CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 19 mai 2011 (24.05)
(OR. en)

10299/11

TELECOM 71
DATAPROTECT 55
JAI 332
PROCIV 66

NOTE

du:	Coreper
au:	Conseil
n° prop. Cion:	8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38
n° doc. préc.:	10003/11 TELECOM 60 DATAPROTECT 48 JAI 308 PROCIV 64
Objet:	Protection des infrastructures d'information critiques "Réalisations et prochaines étapes: vers une cybersécurité mondiale" - Adoption des conclusions du Conseil

1. Le 1er avril 2011, la Commission a transmis au Conseil sa communication relative à la protection des infrastructures d'information critiques (PIIC), intitulée "Réalisation et prochaines étapes: vers une cybersécurité mondiale".

2. Cette communication récapitule les résultats obtenus depuis l'adoption en 2009 du plan d'action PIIC[1], lancé pour renforcer la résilience et la sécurité des infrastructures essentielles des technologies de l'information et des communications. En outre, elle décrit les prochaines étapes que la Commission propose pour chaque action, au niveau européen comme au niveau international.

[1] Le plan d'action PIIC est exposé dans le communication de la Commission du 30 mars 2009 relative à la protection des infrastructures d'information critiques, intitulée "Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience".

3. La cybersécurité et la protection des infrastructures d'information critiques sont essentielles pour que les utilisateurs privés et les entreprises aient confiance dans l'internet et les autres réseaux et elles constituent une grande priorité de la stratégie numérique pour l'Europe[2]. La communication relative à la protection des infrastructures d'information critiques s'intéresse 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. Elle propose de promouvoir des actions coordonnées visant à prévenir, détecter et atténuer toutes les formes de perturbations, naturelles ou liées à l'homme et à y apporter une réponse, et d'associer toutes les personnes intéressées.

4. Afin de parvenir à un niveau accru de sensibilisation et de préparation dans l'ensemble de l'UE, la Commission propose plusieurs actions concrètes. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) joue un rôle important dans bon nombre de ces actions. La communication propose, entre autres, des actions destinées à promouvoir des principes pour la résilience et la stabilité de l'internet, à constituer des partenariats stratégiques de dimension internationale, à accomplir des efforts coordonnés dans les enceintes internationales, ainsi qu'à améliorer l'état de préparation de l'UE.

5. Les 14 et 15 avril 2011, la présidence du Conseil a organisé, en collaboration avec la Commission, une conférence ministérielle sur la protection des infrastructures d'information critiques, à Balatonfüred (Hongrie). Le groupe "Télécommunications et société de l'information" a pris acte des résultats de cette conférence, ainsi que de la déclaration faite par la présidence à cette occasion. Dans cette dernière, la présidence a souligné qu'il était nécessaire que les États membres intensifient leurs efforts dans le domaine du renforcement de leurs capacités nationales en matière de cybersécurité. Elle a également mis l'accent sur l'importance de réformer, de moderniser et de renforcer rapidement l'ENISA afin qu'elle soit en mesure de répondre aux défis, ainsi que sur la nécessité pour l'Union d'attendre un niveau de sécurité élevé des réseaux et de l'information.

---

[2] Doc. 9981/10.

6. La protection durable des infrastructures d'information critiques européennes revêt une importance stratégique. Le projet de conclusions souligne qu'il importe de mettre en place des équipes nationales ou gouvernementales d'intervention en cas d'urgence informatique, d'élaborer des plans d'urgence nationaux en cas d'incident informatique et d'organiser des exercices nationaux dans le domaine de la cybersécurité. En ce qui concerne la coopération européenne, le projet de conclusions met l'accent sur la nécessité d'encourager la coopération entre les États membres en mettant au point des mécanismes de coopération entre les États membres en cas d'incident informatique, en organisant des exercices à l'échelle paneuropéenne, et en favorisant le dialogue sur les questions liées à la sécurité des TIC. Les efforts déployés par les États membres dans les enceintes internationales sont très importants. Afin de renforcer la coopération internationale dans le domaine de la sécurité des réseaux et de l'information et d'établir des partenariats stratégiques internationaux aux niveaux bilatéral et multilatéral, les États membres et la Commission sont invités à travailler en étroite coordination. Dans le projet de conclusions, l'ENISA est invitée à soutenir activement les États membres dans les efforts qu'ils déploient afin de renforcer leurs capacités nationales et de coopérer les uns avec les autres. Dans ce contexte, les États membres soulignent l'importance que revêt une modernisation rapide et appropriée de l'ENISA. Enfin, les parties prenantes sont invitées à lancer et promouvoir des actions visant à renforcer la sécurité des réseaux et de l'information et à améliorer la sécurité des services et réseaux de communications électroniques et la confiance des utilisateurs, et à participer à ces actions.

7. Le groupe "Télécommunications et société de l'information" a examiné le projet de conclusions lors de plusieurs réunions et est parvenu à un accord de principe sur le texte qui figure en annexe. Lors de la réunion du Coreper du 18 mai 2011, la Commission a rappelé les préoccupations que lui inspirent certaines questions déjà traitées par le groupe.

8. Le Conseil est invité à examiner les conclusions jointes en annexe en vue de leur adoption.

_____

CONCLUSIONS DU CONSEIL

sur la protection des infrastructures d'information critiques
"Réalisations et prochaines étapes: vers une cybersécurité mondiale"

LE CONSEIL DE L'UNION EUROPÉENNE,

I. NOTE AVEC SATISFACTION

la communication de la Commission du 31 mars 2011 relative à la protection des infrastructures d'information critiques intitulée "Réalisations et prochaines étapes: vers une cybersécurité mondiale"[3];

II. RAPPELLE

1. les conclusions du Conseil du 20 avril 2007 sur un programme européen de protection des infrastructures critiques[4];
2. la directive 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[5];
3. la communication de la Commission du 30 mars 2009 relative à la protection des infrastructures d'information critiques, intitulée "Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité, et la résilience" exposant un plan d'action destiné à renforcer la sécurité et la résilience des infrastructures essentielles des technologies de l'information et des communications (TIC)[6];
4. les conclusions de la présidence sur la protection des infrastructures d'information critiques à l'occasion de la conférence ministérielle de Tallinn organisée les 27 et 28 avril 2009[7];

---

3 Doc. 8548/11.
4 Doc. 7743/07.
5 JO L 345 du 23.12.2008, p. 75.
6 Doc. 8375/09.
7 http://www.riso.ee/tallinnciip/
http://www.riso.ee/tallinnciip/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

5. les dispositions pertinentes, en matière de sécurité des réseaux et de l'information, du nouveau cadre réglementaire pour les communications électroniques[8];
6. la résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information[9];
7. la communication de la Commission du 19 mai 2010 concernant "Une stratégie numérique pour l'Europe", soulignant la nécessité de renforcer la sécurité dans la société numérique et ainsi améliorer la confiance dans les réseaux[10];
8. les conclusions du Conseil du 31 mai 2010 sur la stratégie numérique pour l'Europe[11];
9. la communication de la Commission du 22 novembre 2010 intitulée "La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre"[12];
10. la déclaration faite par la présidence sur la protection des infrastructures d'information critiques à l'occasion de la conférence ministérielle de Balatonfüred, organisée les 14 et 15 avril 2011[13];

III. EST CONSCIENT:

1. de l'importance croissante des systèmes, infrastructures et services des TIC ainsi que de l'internet, notamment pour les citoyens européens, les entreprises européennes et l'économie européenne dans son ensemble, ce qui montre la dépendance sociale, politique et économique de l'Europe vis-à-vis des TIC, de même que la nécessité de sécuriser nos systèmes et réseaux informatiques pour qu'ils résistent à toutes les perturbations possibles, qu'elles soient accidentelles ou intentionnelles;
2. que, en dehors des perturbations graves des réseaux et des systèmes d'information, des incidents affectant la sécurité risquent aussi de saper la confiance des utilisateurs dans les technologies, les réseaux et les services, ce qui aura des répercussions sur leur capacité à exploiter pleinement les TIC et à les utiliser à grande échelle pour contribuer à la croissance économique ainsi qu'à une meilleure qualité de vie;

---

8 JO L 337 du 18.12.2009, p. 11.
9 Doc. 15841/09.
10 Doc. 9981/10.
11 Doc. 10130/10.
12 Doc. 16797/10.
13 http://www/eu2011.hu/document/presidency-statement-en-ministerial-conference-critical-information-infrastructure-protecti

3. que les efforts déployés en la matière devraient non seulement contribuer à dynamiser la croissance et l'emploi, mais aussi permettre à l'Union de protéger efficacement ses intérêts vitaux;
4. que les risques croissants qui découlent de nouvelles menaces de plus en plus complexes pesant sur les réseaux et services des TIC et sur l'internet notamment, peuvent être traités, entre autres, grâce à la mise au point de nouveaux systèmes plus perfectionnés capables de se protéger eux-mêmes, reposant sur des recherches et des innovations efficaces, mais qu'ils rendent également une protection efficace plus urgente que jamais;
5. que la vulnérabilité ou la perturbation des systèmes, infrastructures et services des technologies de l'information et des communications pourraient causer des dégâts énormes à l'économie européenne, compte tenu du fait que toute perturbation substantielle, survenant dans un État membre a des répercussions dans d'autres États et dans l'ensemble de l'UE;
6. qu'il est dès lors nécessaire - en tant qu'objectif commun pour l'Europe - de stimuler et de soutenir la réalisation d'un niveau élevé de préparation, de sécurité et de capacités de résilience, et d'améliorer les compétences techniques pour permettre à l'Europe de faire face aux problèmes de protection des réseaux et des infrastructures d'information;
7. de la nécessité d'utiliser les exigences minimales, principes fondamentaux et normes généralement admis qui existent à l'heure actuelle dans le domaine de la sécurité des réseaux et de l'information et de les perfectionner, afin de promouvoir la prise en compte de la sécurité dès la conception, ainsi que des produits et des services qui soient sûrs par défaut, dans la mesure du possible;
8. de la nécessité de susciter la confiance et de renforcer le sentiment de sécurité de toutes les parties concernées, ce qui est indispensable si l'on veut améliorer la coopération en matière de protection des infrastructures essentielles et faire entrer tous les Européens dans l'ère numérique, conformément aux objectifs énoncés dans la stratégie numérique pour l'Europe;
9. de la nécessité d'adopter une approche concertée en matière de sécurité des réseaux et de l'information, associant toutes les parties prenantes et tenant compte de l'utilisation généralisée des TIC et de l'internet par tous les types d'utilisateurs et pour toutes sortes de finalités, dans le but de mieux sensibiliser et conscientiser tous les utilisateurs;
10. de la nécessité que les partenaires publics et privés collaborent et assument la responsabilité du développement de leurs propres capacités et de leur préparation afin de prévenir, de détecter et de régler les problèmes de sécurité susceptibles d'avoir des répercussions sur la disponibilité des réseaux et services de communications électroniques;

11. de la nécessité de faire de l'objectif de prévention de toute perturbation non seulement un défi national et européen, mais aussi un défi international et mondial, compte tenu de l'interconnexion des systèmes, infrastructures et services des technologies de l'information et des communications.

IV. SOULIGNE

1. l'importance stratégique de l'industrie européenne des TIC et de la sécurité des réseaux et de l'information en ce qui concerne la protection durable des infrastructures d'information critiques européennes;
2. en ce qui concerne les capacités nationales, l'importance de mettre en place des équipes nationales ou gouvernementales d'intervention en cas d'urgence informatique et d'élaborer des plans d'urgence nationaux en cas d'incident informatique ainsi que d'organiser des exercices nationaux dans le domaine de la cybersécurité;
3. en matière de coopération européenne, la nécessité d'encourager la coopération entre les États membres en mettant au point des mécanismes de coopération entre les États membres en cas d'incident informatique, en organisant des exercices à l'échelle paneuropéenne, en favorisant le dialogue sur les questions liées à la sécurité des TIC, par exemple sur les critères relatifs aux TIC pour les infrastructures européennes critiques, le cas échéant, ou sur la stabilité et la résilience de l'internet, ainsi qu'en encourageant, en collaboration avec le secteur privé, l'émergence d'une filière solide de la sécurité informatique;
4. les progrès significatifs accomplis par le Forum européen des États membres dans la promotion des débats et des échanges entre les États membres ainsi qu'entre les États membres et l'Union en ce qui concerne les bonnes pratiques en matière de sécurité et de résilience des infrastructures des TIC;
5. l'importance des efforts multipartites, par exemple en rapport avec le partenariat public-privé européen pour la résilience (EP3R), un cadre de collaboration évolutif à l'échelle européenne pour la résilience des infrastructures des TIC;
6. le rôle important que joue l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) par rapport aux activités menées par les États membres et les partenaires publics et privés dans l'Union dans le domaine de la sécurité des réseaux et de l'information, notamment en ce qui concerne la mise en place d'équipes nationales ou gouvernementales performantes pour les interventions en cas d'urgence informatique;

7. le succès du premier exercice paneuropéen, qui a eu lieu le 4 novembre 2010 et qui a démontré qu'il existait une volonté commune de collaboration transfrontière entre les États membres;
8. les avantages qui découlent, en termes de sécurité des réseaux et de l'information, d'une culture nationale, européenne et mondiale de l'analyse et de la gestion des risques à tous les niveaux et par toutes les parties prenantes, axée sur la promotion d'actions coordonnées visant à prévenir, détecter et atténuer toutes les formes de perturbations et à y apporter une réponse;
9. les possibilités en termes de compétitivité économique liées à l'exploitation du potentiel qu'offrent les nouvelles connaissances en matière de systèmes de sécurité des réseaux et de l'information, et tout particulièrement de prise en compte de la sécurité des applications dès leur conception et des nouveaux systèmes capables de se protéger eux-mêmes;
10. l'intérêt qu'il pourrait y avoir à poursuivre la promotion, avec le soutien de l'ENISA, d'une approche cohérente et concertée en matière de sécurité des réseaux et de l'information dans les États membres, dans les institutions de l'UE et dans le secteur privé.

V. SOULIGNE

l'importance que revêt une modernisation rapide et appropriée de l'ENISA pour lui permettre de mieux assumer son rôle, de mieux se recentrer sur celui-ci et de continuer à contribuer au renforcement de la sécurité des réseaux et de l'information en Europe.

VI. INVITE LES ÉTATS MEMBRES À:

1. intensifier les efforts visant à promouvoir une culture de la gestion des risques et des programmes d'éducation, de formation et de recherche en matière de sécurité des réseaux et de l'information;
2. créer des équipes d'intervention en cas d'urgence informatique dans les États membres qui n'ont pas encore mis en place de telles capacités;
3. favoriser la coopération entre les équipes nationales ou gouvernementales d'intervention en cas d'urgence informatique déjà créées ou à créer et les autres équipes d'intervention en cas d'urgence informatique internationalement reconnues qui sont actives dans les États membres;
4. favoriser la mise en place d'ici à 2012, le cas échéant avec le soutien de l'ENISA, d'un réseau performant regroupant les équipes nationales ou gouvernementales d'intervention en cas d'urgence informatique et les autres équipes d'intervention en cas d'urgence informatique internationalement reconnues qui sont actives dans les États membres;

5. définir une approche commune sur les modalités de mise en œuvre d'un système européen de partage d'information et d'alerte (SEPIA) dans le but d'établir leurs systèmes nationaux de partage d'informations et d'alerte, le cas échéant avec le soutien de l'ENISA;
6. envisager d'adopter une stratégie nationale en matière de cybersécurité lorsqu'il n'en existe pas;
7. élaborer des plans d'urgence nationaux en cas d'incident informatique afin d'être en mesure d'intervenir et, au besoin, de coopérer avec les États membres en cas d'incident grave;
8. renforcer la collaboration entre les États membres et contribuer, en s'appuyant sur l'expérience acquise et les résultats obtenus au niveau national en matière de gestion de crise et en coopération avec l'ENISA, à la mise au point de mécanismes de coopération européens en cas d'incident informatique, qui devront être mis à l'épreuve dans le cadre du prochain exercice "CyberEurope" en 2012;
9. organiser des exercices nationaux ou transfrontaliers dans le domaine de la cybersécurité afin de tester le niveau de préparation des États membres pour faire face aux perturbations de la sécurité des réseaux et de l'information, contribuer de manière appropriée à l'organisation d'exercices dans le domaine de la cybersécurité au niveau européen et participer à ceux-ci selon un calendrier pertinent et réalisable, ainsi qu'à d'autres activités visant à renforcer les capacités qui sont menées à l'échelle de l'Union;
10. poursuivre, avec le Forum européen des États membres et en collaboration avec l'EP3R les travaux concernant les critères pour recenser les infrastructures européennes critiques dans le secteur des TIC, portant plus particulièrement sur les communications fixes et mobiles et l'internet;
11. se prêter mutuellement assistance, sur une base volontaire, en cas d'incidents transfrontaliers;
12. poursuivre et coordonner les efforts déployés dans toutes les enceintes internationales compétentes, et œuvrer de concert au sein des institutions de l'Union afin de renforcer la coopération internationale dans le domaine de la sécurité des réseaux et de l'information à l'échelle mondiale et d'établir des partenariats stratégiques internationaux aux niveaux bilatéral et multilatéral, notamment par une participation, en étroite coordination avec la Commission, aux activités du groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité;
13. stimuler et soutenir la coopération avec le secteur privé tant au niveau national qu'à l'échelle européenne.

VII. INVITE LA COMMISSION À:

1. promouvoir la résilience et la stabilité de l'internet à tous les niveaux, en collaboration avec les parties prenantes du secteur public et du secteur privé;
2. promouvoir une approche européenne cohérente et efficace de la sécurité des réseaux et de l'information afin d'éviter la duplication des efforts et de garantir une compréhension commune des différents enjeux;
3. promouvoir, en concertation avec les États membres et l'ENISA, l'application des exigences minimales, principes fondamentaux et normes généralement admis dans le domaine de la sécurité des réseaux et de l'information ainsi que leur développement ultérieur, dans le but de favoriser la prise en compte de la sécurité dès la conception et de promouvoir des produits et services aussi sûrs que possible par défaut;
4. coopérer étroitement avec les États membres et, le cas échéant, appuyer les mesures qu'ils prennent à la suite des présentes conclusions;
5. soutenir l'action menée par les États membres au sein du Forum européen des États membres et de l'EP3R dans le cadre des travaux sur les critères de recensement des infrastructures européennes critiques dans le secteur des TIC, portant plus particulièrement sur les communications fixes et mobiles et l'internet;
6. coopérer autant que possible avec le secteur privé dans ses activités visant à renforcer la sécurité des réseaux et de l'information à l'échelle mondiale;
7. favoriser l'élaboration d'un programme de recherche et de développement ambitieux dans le domaine de la sécurité des réseaux, des systèmes d'information et des applications, et établir des correspondances concrètes entre ce programme et les plans de protection des infrastructures d'information critiques;
8. soutenir les États membres dans leurs efforts visant à étudier les possibilités de mettre au point des mécanismes de coopération européens en cas d'incident informatique, qui devront être mis à l'épreuve dans le cadre du prochain exercice "CyberEurope" en 2012;
9. suivre l'élaboration des meilleures stratégies de gouvernance pour les technologies émergentes ayant une incidence mondiale, telles que l'informatique en nuage;

10. améliorer la préparation de l'UE par la mise en place d'une équipe d'intervention en cas d'urgence informatique pour les institutions de l'Union;
11. en étroite coordination avec les États membres et les organes compétents de l'Union, œuvrer au renforcement de la coopération internationale dans le domaine de la sécurité des réseaux et de l'information avec les partenaires internationaux compétents et au sein de diverses enceintes compétentes telles que le groupe de travail conjoint UE-États-Unis sur la cybersécurité et la cybercriminalité;
12. informer régulièrement le Parlement européen et le Conseil des initiatives prises au niveau de l'UE dans le domaine de la sécurité des réseaux et de l'information.

VIII. INVITE l'ENISA À

1. continuer de soutenir activement les États membres dans les efforts qu'ils déploient afin de renforcer leurs capacités nationales et de coopérer les uns avec les autres;
2. renforcer encore son expertise en matière de sécurité des réseaux et de l'information et contribuer à une meilleure compréhension des défis émergents en Europe dans ce domaine.

IX. INVITE LES PARTIES PRENANTES À:

1. lancer et promouvoir des actions visant à renforcer la sécurité des réseaux et de l'information, et à améliorer la sécurité des services et réseaux de communications électroniques ainsi que la confiance des utilisateurs, et à participer à ces actions;
2. répartir les efforts avec les parties prenantes du secteur public pour relever les défis dans le domaine de la sécurité des réseaux et de l'information et contribuer à définir les responsabilités individuelles, notamment pour les utilisateurs finaux;
3. concevoir et proposer des produits, des services, des équipements et des logiciels plus sûrs et plus fiables dans le secteur des TIC, pour contribuer à protéger nos économies, qui dépendent fortement de ce secteur;
4. participer à des partenariats entre le secteur public et le secteur privé afin de contribuer au développement de réseaux sûrs et résistants ainsi qu'à l'émergence d'une filière solide de la sécurité informatique en Europe. Ces partenariats devraient également favoriser un dialogue entre les parties prenantes ainsi qu'une bonne compréhension de l'ensemble des enjeux;

5. sensibiliser les utilisateurs aux risques liés à la sécurité des réseaux et de l'information et les informer des meilleurs moyens de prévenir ces risques et de réagir en cas d'incident;
6. soutenir les efforts des États membres visant à élaborer des plans d'urgence nationaux en cas d'incident informatique et à organiser, le cas échéant, des exercices de simulation d'incident;
7. prendre toutes les mesures techniques et organisationnelles appropriées pour garantir la disponibilité et la sécurité des réseaux et des services de communications électroniques;
8. participer à la définition et à l'application des exigences minimales et des normes généralement admises au niveau international dans le domaine de la sécurité des réseaux et de l'information.