à l'élaboration d'un **système européen de partage d'informations et d'alerte d'ici 2013**.

Le Parlement salue le travail de consultation effectué par la Commission pour renforcer le dialogue avec les fournisseurs de services informatiques. Á cet égard, il salue les diverses **consultations de parties prenantes** concernant la sécurité sur l'internet et la PIIC lancées par la Commission, comme le Partenariat public-privé européen pour la résilience. Reconnaissant la participation et l'engagement, déjà importants, des fournisseurs de TIC dans ces actions, le Parlement invite la Commission à poursuivre ses efforts visant à encourager les universités et les associations d'utilisateurs de TIC à jouer un rôle plus actif et à favoriser un dialogue pluripartite constructif sur les problèmes de cybersécurité. Il suggère à la Commission de lancer une **initiative publique paneuropéenne en matière d'éducation**, axée sur l'éducation et la sensibilisation des utilisateurs finaux, privés et commerciaux, et sur les menaces potentielles sur l'internet et les appareils TIC fixes et mobiles à chaque niveau de la chaîne d'utilisation. Il soutient également la création d'un programme de cours européen destiné aux experts universitaires dans le domaine de la sécurité de l'information.

Pour une stratégie européenne de cybersécurité : le Parlement invite la Commission à proposer d'ici la fin 2012 une **stratégie détaillée en matière de sécurité de l'internet pour l'Union**, reposant sur une terminologie claire ayant pour objectif la création d'un cyberespace (soutenu par une infrastructure sûre et résiliente et des normes ouvertes) propice à l'innovation et à la prospérité par la libre transmission d'informations, tout en assurant une **protection forte de la vie privée et d'autres libertés civiles**. Cette stratégie devrait détailler les principes, les objectifs, les méthodes, les instruments et les politiques (internes et externes) nécessaires à la rationalisation des efforts nationaux et européens, et établir des normes minimales de résilience dans les États membres. La stratégie devrait en outre prendre comme point de référence principal, les travaux réalisés dans le domaine de la protection des infrastructures d'information critiques et prévoir tant des mesures volontaristes, telles que l'introduction de normes minimales pour les mesures de sécurité que des mesures réactives, telles que des **sanctions pénales, civiles et administratives**. Le Parlement demande également que la Commission présente une **proposition législative punissant davantage les cyberattaques** (harponnage, fraude en ligne, etc.).

En ce qui concerne **la coordination des mesures nationales**, le Parlement demande que le mécanisme de coordination soit doté d'experts et de ressources administratives et financières suffisantes.

Il demande également :

- la mise en place par la Commission d'un cadre européen pour la notification des violations de la sécurité dans les secteurs critiques, notamment les secteurs de l'énergie, des transports, de l'approvisionnement en eau et en nourriture mais aussi pour les TIC et les services financiers ;
- la disponibilité de données statistiquement représentatives concernant les coûts des attaques informatiques dans l'Union, les États membres et l'industrie ;
- des mesures destinées à éviter d'entraver la croissance de l'économie européenne sur l'internet et la prévision d'incitants pour exploiter pleinement le potentiel des partenariats entre les entreprises et entre secteurs public et privé dans ce domaine.

L'ensemble de ces mesures ne doivent toutefois aller à l'encontre de certains droits. Le Parlement européen rappelle à cet égard qu'il a insisté à maintes reprises sur l'application de normes élevées en matière de vie privée et de protection des données, de neutralité de l'internet et de protection des droits de propriété intellectuelle.

3) Coopération internationale : le Parlement rappelle que la coopération internationale est l'instrument principal pour l'introduction de mesures efficaces en matière de cybersécurité. Or, à l'heure actuelle, l'Union européenne n'est pas engagée activement dans les processus de coopération internationale et dans les dialogues relatifs à la cybersécurité. Il appelle dès lors la Commission et le service européen pour l'action extérieure (SEAE) à entamer un dialogue constructif avec les pays dont les opinions convergent afin de développer une interprétation uniforme et des politiques visant à renforcer la résilience de l'internet et des infrastructures critiques.

Le Parlement demande également :

- l'inclusion des problèmes de sécurité de l'internet dans ses relations extérieures, y compris dans les accords avec les pays tiers ;
- la coordination des actions menées par les États membres et l'UE avec les diverses institutions, organes et agences internationales afin d' éviter les doubles emplois.

Saluant la création, lors du sommet UE-États-Unis, du groupe conjoint sur la cybersécurité et la cybercriminalité ainsi que d'un programme commun et d'une feuille de route en vue d'organiser des exercices transcontinentaux communs ou synchronisés dans le domaine de la cybersécurité en 2012 /2013, le Parlement appelle à un **dialogue structuré entre les législateurs européens et américains** afin de discuter des problèmes liés à l'internet dans le cadre de la recherche d'une compréhension et d'une interprétation uniformes et de positions communes.

Il invite enfin le SEAE, la Commission et l'ENISA à défendre une position active dans les forums internationaux pertinents, notamment en coordonnant les positions des États membres afin de promouvoir les valeurs, les politiques et les objectifs essentiels de l'Union européenne en matière de sécurité et de résilience de l'internet au sein d'agences comme l'OTAN, l'ONU, la Société pour l'attribution des noms de domaine sur internet, l'OSCE, l'OCDE, …