Annexe 2 : Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information

des réseaux et des systèmes d'information;

11. qu'il est important d'étudier les effets, les risques et les perspectives stratégiques de la création d'équipes d'intervention en cas d'urgence informatique pour les institutions de l'UE et de réfléchir au futur rôle éventuel de l'ENISA dans ce domaine;

12. des travaux réalisés jusqu'à présent par l'ENISA dans le domaine de la sécurité des réseaux et de l'information et de la nécessité de continuer à développer cette agence pour en faire un organisme efficace apportant des avantages clairs dans le domaine de la sécurité des réseaux et de l'information;

V. SOULIGNE:

1. qu'une stratégie européenne renforcée et globale en matière de sécurité des réseaux et de l'information, avec des rôles clairement définis pour la Commission européenne, les États membres et l'ENISA, revêt une importance fondamentale pour relever les défis actuels et futurs;

2. qu'après une consultation et une analyse appropriées, il convient d'envisager, dans le cadre du processus législatif, la modernisation et le renforcement de l'ENISA en lui donnant un mandat qui autorise une certaine souplesse et permette aux États membres et à la Commission d'exercer une surveillance et aux représentants des parties prenantes du secteur privé de jouer un rôle efficace. Ce mandat devrait tenir compte du cadre réglementaire pour les réseaux et services de communications électroniques, être conforme aux ambitions définies dans le programme de Lisbonne et comprendre des objectifs liés à la recherche, à l'innovation, à la compétitivité, à la croissance économique et à l'instauration de la confiance;

VI. INVITE LES ÉTATS MEMBRES À:

1. poursuivre les travaux visant à renforcer la confiance des utilisateurs finaux dans les TIC par des campagnes de sensibilisation;

2. organiser des exercices nationaux et/ou participer à des exercices européens périodiques dans le domaine de la sécurité des réseaux et de l'information, en tenant compte de la nécessité d'une planification détaillée liée à la complexité du domaine et à la participation du secteur privé. L'ENISA pourrait, à leur demande, aider les États membres à cette fin. L'ampleur et la dimension géographique des exercices devraient évoluer naturellement dans le temps et reposer sur les risques reconnus;

3. créer des équipes d'intervention en cas d'urgence informatique dans les États membres qui n'ont pas encore mis en place une telle capacité et renforcer la coopération entre ces équipes à un niveau européen. L'ENISA pourrait aider les États membres à cette fin;

4. intensifier les efforts consacrés aux programmes d'éducation, de formation et de recherche en matière de sécurité des réseaux et de l'information afin de garantir la disponibilité au sein de l'UE des compétences techniques et des experts nécessaires et d'accroître le professionnalisme de ces derniers dans ce domaine;

5. réagir de concert en cas d'incident transfrontière et renforcer leur capacité à le faire de manière appropriée, ce qui requiert un renforcement du dialogue entre les décideurs concernés, en particulier sur les questions de confidentialité;

VII. INVITE LA COMMISSION À:

1. apporter, le cas échéant, un soutien aux États membres dans la mise en œuvre de la présente résolution;

2. 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;

3. en collaboration avec l'ENISA, lancer une campagne visant à sensibiliser le public européen et les acteurs privés à l'importance d'une gestion du risque appropriée dans le domaine de la sécurité des réseaux et de l'information;

4. continuer, en collaboration avec les États membres, à recenser les mesures susceptibles d'inciter les fournisseurs d'infrastructures de communications électroniques à offrir des infrastructures solides et résilientes aux utilisateurs finaux, aux entreprises et aux pouvoirs publics;

5. en collaboration avec les États membres, mettre au point des méthodes permettant une évaluation comparative au niveau de l'UE de l'impact socio-économique des incidents et de l'efficacité des mesures préventives;

6. encourager et améliorer les modèles multipartites, qui doivent apporter une valeur ajoutée manifeste pour les utilisateurs finaux et les entreprises;

7. présenter une stratégie globale en matière de sécurité des réseaux et de l'information (1), comprenant des propositions relatives à un mandat renforcé et souple pour l'ENISA et prévoyant une surveillance accrue des États membres et de la Commission;

8. réaliser une analyse, en collaboration avec les États membres, sur les équipes d'intervention en cas d'urgence informatique, afin de recenser les domaines dans lesquels une plus ample coopération est nécessaire;

9. poursuivre l'examen concernant la mise au point d'une approche commune ou interopérable pour les institutions de l'UE en ce qui concerne l'achat de systèmes et de services TIC sécurisés;

VIII. ENGAGE L'ENISA À:

1. continuer d'apporter un soutien actif aux États membres, à la Commission européenne et aux autres parties prenantes concernées dans la mise en œuvre des politiques européennes en matière de sécurité des réseaux et de l'information et du plan d'action pour la protection des infrastructures d'information critiques;

2. travailler en collaboration avec les États membres, la Commission et les organismes statistiques en vue de la mise au point d'un cadre de données statistiques sur l'état de la sécurité des réseaux et de l'information en Europe;

IX. INVITE LES PARTIES PRENANTES À:

1. intensifier leurs efforts pour renforcer le niveau de sécurité des réseaux et de l'information, notamment en ce qui concerne l'offre de produits et services fiables, dignes de confiance et faciles à utiliser;

2. informer les utilisateurs de manière adéquate des risques en matière de sécurité liés aux produits et services et des moyens de s'en protéger;

3. prendre toutes les mesures techniques et organisationnelles appropriées pour garantir la continuité, l'intégrité et la confidentialité des réseaux et services de communications électroniques;

4. poursuivre les travaux de normalisation dans le domaine de la sécurité des réseaux et de l'information afin d'essayer de trouver des solutions harmonisées et interopérables;

5. participer avec les États membres à des exercices afin de pouvoir réagir de manière appropriée aux urgences.