Jeudi 12 septembre 2013

4. demande à la Commission d'aider les États membres à réduire les écarts de rémunération d'au moins cinq points de pourcentage par an dans l'objectif d'éliminer les disparités de rémunération entre les hommes et les femmes d'ici à 2020;

5. reconnaît que, pour adopter une approche à plusieurs niveaux et plusieurs volets, il y a lieu que la Commission soutienne les États membres dans la promotion des bonnes pratiques et la mise en œuvre de politiques de réduction de l'écart de rémunération entre les hommes et les femmes;

6. demande instamment à la Commission de réexaminer, sans tarder, la directive 2006/54/CE et de proposer des modifications conformément à l'article 32 de la directive et sur la base de l'article 157 du traité sur le fonctionnement de l'Union européenne, suivant les recommandations détaillées en annexe de la résolution du Parlement du 24 mai 2012;

7. charge son Président de transmettre la présente résolution au Conseil, à la Commission et aux gouvernements des États membres.

P7_TA(2013)0376

Stratégie de cybersécurité de l'UE: un cyberespace ouvert, sûr et sécurisé

Résolution du Parlement européen du 12 septembre 2013 sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé (2013/2606(RSP))

(2016/C 093/16)

Le Parlement européen,

— vu la communication conjointe du 7 février 2013 de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» (JOIN(2013)0001),

— vu la proposition de directive du Parlement européen et du Conseil du 7 février 2013 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (COM(2013)0048),

— vu la communication de la Commission du 19 mai 2010 intitulée «Une stratégie numérique pour l'Europe» (COM(2010) 0245) et la communication de la Commission du 18 décembre 2012 intitulée «Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne» (COM(2012)0784),

— vu la communication de la Commission du 27 septembre 2012 intitulée «Exploiter le potentiel de l'informatique en nuage en Europe»(COM(2012)0529),

— vu la communication de la Commission du 28 mars 2012 intitulée «Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité» (COM(2012)0140) et les conclusions du Conseil du 7 juin 2012 y afférentes,

— vu la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil ([1]),

— vu la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection ([2]),

---

([1]) JO L 218 du 14.8.2013, p. 8.
([2]) JO L 345 du 23.12.2008, p. 75.

— vu la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil ([1]),

— vu le programme de Stockholm ([2]) en matière de liberté, de sécurité et de justice, la communication de la Commission intitulée «Mettre en place un espace de liberté, de sécurité et de justice au service des citoyens européens: plan d'action mettant en œuvre le programme de Stockholm» (COM(2010)0171), la communication de la Commission intitulée «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre» (COM(2010)0673) et sa résolution du 22 mai 2012 sur la stratégie de sécurité intérieure de l'Union européenne ([3]),

— vu la proposition conjointe de la Commission et de la haute représentante en vue d'une décision du Conseil concernant les modalités de mise en œuvre par l'Union de la clause de solidarité (JOIN(2012)0039),

— vu la décision-cadre 2001/413/JAI du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces ([4]),

— vu sa résolution du 12 juin 2012 sur la protection des infrastructures d'information critiques — réalisations et prochaines étapes: vers une cybersécurité mondiale ([5]) et les conclusions du Conseil du 27 mai 2011 sur la communication de la Commission relative à la protection des infrastructures d'information critiques — «Réalisations et prochaines étapes: vers une cybersécurité mondiale» (COM(2011)0163),

— vu sa résolution du 11 décembre 2012 sur l'achèvement du marché unique numérique ([6]),

— vu sa résolution du 22 novembre 2012 sur la sécurité et la défense du cyberespace ([7]),

— vu sa position arrêtée en première lecture le 16 avril 2013 sur la proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) (COM(2010) 0521) ([8]),

— vu sa résolution du 11 décembre 2012 sur une stratégie pour la liberté numérique dans la politique étrangère de l'Union ([9]),

— vu la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001,

— vu les obligations internationales de l'Union, notamment au titre de l'accord général sur le commerce des services (GATS),

— vu l'article 16 du traité sur le fonctionnement de l'Union européenne (traité FUE) et la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 6, 8 et 11,

— vu les négociations en cours entre l'Union européenne et les États-Unis d'Amérique au sujet du partenariat transatlantique de commerce et d'investissement,

— vu l'article 110, paragraphe 2, de son règlement,

A. considérant que les défis croissants qui se posent en matière de cybersécurité en raison des menaces et des attaques toujours plus sophistiquées mettent gravement en péril la sécurité, la stabilité et la prospérité économique non seulement des États membres, mais aussi du secteur privé et de la population dans son ensemble; que, par conséquent, la protection de notre société et de notre économie constituera un défi en constante évolution;

([1]) JO L 335 du 17.12.2011, p. 1.
([2]) JO C 115 du 4.5.2010, p. 1.
([3]) Textes adoptés de cette date, P7_TA(2012)0207.
([4]) JO L 149 du 2.6.2001, p. 1.
([5]) Textes adoptés de cette date, P7_TA(2012)0237.
([6]) Textes adoptés de cette date, P7_TA(2012)0468.
([7]) Textes adoptés de cette date, P7_TA(2012)0457.
([8]) Textes adoptés de cette date, P7_TA(2013)0103.
([9]) Textes adoptés de cette date, P7_TA(2012)0470.

Jeudi 12 septembre 2013

B. considérant qu'il y a lieu de faire du cyberespace et de la cybersécurité l'un des piliers essentiels des stratégies de sécurité et de défense de l'Union et de chacun des États membres; qu'il est primordial de veiller à ce que le cyberespace demeure ouvert à la libre circulation des idées et des informations, ainsi qu'à la liberté d'expression;

C. considérant que le commerce électronique et les services en ligne constituent une force vitale de l'internet et sont cruciaux pour atteindre les objectifs de la stratégie Europe 2020, et qu'ils procurent des avantages aussi bien aux citoyens qu'au secteur privé; que l'Union doit exploiter pleinement le potentiel et les possibilités offerts par l'internet en ce qui concerne le développement du marché unique, notamment le marché unique du numérique;

D. considérant que les priorités stratégiques énoncées dans la communication conjointe relative à la stratégie de cybersécurité de l'Union européenne comprennent notamment la cyber-résilience, la réduction de la cybercriminalité, le développement d'une politique et des moyens de cyberdéfense en relation avec la politique de sécurité et de défense commune (PSDC) et l'instauration d'une politique internationale de l'Union cohérente en matière de cyberespace;

E. considérant que les réseaux et les systèmes d'information sur tout le territoire de l'Union présentent un degré élevé d'interconnexion; considérant, au vu du caractère planétaire de l'internet, que bon nombre d'incidents de sécurité des réseaux et de l'information transcendent les frontières nationales et sont susceptibles d'entraver le fonctionnement du marché unique et d'entamer la confiance des consommateurs dans le marché unique du numérique;

F. considérant que la cybersécurité au sein de l'Union, comme dans le reste du monde, comporte des failles et que les perturbations rencontrées dans un secteur ou un État membre se répercutent sur d'autres secteurs ou États membres, ce qui génère un effet d'entraînement ayant des conséquences pour l'ensemble de l'économie de l'Union;

G. considérant qu'en avril 2013, seuls 13 États membres avaient officiellement adopté une stratégie nationale en matière de cybersécurité; que des différences fondamentales subsistent entre les États membres en ce qui concerne la préparation, la sécurité, la culture stratégique et la capacité à élaborer et à mettre en œuvre des stratégies nationales de cybersécurité, et qu'il y a lieu d'effectuer une analyse de ces différences;

H. considérant que les différences culturelles en matière de sécurité et l'absence d'un cadre juridique contribuent à la fragmentation du marché unique du numérique et constituent un problème à traiter en priorité; que l'absence d'une approche harmonisée en matière de cybersécurité constitue une menace grave pour la prospérité économique et la sécurité des transactions, et que les gouvernements, le secteur privé ainsi que les organes répressifs et de renseignement devraient par conséquent conjuguer leurs efforts et coopérer plus étroitement;

I. considérant que la cybercriminalité est un fléau international dont le coût est en constante augmentation, celui-ci s'élevant actuellement, selon les estimations de l'Office des Nations unies contre la drogue et le crime, à un montant annuel de 295 milliards d'euros;

J. considérant que la criminalité organisée internationale, tirant parti des avancées technologiques, continue d'élargir son champ d'action au cyberespace et que la cybercriminalité transforme radicalement la structure traditionnelle des groupes criminels organisés; considérant que la criminalité organisée est dès lors moins circonscrite à un territoire et plus à même d'exploiter la territorialité ainsi que des juridictions nationales différentes à l'échelle internationale;

K. considérant que, dans le cadre de leurs enquêtes sur la cybercriminalité, les autorités compétentes se heurtent toujours à de nombreux obstacles, tels que le recours, lors des transactions dans le cyberespace, à des «devises virtuelles» qui peuvent être utilisées pour blanchir de l'argent, les problèmes de territorialité et de limites entre juridictions, des possibilités limitées en matière de partage d'informations, le manque de formation du personnel, ainsi qu'une coopération insuffisante avec les autres parties prenantes;

L. considérant que le développement du cyberespace repose sur la technologie et qu'une adaptation constante aux évolutions technologiques est essentielle pour améliorer la résilience et la sécurité du cyberespace de l'Union; considérant qu'il y a lieu de prendre des mesures pour veiller à ce que la législation soit adaptée aux dernières avancées technologiques afin que les cybercriminels soient identifiés et poursuivis de manière efficace et que les victimes de cybercriminalité soient protégées; que la stratégie de l'Union en matière de cybersécurité doit inclure des mesures axéee

sur la sensibilisation, l'éducation, la constitution d'équipes d'intervention en cas d'urgence informatique (CERT), le développement d'un marché intérieur pour les produits et services du domaine de la cybersécurité, et la promotion des investissements dans la recherche, le développement et l'innovation;

1. se félicite de la communication conjointe relative à la stratégie de cybersécurité de l'Union européenne et de la proposition de directive concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union;

2. souligne l'importance considérable et croissante que revêtent l'internet et le cyberespace pour les échanges politiques, économiques et sociétaux, non seulement au sein de l'Union, mais aussi dans le cadre des relations avec d'autres acteurs du monde entier;

3. souligne qu'il est essentiel d'élaborer une politique de communication stratégique sur la cybersécurité de l'Union, les situations de cybercrise, les repositionnements stratégiques, la collaboration entre le secteur public et le secteur privé et les alertes, ainsi que des recommandations à l'intention du public;

4. rappelle que le niveau de sécurité des réseaux et de l'information doit être élevé, non seulement pour conserver des services qui sont indispensables au bon fonctionnement de la société et de l'économie, mais aussi pour préserver l'intégrité physique des citoyens en améliorant l'efficacité, l'efficience et le fonctionnement sûr des infrastructures critiques; souligne que, si la sécurité des réseaux et de l'information doit être assurée, il y a lieu aussi d'améliorer la sécurité physique; souligne que les infrastructures doivent être protégées contre les perturbations volontaires et involontaires; insiste dès lors sur le fait que, s'agissant de la stratégie de cybersécurité, l'accent devrait être mis sur les causes courantes de dysfonctionnement involontaire des systèmes;

5. appelle de nouveau les États membres à adopter, dans les meilleurs délais, des stratégies nationales de cybersécurité qui couvrent les aspects techniques, de coordination, de ressources humaines et d'allocations financières, et qui comprennent des règles spécifiques sur les avantages et les responsabilités du secteur privé, dans le but d'assurer la participation de ce dernier, ainsi qu'à prévoir des procédures complètes de gestion des risques et à préserver le cadre réglementaire;

6. fait remarquer que seules la prise de décisions et l'appropriation politique de la part des institutions de l'Union et des États membres permettront d'atteindre un niveau élevé de sécurité des réseaux et de l'information au sein de l'Union et d'assurer ainsi le fonctionnement sûr et sans encombre du marché unique;

7. souligne que la stratégie de l'Union en matière de cybersécurité devrait fournir un environnement numérique sûr et fiable ayant comme fondements et comme objectifs la protection et la préservation des libertés et le respect des droits fondamentaux en ligne, notamment les droits au respect de la vie privée et à la protection des données, conformément à la Charte des droits fondamentaux de l'Union européenne et à l'article 16 du traité sur le fonctionnement de l'Union européenne; estime qu'une attention particulière doit être accordée à la protection des enfants en ligne;

8. invite les États membres et la Commission à prendre toutes les mesures qui s'imposent afin d'élaborer des programmes de formation visant à promouvoir et à améliorer la sensibilisation, les compétences et la formation des citoyens européens, notamment en ce qui concerne la sécurité personnelle, dans le cadre d'un programme d'études dans le domaine des compétences numériques applicable dès le plus jeune âge; se félicite du projet de mois européen de la cybersécurité, avec le soutien de l'ENISA et en coopération avec les autorités publiques et le secteur privé, dans le but de sensibiliser davantage aux défis inhérents à la protection des réseaux et des systèmes d'information;

9. estime que la formation à la cybersécurité sensibilise la société européenne aux menaces liées à l'internet et favorise ainsi une utilisation responsable du cyberespace, tout en encourageant le développement des compétences relatives à l'internet; reconnaît qu'Europol et son nouveau Centre européen de lutte contre la cybercriminalité (EC3), ainsi que l'ENISA et Eurojust, jouent un rôle essentiel dans l'organisation d'activités de formation au niveau de l'Union en ce qui concerne l'utilisation des outils de coopération judiciaire internationale et l'application de la législation portant sur divers aspects de la cybercriminalité;

10. réaffirme qu'il est nécessaire de fournir des conseils techniques et des informations juridiques ainsi que de concevoir des programmes sur la prévention de la cybercriminalité et la lutte contre celle-ci; encourage la formation des ingénieurs informatiques spécialisés dans la protection des infrastructures critiques et des systèmes d'information, ainsi que des opérateurs des systèmes de commande pour le transport et des centres de gestion du trafic; souligne le besoin urgent de mettre en place des programmes réguliers de formation à la cybersécurité à l'intention du personnel du secteur public, et ce à tous les niveaux;

Jeudi 12 septembre 2013

11. appelle de nouveau à faire preuve d'une grande prudence dans l'application de restrictions à la capacité des citoyens à faire usage des outils des technologies de l'information et de la communication et souligne que les États membres devraient s'efforcer de ne jamais compromettre les droits et les libertés de leurs citoyens lorsqu'ils élaborent des réponses aux menaces et aux attaques informatiques, et que leur législation devrait permettre d'opérer une distinction entre les incidents informatiques civils et militaires;

12. estime que l'intervention réglementaire dans le domaine de la cybersécurité devrait être orientée sur les risques, axée sur les infrastructures critiques, dont le bon fonctionnement constitue un intérêt public majeur, et devrait se fonder sur les mesures axées sur le marché prises actuellement par le secteur pour garantir la résilience des réseaux; souligne le rôle fondamental que joue la coopération au niveau opérationnel pour stimuler l'amélioration des échanges d'informations relatives aux menaces informatiques entre les autorités publiques et le secteur privé — à la fois à l'échelle de l'Union et à l'échelle nationale, ainsi qu'avec les partenaires stratégiques de l'Union — dans le but d'assurer la sécurité des réseaux et de l'information en instaurant un climat de confiance mutuelle, de partage des valeurs et d'engagement, et en partageant leur expertise; estime que les partenariats public-privé devraient être fondés sur la neutralité des réseaux et des technologies, et devraient être axés sur les mesures à prendre pour régler les problèmes ayant une grande incidence sur le public; demande à la Commission d'inviter tous les opérateurs du marché concernés à se montrer plus vigilants et à coopérer davantage afin d'aider les autres opérateurs à protéger leurs services;

13. reconnaît que la détection et la notification des incidents de cybersécurité sont essentielles pour favoriser la cyber-résilience au sein de l'Union; estime que des exigences proportionnées et nécessaires en matière de divulgation devraient être mises en place afin de permettre la notification aux autorités nationales compétentes des incidents dus à des manquements significatifs à la sécurité et, par la même, d'améliorer le suivi des cas de cybercriminalité et de faciliter les efforts de sensibilisation menés à tous les niveaux;

14. invite la Commission et les autres acteurs à prendre des mesures de cybersécurité et de cyber-résilience qui incluent des incitations économiques visant à promouvoir des niveaux élevés de cybersécurité et de cyber-résilience;

Cyber-résilience

15. note que les différents secteurs et les États membres ne disposent pas des mêmes moyens et compétences, ce qui entrave le développement d'une coopération basée sur la confiance et nuit au bon fonctionnement du marché unique;

16. estime que les exigences imposées aux petites et moyennes entreprises devraient relever d'une approche proportionnée et axée sur les risques;

17. insiste sur le développement de la cyber-résilience pour les infrastructures critiques et rappelle que les futures modalités de mise en œuvre de la clause de solidarité (article 222 du traité FUE) devraient tenir compte des risques d'attaques informatiques contre les États membres; invite la Commission et la haute représentante à prendre ces risques en considération dans leurs rapports conjoints d'évaluation intégrée des menaces et des risques, attendus à partir de 2015;

18. souligne qu'afin de garantir l'intégrité, la disponibilité et la confidentialité des services critiques en particulier, il y a lieu de maintenir à jour l'identification et la catégorisation des infrastructures critiques et de définir les exigences minimales de sécurité pour leurs réseaux et leurs systèmes d'information;

19. reconnaît que la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union prévoit de telles exigences minimales en matière de sécurité applicables aux prestataires de services de la société de l'information et aux opérateurs d'infrastructures critiques;

20. invite les États membres et l'Union à instaurer des cadres adéquats pour la mise en place de systèmes d'échanges d'informations qui garantissent l'anonymat au secteur privé tout en fournissant au secteur public des informations constamment mises à jour et, le cas échéant, à fournir une assistance au secteur privé;

21. se félicite de l'idée émise par la Commission d'adopter une culture de gestion des risques en matière de cybersécurité et prie instamment les États membres et les institutions de l'Union d'inclure sans délai la gestion des crises informatiques dans leurs stratégies de gestion des risques et leurs analyses de risques; invite en outre les gouvernements des États membres et la Commission à encourager les acteurs du secteur privé à inclure la gestion des crises informatiques dans leurs stratégies de gestion et leurs analyses de risques, ainsi qu'à former leur personnel à la cybersécurité;

22. prie tous les États membres et les institutions de l'Union de mettre en place un réseau d'équipes d'intervention en cas d'urgence informatique (CERT) qui soient efficaces et opérationnelles 24 heures sur 24, sept jours sur sept; souligne que les CERT nationales devraient faire partie d'un réseau efficace dans lequel les informations pertinentes sont échangées conformément aux normes de confiance et de confidentialité nécessaires; note que les initiatives à composantes multiples réunissant les CERT et d'autres organes de sécurité concernés peuvent s'avérer des instruments utiles pour instaurer un climat de confiance dans un contexte transfrontalier ou intersectoriel; reconnaît le caractère essentiel d'une coopération efficace et efficiente entre les CERT et les organes chargés de l'application des lois dans la lutte contre la cybercriminalité;

23. soutient l'ENISA dans l'exercice de ses fonctions en ce qui concerne la sécurité des réseaux et de l'information, notamment en fournissant des indications et des conseils aux États membres, ainsi qu'en favorisant l'échange de bonnes pratiques et l'instauration d'un climat de confiance;

24. souligne que les entreprises doivent mettre en œuvre les exigences appropriées de performance en matière de cybersécurité d'un bout à l'autre de la chaîne de valeur des produits TIC utilisés dans les réseaux de transport et les systèmes d'information, procéder à une gestion appropriée des risques, adopter des normes et des solutions de sécurité, d'élaborer de bonnes pratiques et développer le partage d'informations en vue d'assurer une protection solide des systèmes de transport;

Ressources industrielles et technologiques

25. estime qu'un niveau élevé de sécurité des réseaux et de l'information est essentiel pour accroître la compétitivité à la fois des fournisseurs et des utilisateurs des solutions en matière de sécurité au sein de l'Union; considère que si la filière de la sécurité informatique de l'Union recèle un potentiel inexploité, les utilisateurs des secteurs privé et public ainsi que les entreprises ne sont souvent pas informés du coût et des avantages que représentent les investissements dans la cybersécurité et demeurent par conséquent vulnérables face aux menaces informatiques préjudiciables; souligne que la mise en place des CERT est une mesure pertinente à cet égard;

26. estime que pour proposer une offre abondante de solutions en matière de cybersécurité et générer une forte demande, les autorités nationales concernées par les TIC doivent investir de manière appropriée dans les ressources universitaires, la recherche et le développement et l'acquisition de connaissances et de capacités afin d'encourager les innovations et de sensibiliser suffisamment aux risques de sécurité liés aux réseaux et à l'information, de sorte que le secteur européen de la sécurité coopère plus étroitement;

27. invite les institutions de l'Union et les États membres à prendre les mesures qui s'imposent pour instaurer un «marché unique de la cybersécurité» au sein duquel les utilisateurs et les fournisseurs pourraient tirer le meilleur parti des innovations, des synergies et des expertises combinées, et auquel les PME auraient accès;

28. invite les États membres à envisager des investissements conjoints dans la filière européenne de la cybersécurité, à l'image de ce qui a été fait dans d'autres secteurs, comme celui de l'aviation;

Cybercriminalité

29. estime que les activités criminelles dans le cyberespace peuvent nuire autant au bien-être de la société que les crimes et délits commis dans le monde physique, et que ces différentes formes de méfaits se renforcent souvent mutuellement, par exemple dans le cas de l'exploitation sexuelle des enfants ou de la criminalité organisée et du blanchiment d'argent;

30. note qu'il existe parfois un lien entre les activités commerciales légitimes et illicites; souligne l'importance du lien, facilité par l'internet, entre le financement du terrorisme et la grande criminalité organisée; souligne que le public doit être informé du fait que l'implication dans des actes de cybercriminalité constitue une infraction grave, et qu'un délit qui peut sembler a priori anodin, tel que le téléchargement illégal de films, rapporte souvent beaucoup d'argent aux organisations criminelles internationales;

Jeudi 12 septembre 2013

31. convient avec la Commission que les normes et les principes applicables hors ligne le sont aussi en ligne et que, dès lors, la lutte contre la cybercriminalité doit être renforcée au moyen d'une législation actualisée et de nouvelles capacités opérationnelles;

32. estime qu'étant donné la nature transfrontalière de la cybercriminalité, il est essentiel d'accomplir des efforts conjoints et de procéder à des échanges d'expertise à l'échelle de l'Union, au-delà du niveau national, et qu'Eurojust, l'EC3 d'Europol, les CERT ainsi que les universités et les centres de recherche doivent disposer des ressources et des capacités adéquates pour remplir correctement leur rôle de pôles d'expertise, de coopération et de partage d'informations;

33. se félicite vivement de la création de l'EC3 et encourage le futur développement de cette agence et le rôle crucial qu'elle joue en coordonnant l'échange transfrontalier en temps utile et efficace d'informations et d'expertise en vue de soutenir la prévention et la détection de la cybercriminalité ainsi que les enquêtes en la matière;

34. invite les États membres à veiller à ce que les citoyens puissent accéder facilement aux informations sur les menaces informatiques et sur les moyens d'y faire face; estime que ces conseils devraient inclure des informations sur la façon dont les utilisateurs peuvent protéger leur vie privée sur l'internet, sur les moyens de détecter et de révéler des cas de manipulation psychologique, sur l'installation des logiciels et des pare-feux, sur la gestion des mots de passe et sur la détection des fausses identités («phishing»), des dévoiements («pharming») et d'autres attaques;

35. enjoint les États membres qui n'ont pas encore ratifié la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest) de le faire le plus rapidement possible; se félicite que le Conseil de l'Europe envisage d'adapter ladite convention aux évolutions technologiques afin qu'elle puisse continuer à lutter efficacement contre la cybercriminalité, et invite la Commission et les États membres à prendre part aux discussions; soutient les efforts en faveur de la ratification de la convention par les pays tiers et invite la Commission à la promouvoir activement en dehors de l'Union;

Cyberdéfense

36. souligne que les défis, les menaces et les attaques informatiques mettent en péril la défense et la sécurité nationale des États membres, et que les stratégies civile et militaire de protection des infrastructures critiques devraient toutes deux être optimisées au moyen d'efforts permettant de créer des synergies;

37. invite dès lors les États membres à coopérer davantage avec l'Agence européenne de défense (AED) afin d'élaborer des propositions et des initiatives en matière de capacités de cyberdéfense fondées sur des initiatives et des projets récents; souligne qu'il est nécessaire d'intensifier la recherche et le développement, notamment par la mise en commun et l'échange ressources;

38. rappelle que si l'Union veut mettre au point une stratégie complète de cybersécurité, elle doit tenir compte de la valeur ajoutée des agences et des organes existants, ainsi que des bonnes pratiques fournies par les États membres qui appliquent déjà leurs propres stratégies nationales de cybersécurité;

39. invite la vice-présidente de la Commission/haute représentante de l'Union à inclure la gestion des crises informatiques dans la planification de la gestion des crises et souligne que les États membres doivent élaborer des plans en coopération avec l'AED afin de protéger les missions et les opérations de la politique de sécurité et de défense commune (PSDC) contre les cyberattaques; invite ceux-ci à mettre en place une force européenne de cyberdéfense;

40. souligne la bonne coopération opérationnelle avec l'OTAN dans le domaine de la cybersécurité et la nécessité de renforcer cette coopération, notamment grâce à une meilleure coordination en ce qui concerne la planification, les technologies, la formation et l'équipement;

41. prie l'Union de s'employer, dans la mesure du possible, à pratiquer des échanges avec les partenaires internationaux, notamment l'OTAN, à recenser les domaines de coopération, à éviter les doubles emplois et à compléter les activités;

Politique internationale

42. estime que la coopération et le dialogue à l'échelle internationale jouent un rôle primordial dans l'instauration d'un climat de confiance et de transparence et dans la promotion d'un niveau élevé de coopération en réseau et d'échange d'informations au niveau mondial; invite dès lors la Commission et le Service européen pour l'action extérieure (SEAE) à mettre sur pied une équipe de cyberdiplomatie chargée de favoriser le dialogue avec les pays et les organisations partageant les mêmes convictions; invite l'Union à participer de manière plus active aux diverses conférences internationales de haut niveau sur la cybersécurité;

43. estime qu'il y a lieu de parvenir à un équilibre entre les objectifs concurrents de transfert de données entre pays, de protection des données et de cybersécurité, conformément aux obligations internationales de l'Union, notamment au titre du GATS;

44. invite la vice-présidente de la Commission/haute représentante de l'Union à intégrer la dimension de la cybersécurité dans la politique extérieure de l'Union, notamment dans le cadre des relations avec les pays tiers, afin de renforcer la coopération, ainsi que les échanges d'expériences et d'informations, sur la façon de gérer la cybersécurité;

45. prie l'Union de s'employer, dans la mesure du possible, à pratiquer des échanges avec les partenaires internationaux afin de recenser les domaines de coopération, d'éviter les doubles emplois et de compléter les activités; invite la vice-présidente de la Commission/haute représentante de l'Union à se montrer proactive au sein des organisations internationales et à coordonner les positions des États membres sur la façon de promouvoir efficacement des stratégies et des solutions en matière de cybersécurité;

46. estime que des efforts devraient être accomplis pour s'assurer que les instruments juridiques internationaux existants, notamment la convention du Conseil de l'Europe sur la cybercriminalité, soient mis en œuvre dans le cyberespace; juge par conséquent qu'il n'est pour l'heure pas nécessaire de créer de nouveaux instruments juridiques au niveau international; se félicite toutefois de la coopération internationale visant à élaborer des normes de comportement dans le cyberespace, lesquelles soutiennent l'état de droit dans le cyberespace; considère qu'il y a lieu d'envisager une mise à jour des instruments juridiques en vigueur afin que ceux-ci reflètent les avancées technologiques; est d'avis que les questions juridictionnelles requièrent un débat approfondi sur la coopération et les poursuites judiciaires dans les affaires de criminalité transnationale;

47. estime notamment que le groupe de travail Union européenne — États-Unis sur la cybersécurité et la cybercriminalité devrait permettre à l'Union et aux États-Unis d'échanger, dans la mesure du possible, les bonnes pratiques en matière de cybersécurité; fait remarquer, à cet égard, que les domaines relatifs à la cybersécurité, tels que les services dépendant du bon fonctionnement des systèmes de réseaux et d'information, seront inclus dans les négociations à venir sur le partenariat transatlantique de commerce et d'investissement (TTIP), à conclure de manière à préserver la souveraineté de l'Union et l'indépendance de ses institutions;

48. note que les compétences en matière de cybersécurité et la capacité à prévenir, à détecter et à contrer efficacement les menaces et les attaques malveillantes ne sont pas développées de la même manière dans tous les pays du globe; souligne que les efforts produits en vue d'accroître la cyber-résilience et de parer aux menaces informatiques ne doivent pas se limiter aux partenaires partageant des convictions similaires, mais qu'ils doivent aussi s'étendre à des régions dont les capacités, les infrastructures techniques et les cadres juridiques sont moins développés; estime que la coordination des CERT est primordiale à cet égard; prie la Commission de faciliter et, en cas de nécessité, de soutenir, à l'aide des moyens appropriés, les efforts entrepris par les pays tiers pour se doter de leurs propres capacités dans le domaine de la cybersécurité;

Mise en œuvre

49. demande des évaluations régulières de l'efficacité des stratégies de cybersécurité nationales au plus haut niveau politique, afin de s'assurer qu'elles soient adaptées aux nouvelles menaces internationales et de garantir le même niveau de cybersécurité dans l'ensemble des États membres;

50. invite la Commission à élaborer une feuille de route claire présentant le calendrier des objectifs à accomplir au niveau de l'Union au titre de la stratégie de cybersécurité et des évaluations de cette dernière; demande aux États membres de convenir d'un calendrier similaire pour les actions entreprises au niveau national au titre de cette stratégie;

Jeudi 12 septembre 2013

51. réclame des rapports réguliers de la part de la Commission, des États membres, d'Europol et de l'EC3 récemment créé, d'Eurojust et de l'ENISA, évaluant les progrès accomplis par rapport aux objectifs de la stratégie de cybersécurité, notamment des indicateurs de performances clés mesurant les avancées en matière de mise en œuvre;

o

o o

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

P7_TA(2013)0377

Proposition de résolution — Stratégie numérique pour la croissance, la mobilité et l'emploi

Résolution du Parlement européen du 12 septembre 2013 sur la stratégie numérique pour la croissance, la mobilité et l'emploi: il est temps de passer à la vitesse supérieure (2013/2593(RSP))

(2016/C 093/17)

Le Parlement européen,

— vu la communication de la Commission du 18 décembre 2012 intitulée «Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne» (COM(2012)0784),

— vu les questions à la Commission et au Conseil sur la stratégie numérique pour la croissance, la mobilité et l'emploi: il est temps de passer à la vitesse supérieure (O-000085 — B7-0219/2013 et O-000086 — B7-0220/2013),

— vu le règlement (UE) n° 531/2012 du Parlement européen et du Conseil du 13 juin 2012 concernant l'itinérance sur les réseaux publics de téléphonie mobile à l'intérieur de l'Union ([1]),

— vu la décision n° 243/2012/UE du Parlement européen et du Conseil du 14 mars 2012 établissant un programme pluriannuel en matière de politique du spectre radioélectrique ([2]),

— vu les négociations en cours sur le mécanisme pour l'interconnexion en Europe et, en particulier, la proposition modifiée de règlement du Parlement européen et du Conseil concernant des orientations pour les réseaux transeuropéens de télécommunications et abrogeant la décision n° 1336/97/CE (COM(2013)0329),

— vu sa résolution du 5 mai 2010 sur un nouvel agenda numérique pour l'Europe: 2015.eu ([3]),

— vu la communication de la Commission du 27 septembre 2012 intitulée «Exploiter le potentiel de l'informatique en nuage en Europe» (COM(2012)0529),

— vu la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)0011), en date du 25 janvier 2012,

---

([1]) JO L 172 du 30.6.2012, p. 10.
([2]) JO L 81 du 21.3.2012, p. 7.
([3]) JO C 81 E du 15.3.2011, p. 45.