CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 22 juillet 2013 (OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
n° doc. préc.:	11357/13
Objet:	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

Les délégations trouveront en annexe les conclusions du Conseil relatives à la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, qui ont été adoptées par le Conseil des affaires générales le 25 juin 2013.

ANNEXE

Conclusions du Conseil relatives à la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

Le Conseil de l'Union européenne,

1. CONSCIENT que le cyberespace, transnational par nature, est constitué de réseaux et d'infrastructures d'information interdépendants, notamment l'Internet et les réseaux de télécommunication, qu'il représente l'un des principaux moyens d'aujourd'hui et de demain, de satisfaire les besoins et les intérêts des citoyens et des États membres de l'UE et de respecter leurs droits et qu'il est un atout indispensable pour la croissance économique de l'UE;

2. SOULIGNANT le rôle que jouent les particuliers, le secteur privé et la société civile et les droits dont ils disposent en ce qui concerne les questions inhérentes au cyberespace ainsi que le rôle important que l'UE exerce pour promouvoir et préserver un cyberespace ouvert, sécurisé et résilient, reposant sur les valeurs fondamentales de l'UE telles que la démocratie, les droits de l'homme et l'État de droit, dans l'intérêt de nos économies, de nos administrations et de notre société et aux fins du bon fonctionnement du marché intérieur;

3. CONSCIENT de la nécessité d'améliorer la confidentialité, la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que des informations qui y sont contenues;

4. SACHANT que des garde-fous doivent être mis en place et des mesures prises pour prévenir les risques auxquels sont exposés des réseaux et des infrastructures d'information interdépendants et pour protéger le cyberespace, dans les domaines tant civil que militaire;

5. RÉAFFIRMANT la position de l'UE selon laquelle les normes, principes et valeurs qu'elle défend hors ligne, notamment la Charte des droits fondamentaux de l'UE, devraient aussi s'appliquer dans le cyberespace;

6. CONSCIENT que le droit international, notamment les conventions internationales telles que la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et les conventions relatives au droit humanitaire international et aux droits de l'homme, telles que le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels établissent un cadre juridique applicable au cyberespace. Des efforts devraient donc être déployés pour veiller au respect de ces instruments dans le cyberespace, raison pour laquelle l'UE ne préconise pas la création de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace;

7. AFFIRMANT que la question de la cybersécurité doit être traitée selon une approche intégrée, pluridisciplinaire et horizontale et que les mesures adoptées devraient porter sur un ensemble de questions très diverses concernant le cyberespace;

8. RAPPELANT les nombreuses initiatives lancées par l'UE et au niveau international dans le domaine de la cybersécurité, notamment celles figurant à l'annexe du présent document;

9. RAPPELANT les dispositions de l'article 222 du traité sur le fonctionnement de l'Union européenne et tenant compte des travaux en cours concernant la mise en œuvre de la stratégie;

10. SACHANT que les efforts visant à renforcer la cybersécurité et la lutte contre la cybercriminalité doivent être accomplis non seulement au sein de l'Union européenne mais également dans les pays tiers, notamment ceux à partir desquels les organisations cybercriminelles opèrent;

PAR LES PRÉSENTES CONCLUSIONS

11. ACCUEILLE FAVORABLEMENT la communication conjointe de la Commission et de la haute représentante de l'UE concernant la stratégie de cybersécurité de l'Union européenne;

12. ESTIME qu'il est indispensable et urgent de poursuivre l'élaboration d'une approche globale et de la mettre en œuvre aux fins d'une politique de l'UE sur le cyberespace qui:
    - protège et favorise l'exercice des droits de l'homme et repose sur les valeurs fondamentales de l'UE que sont la démocratie, les droits de l'homme et l'État de droit,
    - fait progresser la prospérité en Europe et renforce les avantages économiques et sociaux du cyberespace, notamment l'Internet,

- favorise une cybersécurité effective et renforcée dans l'ensemble de l'UE et au-delà,
- encourage les efforts visant à réduire la fracture numérique mondiale et soutient la coopération internationale dans le domaine de la cybersécurité,
- reflète le rôle et les droits des particuliers, du secteur privé et de la société civile à l'égard des questions inhérentes au cyberespace, et qui est notamment l'expression d'un renforcement de la coopération public-privé et de l'échange d'informations;

ET

13. INVITE les États membres, la Commission et la haute représentante à coopérer, dans le respect des domaines de compétences de chacun et du principe de subsidiarité, pour répondre aux objectifs stratégiques énoncés dans les présentes conclusions;

Valeurs

14. SOULIGNE que les droits de l'homme, notamment la liberté d'expression et le droit à la vie privée, doivent toujours être respectés dans le cadre de l'élaboration de politiques et d'actions portant sur des questions relatives au cyberespace ainsi que dans la législation, et prend acte des négociations actuellement menées en vue de l'adoption d'un cadre juridique de l'UE pour la protection des données à caractère personnel, susceptible de fonctionner efficacement dans le cyberespace;

15. EST CONSCIENT que les valeurs et intérêts défendus et protégés au sein de l'Union devraient l'être également dans ses politiques extérieures en rapport avec les questions relatives au cyberespace;

16. ENGAGE l'UE et ses États membres:
    - à faire valoir de manière déterminée et unifiée leur position concernant l'application universelle des droits de l'homme et des libertés fondamentales dans le cyberespace, notamment la liberté d'opinion, d'expression, d'information, de réunion et d'association.
    - à déterminer comment faire respecter dans le cyberespace les obligations existantes;

17. INVITE l'UE et ses États membres à promouvoir les compétences numériques et à contribuer à sensibiliser davantage les utilisateurs à leurs responsabilités individuelles lorsqu'ils mettent des données à caractère personnel sur l'Internet;

18. INSISTE SUR le rôle important joué par l'UE pour maintenir le modèle multipartite de gouvernance de l'Internet;

19. INVITE les États membres à prendre toutes les mesures raisonnables pour que tous les citoyens de l'UE soient en mesure d'accéder à l'Internet et d'en tirer parti;

Prospérité

20. INVITE la Commission à consentir des efforts particuliers pour promouvoir le marché unique numérique et avancer sur les questions y afférentes au sein de l'Union et dans les enceintes internationales (par exemple au sein de l'Organisation mondiale du commerce (OMC) et dans le cadre des négociations concernant l'accord sur les technologies de l'information (ATI)) ainsi que pour garantir l'accès au marché dans ces secteurs lors de la négociation d'accords de libre-échange avec des pays tiers;

21. SOULIGNE qu'il importe que la législation dans ce domaine soit neutre du point de vue technologique et encourage autant que possible la neutralité de l'Internet afin de ne pas entraver la concurrence par des pratiques discriminatoires à l'encontre du commerce transfrontière en ligne et des nouveaux modèles d'entreprise;

22. SE FÉLICITE qu'il ait été jugé nécessaire d'investir dans la recherche et le développement dans le domaine du cyberespace, domaine important susceptible de créer des emplois de haute qualité et de générer de la croissance économique;

23. ATTIRE L'ATTENTION SUR:
- le fait qu'il est absolument capital que les technologies de l'information et de la communication (TIC) ainsi que la sécurité des TIC constituent un secteur dynamique de l'UE permettant de renforcer la cybersécurité et INVITE les États membres et la Commission à réfléchir aux mesures qui peuvent être prises pour contribuer au développement de ce secteur et à en rendre compte;
- le fait que la législation en faveur de la cybersécurité devrait favoriser l'innovation et la croissance et se concentrer sur la protection des infrastructures et des fonctions clés que les États membres jugent indispensables,
- le fait que l'économie numérique est un facteur déterminant de croissance, d'innovation et d'emploi et que la cybersécurité est essentielle à sa protection,

- l'importance de la protection des infrastructures d'informations critiques (PIIC) au niveau national;

Parvenir à la cyber-résilience

24. PREND NOTE AVEC SATISFACTION des objectifs fixés dans la proposition de directive de la Commission définissant des mesures visant à renforcer:
    - la sécurité des réseaux et de l'information dans l'UE,
    - les moyens et la préparation en matière de cybersécurité au niveau national,
    - la coopération entre les États membres et dans l'ensemble de l'UE afin d'encourager une culture de la gestion des risques dans les secteurs public et privé;

25. APPELLE toutes les institutions, instances et agences de l'UE, en coopération avec les États membres, à prendre les mesures nécessaires pour assurer leur propre cybersécurité, en renforçant leur sécurité selon les normes de sécurité appropriées, en coopération avec l'ENISA afin d'établir les meilleures pratiques conformément au règlement (UE) nº 526/2013[1];

26. RAPPELLE qu'une équipe d'intervention en cas d'urgence informatique (CERT) pour les institutions, instances et agences de l'UE a été mise en place à l'issue d'une phase pilote d'un an et d'une évaluation positive de son rôle et de son efficacité;

27. SOULIGNE l'importance capitale que revêt l'ENISA pour soutenir les États membres et l'Union dans les efforts qu'ils déploient pour atteindre un niveau élevé de sécurité des réseaux et de l'information, notamment en contribuant au renforcement des capacités des États membres et au développement de solides moyens de cyber-résilience au niveau national, aux exercices européens dans le domaine de la cybersécurité ainsi qu'aux efforts de l'Union en ce qui concerne la R&D et la normalisation, et INVITE l'ENISA à coopérer avec d'autres institutions, instances et agences de l'Union sur les questions relatives à la sécurité des réseaux et de l'information (SRI), conformément au règlement (UE) nº 526/2013;

---

[1] JO L 165 du 18.6.2013.

28. MET L'ACCENT SUR la nécessité de renforcer la résilience des infrastructures critiques à l'échelle de l'UE et d'assurer une coopération et une coordination plus étroites entre les acteurs concernés, y compris entre les acteurs civils et militaires de l'UE, notamment entre le secteur public et le secteur privé pour intervenir en cas d'incidents et de problèmes de cybersécurité, par des initiatives telles que l'élaboration de normes communes, des actions de sensibilisation, l'éducation et la formation ainsi que le réexamen et l'expérimentation (ou le développement), qui sont en cours, de mécanismes d'alerte rapide et d'intervention. Il est également nécessaire d'assurer une coopération et une coordination plus étroites dans les interventions menées en réponse à des incidents de cybersécurité par les acteurs du secteur de la défense, les services répressifs, le secteur privé et les autorités chargées de la cybersécurité pour répondre efficacement aux problèmes de cybersécurité, y compris en ce qui concerne la gestion des incidents;

29. INVITE les États membres:

- à prendre des mesures pour veiller à atteindre dans leur pays un bon niveau en matière de cybersécurité, en élaborant et en mettant en œuvre des politiques adéquates ainsi que des capacités organisationnelles et opérationnelles adaptées, en vue de protéger les systèmes informatiques dans le cyberespace , notamment ceux qui sont considérés comme critiques,
- à établir le dialogue avec les entreprises et les universités pour favoriser la confiance, qui est un élément essentiel de la cybersécurité au niveau national, par exemple en mettant en place des partenariats public-privé,
- à soutenir des actions de sensibilisation à la nature des menaces et aux aspects fondamentaux des bonnes pratiques en matière numérique, à tous les niveaux,
- à aider les propriétaires et les fournisseurs de systèmes informatiques à protéger leurs propres systèmes ainsi que les services essentiels qu'ils fournissent,
- à favoriser une coopération paneuropéenne en matière de cybersécurité, notamment en renforçant les exercices paneuropéens dans ce domaine,
- à assurer une coordination et une coopération effectives entre les États membres au niveau de l'UE, en vue de parvenir à une évaluation commune des menaces,

- à renforcer et à étendre la coopération entre utilisateurs des États membres et de l'UE, en s'appuyant sur des structures existantes,
- à prendre en compte les questions de cybersécurité à la lumière des travaux en cours sur la clause de solidarité;

Cybercriminalité

30. SALUE les conclusions du Conseil JAI des 6 et 7 juin 2013 fixant les priorités de l'UE pour la lutte contre la grande criminalité organisée entre 2014 et 2017, qui font de la lutte contre la cybercriminalité une priorité;

31. SOULIGNE que, selon l'évaluation de la menace que représente la grande criminalité organisée (SOCTA) réalisée par Europol en 2013, la cybercriminalité est une forme de criminalité qui représente une menace croissante pour l'UE pouvant se concrétiser par des violations de données à grande échelle, des fraudes en ligne et l'exploitation sexuelle des enfants, tandis que la cybercriminalité à but lucratif en vient à jouer un rôle de catalyseur pour d'autres activités criminelles;

32. SE FÉLICITE DE la création du Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol et INVITE les États membres à recourir à ce centre pour renforcer la coopération entre agences nationales dans le cadre de son mandat;

33. INVITE Europol et Eurojust à continuer de renforcer leur coopération avec toutes les parties intéressées, notamment les agences de l'UE, Interpol, l'ensemble du réseau des équipes d'intervention en cas d'urgence informatique (CERT) et le secteur privé, dans la lutte contre la cybercriminalité, y compris en mettant l'accent sur les synergies et les complémentarités conformément aux mandats et compétences respectifs desdites parties;

34. ANTICIPE la ratification rapide, par tous les États membres, de la convention de Budapest sur la cybercriminalité;

35. APPELLE la Commission, Europol, le CEPOL et l'ENISA à soutenir la formation et l'amélioration des compétences dans les États membres où les gouvernements et les autorités répressives ont besoin de mettre en place des capacités dans le domaine du cyberespace pour lutter contre la cybercriminalité;

36. INVITE la Commission:

- à aider les États membres qui en font la demande à recenser les insuffisances dans leur pays et à renforcer leurs moyens d'enquête et de lutte contre la cybercriminalité,
- à utiliser le Fonds pour la sécurité intérieure, dans les limites de son budget (tout en tenant compte de ses autres priorités), pour aider les autorités compétentes à lutter contre la cybercriminalité,
- à recourir à l'instrument de stabilité pour développer la lutte contre la cybercriminalité ainsi qu'à des initiatives visant à renforcer les capacités, y compris en ce qui concerne la coopération policière et judiciaire dans les pays tiers à partir desquels opèrent les organisations cybercriminelles,
- à faciliter la coordination des programmes de renforcement des capacités afin d'éviter les doublons et de créer des synergies,
- à fournir des informations concernant les progrès de l'Alliance mondiale contre les abus sexuels commis contre des enfants via Internet,
- à continuer de faciliter le suivi de l'environnement politique de l'UE en matière de lutte contre la cybercriminalité, notamment à la lumière des résultats et des informations stratégiques fournies par Europol (EC3),
- à continuer de favoriser la coopération intercommunautaire, notamment en soutenant Europol (EC3);

Politique de sécurité et de défense commune (PSDC)

37. Dans le contexte de la PSDC, MET EN LUMIÈRE:

- la nécessité urgente de mettre en œuvre et de développer les aspects de la stratégie ayant trait à la cyberdéfense qui relèvent de la PSDC, afin de mettre en place un cadre en matière de cyberdéfense, s'il y a lieu, ainsi que de définir des mesures concrètes et égard, également dans la perspective du débat sur la sécurité et la défense prévu par le Conseil européen en décembre 2013. Un point de contact unique devrait être désigné au sein du SEAE pour orienter ces efforts,

- la nécessité de renforcer les capacités des États membres en matière de cyberdéfense, y compris par l'élaboration de normes communes, ainsi que la sensibilisation par la formation et l'éducation dans le domaine de la cybersécurité, en tirant parti du Collège européen de sécurité et de défense et en continuant d'améliorer les possibilités de formation et d'exercice mises à la disposition des États membres,
- la possibilité d'utiliser des mécanismes existants de mutualisation et partage et de mettre à profit des synergies avec des politiques plus générales de l'UE pour mettre en place, de la manière la plus efficace possible, les capacités nécessaires des États membres en matière de cyberdéfense,
- la nécessité de la recherche et du développement. Il s'agit en priorité d'encourager les États membres à développer des technologies sûres et résilientes en matière de cyberdéfense, avec une forte participation du secteur privé et des universités, et de renforcer les aspects liés à la cybersécurité dans les projets de recherche de l'AED sur la base d'une approche collaborative, ce qui constituerait en outre un bon exemple de la coordination qui peut avoir lieu entre l'AED et la Commission au titre de la coopération-cadre européenne pour des projets à double usage,
- l'utilité de réexaminer et de tester les mécanismes d'alerte rapide et d'intervention à la lumière de nouvelles cybermenaces, par un dialogue entre le SEAE, l'ENISA, l'EC3, l'AED, la Commission et les États membres, afin de trouver des synergies et de nouer des liens avec le secteur de la défense,
- la nécessité de poursuivre et de renforcer la coopération entre l'UE et l'OTAN dans le domaine de la cyberdéfense, en établissant des priorités pour la poursuite de cette coopération dans le cadre existant, y compris en ce qui concerne la participation mutuelle à des exercices et à des formations en matière de cyberdéfense,
- la prise en compte d'aspects liés à la cyberdéfense dans la politique plus large menée en matière de cyberespace;

Industrie et technologie

38. CONSCIENT de la nécessité pour l'Europe de continuer à développer ses ressources industrielles et technologiques pour parvenir à un niveau adéquat de diversité et de confiance au sein de ses réseaux et systèmes informatiques, le Conseil SE FÉLICITE vivement du fait que la stratégie de cybersécurité européenne de l'UE appelle à soutenir une politique industrielle forte, afin de promouvoir un secteur européen fiable dans le domaine des TIC et de la cybersécurité et de dynamiser le marché intérieur par la R&D;

39. INVITE les États membres, la Commission et l'ENISA à renforcer les efforts qu'ils déploient pour la recherche et le développement dans le domaine des TIC et de la cybersécurité ainsi que pour disposer de professionnels bien préparés en matière de cybersécurité, ce qui est essentiel pour dynamiser la compétitivité des technologies européennes de l'information et de la communication (TIC) et des secteurs des services et de la sécurité et pour renforcer leur capacité à mettre en place des solutions fiables et sûres, en conséquence de quoi le Conseil ENCOURAGE la Commission à tirer parti du programme-cadre pour la recherche et l'innovation "Horizon 2020";

40. SOULIGNE que le développement de partenariats public-privé sera un instrument pertinent pour renforcer les capacités en matière de cybersécurité; et APPELLE par conséquent la Commission à encourager les synergies, dans le cadre de l'initiative Horizon 2020, entre les opérateurs d'infrastructures critiques et les instituts de recherche travaillant dans le domaine des TIC et de la sécurité sur des questions liées à la cybersécurité et à la cybercriminalité, et avec les politiques de l'Union en matière de sécurité intérieure et extérieure;

41. APPELLE les États membres et la Commission à prendre des mesures spécifiques en faveur de la cybersécurité dans les petites et moyennes entreprises, particulièrement vulnérables aux attaques informatiques et encourage les États membres à développer des technologies sûres et résilientes en matière de cybersécurité, avec la collaboration du secteur privé et des universités;

42. INVITE la Commission à tenir compte des normes qui existent dans le domaine de la cybersécurité et SOULIGNE que la coopération et l'échange d'informations en matière de normes - par exemple, en ce qui concerne la gestion des risques - devrait continuer de se développer, en coopération avec les États membres, l'industrie et d'autres parties intéressées;

Coopération internationale en matière de cyberespace

43. RÉAFFIRME que l'UE est déterminée à soutenir l'élaboration de mesures visant à instaurer la confiance en matière de cybersécurité, à accroître la transparence et à limiter le risque de malentendu face à l'attitude de l'État, en encourageant la mise en place de normes internationales dans ce domaine;

44. APPELLE la Commission et la haute représentante, conformément aux procédures prévues à cet égard par les traités:

- a) à promouvoir la convention de Budapest comme modèle pour la rédaction de la législation nationale en matière de cybercriminalité et comme base de la coopération internationale dans ce domaine, b) à promouvoir le respect des droits fondamentaux dans le cyberespace et c) à faire pleinement usage de tous les instruments de coopération internationale disponibles pour développer la lutte contre la cybercriminalité ainsi que la coopération policière et judiciaire qui y est liée dans les pays tiers à partir desquels les organisations cybercriminelles opèrent,
- à faire appel à l'expertise des États membres en matière de politique du cyberespace et à l'expérience qu'ils ont tirée de leurs engagements bilatéraux et de la coopération, afin d'élaborer des messages communs de l'UE en matière de cyberespace et de travailler étroitement avec les États membres sur les aspects opérationnels,
- en coopération avec des États membres, des organisations privées concernées et la société civile, à tirer pleinement parti des instruments d'aide pertinents de l'UE pour le renforcement des capacités dans le domaine des TIC, y compris en ce qui concerne la cybersécurité;

45. APPELLE les États membres, la Commission et la haute représentante à œuvrer à l'instauration d'une politique internationale de l'UE cohérente en matière de cyberespace, conformément aux procédures pertinentes prévues par les traités:

- en renforçant les relations avec les principaux partenaires et organismes internationaux de manière à veiller à ce que tous les États membres puissent bénéficier pleinement d'une telle coopération,
- en intégrant les questions relatives au cyberespace dans la PESC,

- en améliorant la coordination des questions inhérentes au cyberespace qui ont une dimension mondiale et en intégrant la cybersécurité, y compris les mesures visant à instaurer la confiance et à renforcer la transparence, dans le cadre général des relations avec des pays tiers et avec des organisations internationales, notamment par une coordination renforcée entre les États membres, la Commission et le SEAE dans le cadre de dialogues et d'autres activités en matière de cybersécurité,
- en assurant une meilleure coordination par le biais des instances préparatoires compétentes du Conseil (y compris le groupe des Amis de la présidence en ce qui concerne les questions inhérentes au cyberespace),
- en appuyant le renforcement des capacités dans les pays tiers, par des actions de formation et d'assistance à la mise en place de politiques, de stratégies et d'institutions nationales pertinentes, en vue de permettre la réalisation de tout le potentiel économique et social des TIC, en soutenant la mise en place de systèmes résilients dans ces pays et en limitant les risques liés au cyberespace pour les institutions de l'UE et les États membres, tout en ayant recours aux réseaux et aux enceintes chargés de la coordination politique et de l'échange d'informations,

Rôles et responsabilités respectifs

46. DEMANDE aux autres parties prenantes - le secteur privé, les milieux universitaires et techniques, la société civile et les citoyens - d'assumer leurs rôles et leurs responsabilités respectifs pour favoriser l'émergence d'un cyberespace ouvert, libre et sûr;

47. DEMANDE à la Commission et à la haute représentante que les activités menées à l'échelon européen soient conçues pour être compatibles avec les structures nationales, le droit constitutionnel et les initiatives des États membres en matière de cybersécurité, afin de promouvoir une approche intégrée et d'éviter les doubles emplois;

ET

48. DEMANDE à la Commission et à la haute représentante de rédiger un rapport d'activité sur la stratégie de cybersécurité qui sera présenté lors de la conférence de haut niveau qui se tiendra en février 2014; et PROPOSE que se tiennent régulièrement des réunions des instances préparatoires compétentes du Conseil (et notamment le groupe des Amis de la présidence en ce qui concerne les questions inhérentes au cyberespace, pour contribuer à définir les priorités et les objectifs stratégiques de l'UE concernant le cyberespace au sein d'un cadre d'action global et pour suivre et soutenir la mise en œuvre de la stratégie.

49. Aux fins de la mise en œuvre des présentes conclusions du Conseil, seuls seront utilisés les fonds et les programmes de financement existants, sans préjudice des négociations sur le futur cadre financier. Dès lors, le Conseil INVITE la Commission à présenter les modalités de financement de la stratégie, en tenant compte des futures négociations avec le Parlement européen.

Références

1. Parlement européen, Conseil et Commission

   - Charte des droits fondamentaux de l'Union européenne[2],

2. Parlement européen et Conseil

   - Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information[3],

   - Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre"), modifiée par la directive 2009/140/CE[4],

3. Parlement européen

   - Résolution du Parlement européen du 11 décembre 2012 sur une stratégie pour la liberté numérique dans la politique étrangère de l'Union,

   - Rapport du Parlement européen de 2012 sur la cybersécurité et la défense,

4. Conseil

   - Le programme de Stockholm - Une Europe ouverte et sûre qui sert et protège les citoyens[5],

   - Une Europe sûre dans un monde meilleur - Stratégie européenne en matière de sécurité, 12 décembre 2003[6],

---

2 JO C 364 du 18.12.2010, p. 1.
3 JO L 77 du 13.3.2004, p. 1.
4 JO L 108 of 24.4.2002, p. 33 et JO L 337 du 18.12.2009, p. 37.
5 Doc. 17024/09 CO EUR-PREP 3 JAI 896 POLGEN 229.
6 Doc. 15849/03 PESC 783.

- Stratégie de sécurité intérieure pour l'Union européenne: "Vers un modèle européen de sécurité"[7],

- 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[8],

- Conclusions du Conseil sur la communication de la Commission intitulée "La stratégie de sécurité intérieure de l'UE en action"[9],

- Conclusions du Conseil sur la communication de la Commission relative à la protection des infrastructures d'information critiques intitulée "Réalisations et prochaines étapes: vers une cybersécurité mondiale"[10],

- Conclusions du Conseil sur la définition des priorités de l'UE pour la lutte contre la grande criminalité organisée entre 2014 et 2017[11],

- Conclusions du Conseil sur l'établissement d'un Centre européen de lutte contre la cybercriminalité[12],

---

7 Doc. 5842/2/10 JAI 90.

8 JO L 345 du 23.12.2008, p. 75.

9 Doc. 6699/11 JAI 124.

10 Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. Cette communication fait suite à la communication de la Commission 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" (doc. 8375/09).

11 Doc. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.

12 Doc. 10603/12 ENFOPOL 154 TELECOM 116.

- Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information, remplaçant la décision-cadre 2005/222/JAI du Conseil. Approbation du texte de compromis final en vue d'un accord en première lecture avec le Parlement européen[13],

- Conclusions du Conseil sur la stratégie européenne pour un Internet mieux adapté aux enfants[14],

- Conclusions du Conseil sur la lutte contre l'exploitation sexuelle des enfants et la pédopornographie sur Internet - Renforcer l'efficacité des activités de police dans les États membres et les pays tiers[15],

- Conclusions du Conseil sur une alliance mondiale contre les abus sexuels commis contre des enfants via Internet[16],

- Conclusions du Conseil relatives à une stratégie de travail concertée et à des mesures concrètes de lutte contre la cybercriminalité[17] et conclusions du Conseil relatives à un plan d'action visant à mettre en œuvre la stratégie concertée de lutte contre la cybercriminalité[18],

- Orientation générale partielle du Conseil concernant la proposition de règlement de la Commission portant établissement du programme-cadre pour la recherche et l'innovation "Horizon 2020" (2014-2020)[19],

- Action commune du Conseil concernant la création de l'Agence européenne de défense[20],

---

13 Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673.
14 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81.
15 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53.
16 Doc. 10607/12 + COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46.
17 Doc. 15569/08 ENFOPOL 224 CRIMORG 190.
18 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32.
19 Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.
20 Doc. 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121.

- Proposition conjointe de décision du Conseil concernant les modalités de mise en œuvre par l'Union de la clause de solidarité[21],

- Conclusions du Conseil sur l'éducation aux médias dans l'environnement numérique[22],

- Droits de l'homme et démocratie: cadre stratégique de l'UE et plan d'action de l'UE[23],
- Rapport sur la mise en œuvre de la stratégie européenne de sécurité[24],

5. Commission

- La stratégie numérique pour l'Europe[25], qui est l'une des sept initiatives phares de la stratégie Europe 2020 pour une croissance intelligente, durable et inclusive[26], et la stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne[27] - qui recentre la stratégie numérique,

- Communication de la Commission intitulée "Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle"[28],

- Communication de la Commission intitulée "Combattre la criminalité à l'ère numérique: établissement d'un Centre européen de lutte contre la cybercriminalité"[29],

---

21 Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165.

22 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380.

23 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603.

24 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139.

25 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216.

28 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6.

29 Doc. 8543/12 ENFOPOL 94 TELECOM 72.

- Communication de la Commission intitulée "Exploiter le potentiel de l'informatique en nuage en Europe"[30],

- Communication de la Commission relative à la protection des infrastructures d'information critiques - "Réalisations et prochaines étapes: vers une cybersécurité mondiale"[31],

- Communication de la Commission relative à la protection des infrastructures d'information critiques - "Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience"[32],

6. Nations unies

- Résolution A/RES 57/239 de l'Assemblée générale des Nations unies sur la création d'une culture mondiale de la cybersécurité,
- Résolution A/HRC/20/L.13 du Conseil des droits de l'homme des Nations unies, du 29 juin 2012, sur la promotion, la protection et l'exercice des droits de l'homme sur l'internet,
- Résolution A/RES 67/27 de l'Assemblée générale des Nations unies intitulée "Progrès de l'informatique et des télécommunications et sécurité internationale",
- Création d'un groupe intergouvernemental d'experts à composition non limitée sur le phénomène de la cybercriminalité, associant l'ONUDC conformément à la résolution 65/230 de l'Assemblée générale des Nations unies,

7. Conseil de l'Europe

- Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,

- Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité

---

30 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585.
31 Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.
32 Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46.

8. Organisation pour la sécurité et la coopération en Europe (OSCE)

- Décision du Conseil permanent n° 1039 du 26 avril 2012: Élaboration de mesures de confiance en vue de réduire les risques de conflit découlant de l'utilisation des technologies de l'information et de la communication,

- Décision du Conseil ministériel n° 4/12 du 7 décembre 2012: Efforts déployés par l'OSCE pour faire face aux menaces transnationales,

- Groupe de travail informel à composition non limitée de l'OSCE chargé d'élaborer un projet de mesures de confiance destinées renforcer la coopération interétatique, la transparence, la prévisibilité et la stabilité et à réduire les risques d'erreur d'appréciation, d'escalade et de conflit découlant de l'utilisation des technologies de l'information et de la communication,

9. Conférences, initiatives et événements

- Conférence internationale sur le cyberespace, tenue à Londres les 1er et 2 novembre 2011, et suivie d'une conférence internationale sur le même sujet tenue à Budapest les 4 et 5 octobre 2012,

- Exercice conjoint UE–États-Unis de simulation de cyberincident ("Cyber Atlantic 2011") et exercices paneuropéens de simulation de cyberincident avec la participation de tous les États membres (Cyber Europe 2010 et Cyber Europe 2012),

- Groupe ad hoc sur la sécurité nucléaire, lequel a examiné la question de la sécurité informatique et de la cybersécurité dans son rapport final[33],

[33] Doc. 10616/12 AHGS 20 ATO 84.

10. Autres

- Évaluation 2013 d'Europol de la menace que représente la grande criminalité organisée (SOCTA)[34],

– - Politique de sécurité en matière d'assurance de l'information concernant la défense des réseaux[35] et lignes directrices concernant la défense des réseaux[36].

---

[34] Doc. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.

[35] Doc. 8408/12 CSCI 11 CSC 20.

[36] Doc. 10578/12 CSCI 20 CSC 34.