**Mardi 12 juin 2012**

65. attire l'attention sur la nécessité de promouvoir le volontariat, en particulier pendant l'Année européenne des citoyens en 2013, et invite la Commission à inclure le soutien au volontariat dans les politiques internationales d'aide au développement, en particulier afin d'atteindre tous les objectifs du Millénaire pour le développement;

66. est favorable à un examen formel de la proposition Solidarité de programme interinstitutionnel en matière de ressources humaines dans les institutions de l'Union afin de faciliter la participation du personnel et des stagiaires des institutions aux activités humanitaires et sociales de volontariat, à travers la formation du personnel et sur leur temps libre;

67. souligne que le programme proposé permet de réduire les coûts et d'apporter une forte valeur ajoutée, et contribuerait à la mise en œuvre des politiques et programmes de l'Union;

68. recommande à la Commission de maintenir les points de contact utiles mis en place avec l'"Alliance pour l'année européenne du volontariat 2011" et avec la plateforme du volontariat qui lui a succédé, qui réunissent de nombreuses organisations de volontariat et des réseaux de la société civile, et avec les organes nationaux de coordination, partenaires stratégiques et porte-parole des gouvernements nationaux dans ce domaine, compte tenu de la grande variété d'entités responsables du volontariat dans l'Union, et encourage ces points de contact à s'engager en faveur de la proposition de portail européen centralisé, en tant que plateforme européenne, en vue de faciliter le renforcement de la coordination et une activité transfrontalière accrue;

69. souligne l'importance de ces réseaux de contacts et de l'échange de bonnes pratiques pour diffuser l'information sur les dispositifs existants au sein de l'Union susceptibles d'aider et d'accompagner les projets de volontariat transfrontalier;

70. demande à la Commission de prendre des mesures, quand elle le juge opportun, concernant l'agenda politique pour le volontariat en Europe, élaboré par les organisations de volontariat réunies au sein de l'Alliance pour l'année européenne du volontariat 2011;

71. charge son Président de transmettre la présente résolution au Conseil, à la Commission ainsi qu'aux gouvernements et aux parlements des États membres.

---

## Protection des infrastructures d'information critiques: vers une cybersécurité mondiale

P7_TA(2012)0237

**Résolution du Parlement européen du 12 juin 2012 sur la protection des infrastructures d'information critiques - Réalisations et prochaines étapes: vers une cybersécurité mondiale (2011/2284(INI))**

(2013/C 332 E/03)

*Le Parlement européen,*

— vu sa résolution du 5 mai 2010 intitulée «Un nouvel agenda numérique pour l'Europe: 2015.eu» [1],

— vu sa résolution du 15 juin 2010 intitulée "La gouvernance de l'internet: les prochaines étapes" [2],

— vu sa résolution du 6 juillet 2011 intitulée "Le haut débit en Europe: investir dans une croissance induite par le numérique" [3],

— vu l'article 48 de son règlement,

— vu le rapport de la commission de l'industrie, de la recherche et de l'énergie et l'avis de la commission des libertés civiles, de la justice et des affaires intérieures (A7-0167/2012),

[1] JO C 81 E du 15.3.2011, p. 45.
[2] JO C 236 E du 12.8.2011, p. 33.
[3] Textes adoptés de cette date, P7_TA(2011)0322.

A. considérant 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;

B. considérant que l'internet et les technologies de l'information et de la communication (TIC) renforcent rapidement leur incidence sur divers aspects de la vie des citoyens et qu'ils sont des moteurs essentiels d'interaction sociale, d'enrichissement culturel et de croissance économique;

C. considérant que la sécurité des TIC et de l'internet est un concept global, qui a une incidence mondiale, dans ses aspects économiques, sociaux, technologiques et militaires, exigeant une définition et une différentiation claires des responsabilités ainsi qu'un mécanisme solide de coopération internationale;

D. considérant que l'initiative phare de l'agenda numérique de l'UE vise à stimuler la compétitivité de l'Europe en renforçant les TIC et à créer les conditions nécessaires pour une croissance élevée et solide et des emplois basés sur la technologie;

E. considérant que le secteur privé demeure le premier investisseur, propriétaire et gestionnaire de produits, services, applications et infrastructures en matière de sécurité de l'information, en ayant investi des milliards d'euros ces dix dernières années; considérant que cette participation devrait être renforcée grâce à des stratégies politiques appropriées visant à soutenir la résilience des infrastructures détenues ou gérées par le secteur public, privé ou public-privé;

F. considérant que la mise au point de réseaux, de services et de technologies TIC à haut niveau de sécurité et de résilience accroîtra la compétitivité de l'économie européenne, aussi bien en améliorant l'évaluation et la gestion des risques informatiques qu'en dotant l'économie de l'UE au sens large d'infrastructures d'information plus solides afin de soutenir l'innovation et la croissance, en créant de nouvelles possibilités pour les entreprises de gagner en productivité;

G. considérant que les données disponibles relatives à la cybercriminalité des services répressifs (couvrant les cyberattaques, mais aussi d'autres types de délits en ligne) semblent indiquer de fortes hausses dans différents pays européens; considérant toutefois que 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;

H. considérant qu'un niveau adéquat de sécurité de l'information est essentiel pour une forte expansion des services basés sur l'internet;

I. considérant que les récents incidents, perturbations et attaques informatiques à l'encontre des infrastructures d'information des institutions européennes, de l'industrie et des États membres démontrent la nécessité de mettre en place un système innovant, efficace et solide de protection des infrastructures d'information critiques (PIIC) reposant sur une totale coopération internationale et des normes minimales de résilience dans les États membres;

J. considérant que le développement rapide de nouveaux modes de TIC, tels que l'informatique en nuage, requiert de placer la sécurité au centre des préoccupations afin de pouvoir pleinement engranger les bénéfices des réalisations technologiques;

K. considérant que le Parlement européen 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;

***Mesures de renforcement de la PIIC au niveau national et européen***

1. 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);

2. estime que les efforts réalisés dans le cadre de la PIIC non seulement amélioreront la sécurité générale des citoyens, mais renforceront également leur sentiment de sécurité et leur confiance dans les mesures adoptées par les pouvoirs publics pour les protéger;

**Mardi 12 juin 2012**

3. note que la Commission envisage la révision de la directive 2008/114/CE du Conseil [1] et demande des preuves de l'efficacité et de l'incidence de la directive avant que d'autres mesures ne soient adoptées; demande que soit envisagée l'extension de son champ d'application, notamment en y incluant le secteur des TIC et les services financiers; demande également qu'il soit tenu compte de domaines comme la santé, les systèmes d'approvisionnement en eau et en nourriture, la recherche et l'industrie nucléaires (lorsque ces domaines ne sont pas couverts par des dispositions particulières); considère que ces secteurs devraient également bénéficier de l'approche intersectorielle adoptée par le CIWIN (consistant en une coopération, un système d'alerte et l'échange de bonnes pratiques);

4. souligne combien il est important de mettre en place et de garantir une intégration durable de la recherche européenne pour maintenir et améliorer l'excellence européenne dans le domaine de la protection des infrastructures d'information critiques;

5. demande, étant donné la nature interconnectée et hautement interdépendante, sensible, stratégique et vulnérable des infrastructures d'information critiques nationales et européennes, la mise à jour régulière des normes minimales de résilience en matière de préparation et de réaction en cas de perturbations, d'incidents, de tentatives de destructions ou d'attaques, tels que ceux résultant d'infrastructures insuffisamment solides ou de terminaux finaux insuffisamment sécurisés;

6. souligne l'importance des normes et des protocoles de sécurité informatique et salue le mandat conféré en 2011 au CEN, au Cenelec et à l'ETSI pour l'établissement de normes de sécurité;

7. compte sur les propriétaires et les gestionnaires d'infrastructures d'information critiques pour permettre aux utilisateurs d'utiliser et, si nécessaire, les aider à utiliser, les moyens appropriés pour les protéger face aux attaques malveillantes et/ou perturbations, par un contrôle à la fois humain et automatique, si besoin est;

8. soutient la coopération entre les acteurs publics et privés au niveau de l'Union, et encourage leurs efforts 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 (qu'elles soient publiques, privées ou publiques-privées);

9. souligne l'importance que revêtent les exercices paneuropéens dans la préparation aux incidents de grande envergure affectant la sécurité des réseaux ainsi que la définition d'un ensemble unique de normes relatives à l'évaluation de la menace;

10. invite la Commission, en coopération avec les États membres, à évaluer la mise en œuvre du plan d'action pour la PIIC; invite instamment les États membres à établir des CERT nationales/gouvernementales fonctionnelles, à développer des stratégies nationales de cybersécurité, à organiser des simulations d'incidents informatiques nationales et paneuropéennes, à développer des plans d'intervention nationaux en cas d'incident informatique et à contribuer au développement d'un plan d'intervention européen en cas d'incident informatique d'ici à la fin 2012;

11. recommande 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;

12. se félicite du réexamen en cours de la décision-cadre 2005/222/JAI du Conseil [2] relative aux attaques visant les systèmes d'information; prend acte de la nécessité de coordonner les efforts de l'UE en matière de lutte contre les cyberattaques, en incluant l'ENISA, les CERT des États membres et les compétences de la future CERT européenne;

13. estime que l'ENISA peut jouer un rôle clé, au niveau européen, dans la protection des infrastructures d'information critiques, en fournissant des conseils techniques aux États membres et aux institutions et organes de l'Union européenne et en présentant des rapports et des analyses sur la situation en matière de sécurité des systèmes d'information aux niveaux européen et mondial;

***Autres activités de l'Union pour une sécurité de l'internet forte***

14. invite instamment l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) 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 les problèmes liés à la cybersécurité;

[1] JO L 345 du 23.12.2008, p. 75.
[2] JO L 69 du 16.3.2005, p. 67.

15. soutient l'ENISA, conformément aux objectifs de l'agenda numérique, dans l'exercice de ses missions relatives à la sécurité des réseaux d'information, en particulier en fournissant des orientations et en conseillant les États membres sur la manière de respecter les capacités de base de leurs CERT, ainsi qu'en soutenant l'échange de bonnes pratiques par le développement d'un environnement de confiance; invite l'Agence à consulter les acteurs concernés afin de définir des mesures similaires en matière de cybersécurité pour les propriétaires et gestionnaires de réseaux et d'infrastructures privés, 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 nationales et européennes et les propriétaires et gestionnaires d'infrastructures, si nécessaire, par la formulation d'exigences communes minimales neutres sur le plan technologique;

16. salue la proposition actuelle de révision du mandat de l'ENISA, en particulier concernant son extension et le développement de ses missions; estime qu'outre l' aide apportée aux États membres au travers de son expertise et de son analyse, l'ENISA devrait être autorisée à gérer plusieurs tâches d'exécution au niveau de l'UE, et en coopération avec ses homologues américains, des tâches liées à la prévention et à la détection des incidents de sécurité des réseaux et de l'information et améliorant la coopération entre les États membres; souligne qu'en vertu du règlement instituant l'ENISA, l'Agence pourrait également 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;

17. salue les résultats des exercices paneuropéens de cybersécurité 2010 et 2011, menés dans toute l'Union et supervisés par l'ENISA, dont l'objectif était d'aider les États membres à concevoir, maintenir et tester un plan d'intervention paneuropéen; invite l'ENISA à maintenir ces exercices à son ordre du jour et à y associer progressivement les opérateurs privés concernés afin d'accroître les capacités globales de l'Europe en matière de sécurité de l'internet; compte sur une expansion internationale accrue auprès de partenaires partageant la même vision;

18. invite les États membres à mettre en place des plans d'intervention nationaux en matière d'incidents informatiques, à inclure des éléments essentiels, tels que les points de contact pertinents, des dispositions concernant l'assistance, l'endiguement et la réparation en cas de perturbations ou d'attaques informatiques de portée régionale, nationale ou transnationale; indique que les États membres devraient également mettre en place des mécanismes et structures de coordination appropriés au niveau national afin de permettre une meilleure coordination entre les autorités nationales compétentes et de rendre leurs actions plus cohérentes;

19. suggère que la Commission propose, au moyen du plan d'urgence européen en cas d'incident informatique, des mesures contraignantes pour une meilleure coordination, au niveau de l'Union, des fonctions techniques et de pilotage des CERT nationales et gouvernementales;

20. invite la Commission et les États membres à prendre les mesures nécessaires pour protéger les infrastructures critiques contre les cyberattaques et à prévoir des mécanismes pour bloquer hermétiquement l'accès à une infrastructure critique dès qu'une cyberattaque directe en menace sérieusement le bon fonctionnement;

21. attend avec impatience la mise en œuvre complète de la CERT-UE, qui sera un facteur essentiel dans la prévention, la détection, la réponse et la réparation en cas de cyberattaques intentionnelles et malveillantes ciblant les institutions de l'Union;

22. recommande que la Commission propose des mesures contraignantes visant à imposer des normes minimales de sécurité et de résilience et à améliorer la coordination entre les équipes nationales d'intervention d'urgence en matière de sécurité informatique;

23. invite les États membres et les institutions de l'Union à garantir l'existence de CERT fonctionnelles, dotées de capacités minimales de sécurité et de résilience basées sur les bonnes pratiques reconnues; souligne que les CERT nationales devraient faire partie d'un réseau efficace dans lequel les informations pertinentes sont échangées conformément aux normes de confidentialité nécessaires; demande 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 entre les points de contacts nationaux;

24. rappelle que le renforcement de la confiance et l'incitation à la coopération entre les États membres sont essentiels pour protéger les données et les réseaux et infrastructures nationaux; invite la Commission à proposer une procédure conjointe de définition et de désignation d'une approche commune permettant de répondre aux menaces informatiques transfrontalières, et attend des États membres qu'ils fournissent à la Commission des informations générales concernant les risques, les menaces et les vulnérabilités de leurs infrastructures d'information critiques;

25. salue l'initiative de la Commission relative à l'élaboration d'un système européen de partage d'informations et d'alerte d'ici 2013;

26. 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; reconnaît la participation et l'engagement, déjà importants, des fournisseurs de TIC dans ces actions, 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; soutient le développement de l'Assemblée numérique en tant que cadre de gouvernance de la PIIC;

27. salue le travail accompli jusqu'ici par le Forum européen des États membres en matière d'établissement de critères sectoriels spécifiques pour répertorier les infrastructures critiques européennes, en mettant l'accent sur les communications fixe et mobile, ainsi que dans les discussions relatives aux orientations et aux principes européens concernant la résilience et la stabilité sur l'internet; entend poursuivre l'établissement du consensus entre les États membres et, dans ce contexte, encourage le forum à compléter l'approche actuelle axée sur les avantages physiques par des efforts visant à englober également les avantages d'infrastructures logiques qui, à mesure que les technologies de virtualisation et de nuages évoluent, deviendront de plus en plus importantes pour l'efficacité de la PIIC;

28. 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, aux menaces potentielles sur l'internet et les appareils TIC fixes et mobiles à chaque niveau de la chaîne d'utilisation et d'encourager des comportements individuels en ligne plus sûrs; rappelle, à cet égard, les risques liés aux équipements et logiciels informatiques obsolètes;

29. invite les États membres, avec le soutien de la Commission, à renforcer les programmes de formation et d'éducation sur la sécurité de l'information, destinés aux services répressifs et aux pouvoirs judiciaires nationaux ainsi qu'aux agences de l'Union concernées;

30. est favorable à la création d'un programme de cours européen destiné aux experts universitaires dans le domaine de la sécurité de l'information, étant donné qu'un tel programme aurait une incidence positive sur l'expertise et le degré de préparation de l'Union en ce qui concerne le cyberespace, en perpétuelle évolution, et les menaces auxquelles il est exposé;

31. recommande d'encourager l'éducation à la cybersécurité (stages de doctorat, cours universitaires, ateliers, formation des étudiants, etc.) et la mise en place d'exercices spécialisés de formation à la PIIC;

32. 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; estime que la stratégie en matière de sécurité de l'internet devrait avoir 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; maintient que 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, afin de garantir un service sûr, continu, solide et résilient, qu'il s'agisse des infrastructures critiques ou de l'utilisation générale de l'internet;

33. souligne que la prochaine "stratégie en matière de sécurité de l'internet" de la Commission devrait prendre comme point de référence principal les travaux réalisés dans le domaine de la protection des infrastructures d'information critiques et viser une approche globale et systématique de la cybersécurité en prévoyant tant des mesures volontaristes, telles que l'introduction de normes minimales pour les mesures de sécurité ou la sensibilisation des utilisateurs individuels, des entreprises et des institutions publiques, que des mesures réactives, telles que des sanctions pénales, civiles et administratives;

34. invite instamment la Commission à proposer un mécanisme solide destiné à coordonner la mise en œuvre et les mises à jour régulières de la stratégie de sécurité de l'internet; estime que ce mécanisme devrait être doté de suffisamment d'experts et de ressources administratives et financières et être compétent pour faciliter l'élaboration des positions de l'UE dans les relations avec les parties prenantes internes et internationales sur les questions relatives à la sécurité de l'internet;

35. invite la Commission à proposer 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 les secteurs des TIC et des services financiers, afin d'informer les autorités des États membres concernés et les utilisateurs des incidents, des attaques et des perturbations informatiques;

36. invite instamment la Commission à améliorer la disponibilité des données statistiquement représentatives concernant les coûts des attaques informatiques dans l'Union, les États membres et l'industrie (en particulier les secteurs des services financiers et des TIC) en améliorant les capacités de collecte de données du centre européen de la cybercriminalité prévu pour 2013, des CERT et d'autres initiatives de la Commission comme le système européen de partage d'informations et d'alerte (SEPIA), afin de garantir la communication et le partage systématiques des données relatives aux attaques informatiques et aux autres formes de criminalité informatique qui touchent l'industrie européenne et les États membres, et de renforcer ainsi les services répressifs;

37. recommande l'instauration d'une relation étroite et la création d'une interaction entre les secteurs privés au niveau national et l'ENISA pour assurer une liaison entre les CERT nationales et gouvernementales et l'évolution du système européen de partage d'informations et d'alerte (EISAS);

38. souligne que l'industrie des TIC est le principal moteur de l'élaboration et de l'utilisation de technologies visant à renforcer la sécurité de l'internet; rappelle que les politiques européennes doivent éviter d'entraver la croissance de l'économie européenne sur l'internet et comporter les incitations nécessaires pour exploiter pleinement le potentiel des partenariats entre les entreprises et entre secteurs public et privé; recommande d'explorer des mesures d'incitation supplémentaires permettant à l'industrie d'élaborer des plans de sécurité d'opérateur plus solides conformément à la directive 2008/114/CE;

39. invite la Commission à présenter une proposition législative punissant davantage les cyberattaques (harponnage, fraude en ligne, etc.);

***Coopération internationale***

40. rappelle que la coopération internationale est l'instrument principal pour l'introduction de mesures efficaces en matière de cybersécurité; reconnaît qu'à l'heure actuelle, l'Union européenne n'est pas engagée activement, sur une base régulière, dans les processus de coopération internationale et dans les dialogues relatifs à la cybersécurité; invite 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; maintient dans le même temps que l'Union européenne devrait également, de manière permanente, inclure les problèmes de sécurité de l'internet dans ses relations extérieures, notamment lors de l'élaboration de différents instruments financiers ou lorsqu'elle s'engage dans des accords internationaux prévoyant l'échange et le stockage de données sensibles;

41. prend acte des réalisations positives de la convention du Conseil de l'Europe sur la cybercriminalité, qui s'est tenue à Budapest en 2001; souligne toutefois que tout en encourageant davantage de pays à signer et à ratifier la convention, le SEAE devrait également élaborer des accords bilatéraux et multilatéraux sur la sécurité et la résilience de l'internet avec les partenaires internationaux partageant la même vision;

42. souligne que le grand nombre d'activités menées actuellement par diverses institutions, organes et agences internationales et de l'Union européenne, ainsi que par plusieurs États membres, doivent être coordonnées afin d'éviter tout effet de double emploi et qu'à ce titre, il convient d'envisager de désigner un responsable officiel chargé de la coordination, éventuellement au moyen de la nomination d'un coordinateur européen de la cybersécurité;

43. souligne l'importance d'un dialogue structuré entre les principaux acteurs et législateurs européens et américains engagés dans la protection des infrastructures d'information critiques pour garantir une compréhension, une interprétation et une position communes en ce qui concerne les cadres juridiques et administratifs.

44. salue la création, lors du sommet UE - États-Unis de novembre 2010, du groupe conjoint UE - États-Unis sur la cybersécurité et la cybercriminalité et soutient les efforts qu'il consent afin d'inclure les questions de sécurité de l'internet dans le dialogue politique transatlantique; salue la mise en place conjointe, par la Commission et le gouvernement américain, sous l'égide du groupe de travail UE-États-Unis, 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;

45. suggère l'instauration d'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;

46. invite le SEAE et la Commission, sur la base du travail réalisé par le Forum européen des États membres, 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; note que ces forums sont notamment l'OTAN, l'ONU (en particulier au sein de l'Union internationale des télécommunications et du Forum sur la gouvernance de l'internet), la Société pour l'attribution des noms de domaine et des numéros sur internet, l'Internet Assigned Numbers Authority (l'autorité chargée de la gestion de l'adressage sur l'internet), l'OSCE, l'OCDE et la Banque mondiale;

47. encourage la Commission et l'ENISA à participer aux principaux dialogues des parties prenantes visant à définir les normes techniques et juridiques dans le cyberespace au niveau international;

*

* *

48. charge son président de transmettre la présente résolution au Conseil et à la Commission.

---

## Coopération avec des partenaires au-delà de nos frontières en matière de politique énergétique

P7_TA(2012)0238

**Résolution du Parlement européen du 12 juin 2012 - "S'investir dans la coopération avec des partenaires au-delà de nos frontières en matière de politique énergétique: une approche stratégique d'un approvisionnement énergétique sûr, durable et compétitif" (2012/2029(INI))**

(2013/C 332 E/04)

*Le Parlement européen,*

— vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée "Sécurité de l'approvisionnement énergétique et coopération internationale. Politique énergétique de l'UE: s'investir avec des partenaires au-delà de nos frontières" (COM(2011)0539),

— vu la proposition de décision de la Commission au Parlement européen et au Conseil établissant un mécanisme d'échange d'informations sur les accords intergouvernementaux conclus entre des États membres et des pays tiers dans le domaine de l'énergie (COM(2011)0540),

— vu les conclusions du Conseil du 24 novembre 2011, intitulées "La sécurité de l'approvisionnement énergétique et la coopération internationale - «La politique énergétique de l'UE: s'investir avec des partenaires au-delà de nos frontières» ",

— vu sa résolution du 25 novembre 2010 sur le thème "Vers une nouvelle stratégie énergétique pour l'Europe pour la période 2011-2020" ([1]),

— vu l'article 48 de son règlement,

— vu le rapport de la commission de l'industrie, de la recherche et de l'énergie et les avis de la commission des affaires étrangères, de la commission du développement et de la commission du commerce international (A7-0168/2012),

([1]) JO C 99 E du 3.4.2012, p 64.