

Proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information

(2002/C 203 E/16)

COM(2002) 173 final — 2002/0086(CNS)

(Présentée par la Commission le 19 avril 2002)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment ses articles 29, 30, paragraphe 1, point a), 31 et 34, paragraphe 2, point b);

vu la proposition de la Commission;

vu l'avis du Parlement européen;

considérant ce qui suit:

- (1) Il a été constaté la perpétration d'attaques contre des systèmes d'information, notamment dues à la criminalité organisée, et une inquiétude croissante face à l'éventualité d'attaques terroristes contre les systèmes d'information appartenant à l'infrastructure critique des États membres. Cette situation risque de compromettre la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union européenne.
- (2) Une réponse efficace à ces menaces suppose une approche d'ensemble en matière de sécurité des réseaux et de l'information, comme l'ont souligné le plan d'action eEurope, la communication de la Commission intitulée «Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne»⁽¹⁾ et la résolution du Conseil, du 6 décembre 2001, relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information.
- (3) La nécessité de renforcer la prise de conscience des problèmes liés à la sécurité de l'information et de fournir une assistance pratique a également été soulignée par la résolution du Parlement européen du 5 septembre 2001⁽²⁾.
- (4) Les vides juridiques et les différences considérables présentées par les législations des États membres dans ce

domaine freinent la lutte contre la criminalité organisée et le terrorisme, et font obstacle à une coopération policière et judiciaire efficace en cas d'attaques contre les systèmes d'information. Les réseaux de télécommunication électroniques modernes étant transnationaux et ne connaissant pas les frontières, ces attaques ont souvent une dimension internationale, et mettent ainsi en lumière le besoin urgent de poursuivre le rapprochement des droits pénaux dans ce domaine.

- (5) Le plan d'action du Conseil et de la Commission concernant les modalités optimales de mise en œuvre des dispositions du Traité d'Amsterdam relatives à l'établissement d'un espace de liberté, de sécurité et de justice⁽³⁾, le conseil européen de Tampere des 15 et 16 octobre 1999, le conseil européen de Santa Maria da Feira des 19 et 20 juin 2000, la Commission dans son tableau de bord⁽⁴⁾, et le Parlement européen dans sa résolution du 19 mai 2000⁽⁵⁾ mentionnent ou appellent à des mesures législatives contre la criminalité utilisant les technologies avancées, notamment des définitions, des incriminations et des sanctions communes.
- (6) Il est nécessaire de compléter le travail réalisé par les organisations internationales, plus particulièrement celui du Conseil de l'Europe sur le rapprochement du droit pénal et les travaux du G8 sur la coopération transnationale dans le domaine de la criminalité utilisant les technologies avancées, en proposant une approche commune dans ce domaine au niveau de l'Union européenne. Cet appel a été plus amplement développé dans la communication que la Commission a adressée au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions, intitulée «Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité»⁽⁶⁾.
- (7) Les règles du droit pénal relatives aux attaques contre les systèmes d'information devraient être rapprochées pour garantir la meilleure coopération policière et judiciaire possible en ce qui concerne les infractions liées à ce type d'attaques et contribuer à la lutte contre la criminalité organisée et le terrorisme.

⁽³⁾ JO C 19 du 23 janvier 1999.

⁽⁴⁾ COM(2001) 278 final.

⁽⁵⁾ A5-0127/2000.

⁽⁶⁾ COM(2000) 890.

⁽¹⁾ COM(2001) 298.

⁽²⁾ [2001/2098(INI)].

- (8) La décision-cadre relative au mandat d'arrêt européen, l'annexe de la convention Europol et la décision du Conseil instituant Eurojust contiennent des références à la délinquance informatique qu'il convient de définir plus précisément. Aux fins de ces instruments, la délinquance informatique comprend les attaques contre les systèmes d'information telles que définies par la présente décision-cadre qui permet de parvenir à un niveau de rapprochement bien plus élevé des éléments constitutifs de ces infractions. La présente décision-cadre complète également la décision-cadre relative à la lutte contre le terrorisme qui couvre les actes terroristes causant de graves dommages à une infrastructure, y compris un système d'information, et constituant un danger pour la vie humaine ou entraînant d'importantes pertes économiques.
- (9) Tous les États membres ont ratifié la 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. Les données à caractère personnel traitées dans le contexte de la mise en œuvre de la présente décision-cadre seront protégées conformément aux principes établies par ladite convention.
- (10) Des définitions communes dans ce domaine, plus particulièrement pour les systèmes d'information et les données informatiques, sont indispensables pour assurer l'application cohérente de la présente décision-cadre dans les États membres.
- (11) Il est nécessaire d'adopter une approche commune pour les éléments constitutifs des infractions pénales, en instituant un délit commun d'accès illicite à un système d'information et d'interférence illicite avec un tel système.
- (12) Il importe d'éviter la surincrimination, notamment pour les comportements mineurs ou insignifiants, de même que l'incrimination de détenteurs de droits et de personnes autorisées, telles que les utilisateurs légitimes privés ou professionnels, les administrateurs, contrôleurs et exploitants de réseaux et de systèmes, les chercheurs scientifiques légitimes et les personnes autorisées procédant aux essais d'un système, que la personne travaille au sein de l'entreprise ou qu'il s'agisse d'une personne employée à l'extérieur et autorisée à tester la sécurité d'un système.
- (13) Il est nécessaire que les États membres prévoient des sanctions efficaces, proportionnées et dissuasives pour réprimer les attaques contre les systèmes d'information, y compris des peines d'emprisonnement dans les cas graves.
- (14) Il convient de prévoir des peines plus sévères lorsque certaines circonstances accompagnant une attaque contre un système d'information en font une menace accrue pour la société. Dans ces cas, les sanctions dont sont passibles les auteurs doivent être suffisantes pour que les attaques contre les systèmes d'information relèvent du champ d'application des instruments déjà adoptés afin de lutter contre la criminalité organisée, tels que l'action commune 98/733/JAI relative à l'incrimination de la participation à une organisation criminelle dans les États membres de l'Union européenne du 21 décembre 1998, adoptée par le Conseil sur la base de l'article K.3 du Traité sur l'Union européenne ⁽¹⁾.
- (15) Des mesures doivent être prises pour que les personnes morales puissent être tenues responsables des infractions pénales visées dans le présent acte et commises à leur profit, et pour que chaque État membre ait compétence pour les infractions commises contre des systèmes d'information lorsque leur auteur est physiquement présent sur son territoire ou lorsque le système d'information se trouve sur ce dernier.
- (16) Des mesures de coopération entre les États membres doivent également être envisagées, afin d'assurer une action efficace contre les attaques visant les systèmes d'information. Des points de contact opérationnels devraient être établis aux fins de l'échange d'informations.
- (17) Comme les objectifs consistant à garantir que des attaques contre des systèmes d'information soient passibles, dans tous les États membres, de sanctions pénales effectives, proportionnées et dissuasives et à améliorer et favoriser la coopération judiciaire en supprimant les obstacles potentiels, ne peuvent être réalisés de manière suffisante par les États membres agissant unilatéralement, puisque les règles doivent être communes et compatibles, et que lesdits objectifs peuvent donc être mieux réalisés au niveau de l'Union, celle-ci peut adopter des mesures, conformément au principe de subsidiarité tel que visé à l'article 2 du traité sur l'UE et prévu à l'article 5 du traité CE. Conformément au principe de proportionnalité tel que visé dans le dernier article, la présente décision-cadre se limite au minimum nécessaire à la réalisation de ces objectifs.
- (18) La présente décision-cadre n'affecte pas les pouvoirs de la Communauté européenne.
- (19) La présente décision-cadre respecte les droits fondamentaux et des principes reconnus en particulier par la Charte des droits fondamentaux de l'Union européenne, notamment ses chapitres II et VI,

A ARRÊTÉ LA PRÉSENTE DÉCISION-CADRE:

Article premier

Champ d'application et objet de la décision-cadre

La présente décision-cadre vise à renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information.

⁽¹⁾ JO L 351 du 29.12.1998, p. 1.

*Article 2***Définitions**

Aux fins de la présente décision-cadre, on entend par:

- a) «réseau de communication électronique»: les systèmes de transmission et, le cas échéant, les commutateurs ou routeurs et autres moyens permettant le transport de signaux par fil, par radio, par support optique ou par tout autre moyen électromagnétique, y compris les réseaux à satellite, les réseaux terrestres fixes (par commutation de circuits et commutation par paquets, y compris Internet) et mobiles, les systèmes de câbles électriques, dans la mesure où ils sont utilisés pour transmettre des signaux, les réseaux utilisés pour les services de radiodiffusion sonore et télévisuelle et les réseaux de télévision par câble, quelle que soit la nature des informations transmises.
- b) «ordinateur»: tout appareil ou groupe d'appareils interconnectés ou reliés entre eux, dont l'un ou plusieurs exécutent, grâce à un programme, le traitement automatique de données informatiques.
- c) «données informatiques»: toute représentation de faits, d'informations ou de notions créée ou mise sous une forme susceptible d'être traitée par un système d'information, notamment un programme permettant à ce dernier d'exécuter une fonction.
- d) «système d'information»: les ordinateurs et réseaux de communication électroniques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance.
- e) «personne morale»: toute entité à laquelle le droit en vigueur reconnaît ce statut, à l'exception des États et des autres collectivités locales exerçant des prérogatives de puissance publique, et des organisations internationales relevant du droit public.
- f) «personne autorisée»: toute personne physique ou morale ayant le droit, en vertu d'un contrat ou d'une loi, ou l'autorisation légale, d'utiliser, d'administrer, de contrôler, de tester, d'effectuer des recherches scientifiques légitimes ou d'exploiter d'une autre manière un système d'information, et qui agit conformément à ce droit ou à cette autorisation.
- g) «sans en avoir le droit»: signifie que les actes de personnes autorisées ou d'autres actes dont le caractère licite est reconnu par le droit national sont exclus.

*Article 3***Accès illicite à des systèmes d'information**

Les États membres font en sorte que l'accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un système d'information devienne une infraction pénale punissable lorsque l'acte a été commis:

- i) contre toute partie d'un système d'information faisant l'objet de mesures de protection particulières; ou
- ii) avec l'intention de porter préjudice à une personne physique ou morale; ou
- iii) avec l'intention d'obtenir un avantage économique.

*Article 4***Interférence illicite avec des systèmes d'information**

Les États membres font en sorte que la commission des actes intentionnels suivants, sans en avoir le droit, devienne une infraction pénale punissable:

- a) perturber gravement ou interrompre le fonctionnement d'un système d'information en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données informatiques;
- b) effacer, détériorer, altérer, supprimer ou rendre inaccessibles des données informatiques d'un système d'information lorsque l'acte est commis avec l'intention de porter préjudice à une personne physique ou morale.

*Article 5***Incitation, aide, complicité et tentative**

1. Les États membres font en sorte que l'incitation, l'aide ou la complicité volontaires à commettre l'une des infractions visées aux articles 3 et 4 soit punissable.

2. Les États membres font en sorte que la tentative de commettre les infractions visées aux articles 3 et 4 soit punissable.

*Article 6***Sanctions**

1. Les États membres font en sorte que les infractions visées aux articles 3, 4 et 5 soient passibles de peines effectives, proportionnées et dissuasives, notamment de peines privatives de liberté dont la durée maximale n'est pas inférieure à un an dans des cas graves. La notion de cas graves exclut les cas dans lesquels l'acte commis n'a pas entraîné de préjudice ou d'avantage économique.

2. Les États membres prévoient la possibilité d'infliger des amendes en plus des peines privatives de liberté, ou comme alternative à ces dernières.

*Article 7***Circonstances aggravantes**

1. Les États membres font en sorte que les infractions visées aux articles 3, 4 et 5 soient passibles d'une peine privative de liberté dont la durée maximale n'est pas inférieure à quatre ans lorsqu'elles sont accompagnées des circonstances suivantes:

- a) l'infraction a été commise dans le cadre d'une organisation criminelle au sens défini par l'action commune 98/733/JAI, du 21 décembre 1998, relative à l'incrimination de la participation à une organisation criminelle dans les États membres de l'Union européenne, indépendamment de la peine qui y est visée;
- b) l'infraction a causé, ou a entraîné, une perte économique importante, directe ou indirecte, des dommages corporels à une personne physique ou un dommage important à une partie de l'infrastructure critique de l'État membre;
- c) l'infraction a entraîné des profits importants.

2. Les États membres font en sorte que les infractions visées aux articles 3 et 4 soient passibles de peines privatives de liberté plus longues que celles prévues à l'article 6 lorsque l'auteur de l'infraction a été condamné pour une infraction similaire par un jugement devenu définitif dans un État membre.

*Article 8***Circonstances particulières**

Nonobstant les articles 6 et 7, les États membres font en sorte que les peines mentionnées aux articles 6 et 7 puissent être réduites lorsque l'autorité judiciaire compétente estime que l'auteur de l'infraction n'a causé que des dommages mineurs.

*Article 9***Responsabilité des personnes morales**

1. Les États membres font en sorte que les personnes morales puissent être tenues pour responsables des comportements visés aux articles 3, 4 et 5 commis à leur profit par toute personne agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, et exerçant un pouvoir de direction en son sein en vertu:

- a) d'un mandat de représentation de la personne morale, ou
- b) d'un pouvoir de prendre des décisions au nom de la personne morale, ou

c) d'un pouvoir d'exercer un contrôle au sein de la personne morale.

2. Outre les cas prévus au paragraphe 1, les États membres font en sorte qu'une personne morale puisse être tenue responsable lorsqu'un défaut de surveillance ou de contrôle imputable à une personne visée au paragraphe 1 a rendu possible la commission des infractions visées aux articles 3, 4 et 5 au profit de cette personne morale par une personne placée sous son autorité.

3. La responsabilité d'une personne morale au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques se rendant coupables des infractions ou des actes visés aux articles 3, 4 et 5.

*Article 10***Sanction des personnes morales**

1. Les États membres font en sorte qu'une personne morale poursuivie au titre de l'article 9, paragraphe premier, soit passible de peines effectives, proportionnées et dissuasives, qui comprendront des amendes pénales ou non pénales, et éventuellement d'autres sanctions telles que:

- a) la déchéance du bénéfice d'avantages ou d'aides d'origine publique,
- b) l'interdiction temporaire ou définitive d'exercer une activité commerciale,
- c) un placement sous contrôle judiciaire, ou
- d) une mesure judiciaire de dissolution.

2. Les États membres font en sorte qu'une personne morale dont la responsabilité est engagée au titre de l'article 9, paragraphe 2, soit passible de peines et de mesures effectives, proportionnées et dissuasives.

*Article 11***Compétence**

1. Chaque État membre établit sa compétence pour les infractions visées aux articles 3, 4 et 5, lorsque l'infraction a été commise:

- a) en tout ou en partie sur son territoire, ou

b) par l'un de ses ressortissants, si l'acte atteint des personnes individuelles ou des groupes de cet État, ou

Article 12

c) au profit d'une personne morale dont le siège est situé sur son territoire.

2. Lorsqu'il établit sa compétence conformément au paragraphe 1, point a), chaque État membre fait en sorte qu'elle comprenne les cas où:

a) l'auteur de l'infraction l'a commise alors qu'il était physiquement présent sur son territoire, même si l'infraction ne vise pas un système d'information situé sur son territoire; ou

b) l'infraction vise un système d'information situé sur son territoire, même si l'auteur de l'infraction n'était pas physiquement présent sur ce territoire.

3. Un État membre peut décider de ne pas appliquer la règle de compétence énoncée au paragraphe 1, points b) et c), ou de ne l'appliquer qu'à des cas ou des circonstances particuliers.

4. Chaque État membre prend également les mesures nécessaires en vue d'établir sa compétence pour les infractions visées aux articles 3 à 5 lorsqu'il refuse de livrer une personne présumée être l'auteur d'une telle infraction ou condamnée pour l'avoir commise à un autre État membre ou à un pays tiers ou de l'extrader vers cet État membre ou ce pays tiers.

5. Lorsqu'une infraction relève de la compétence de plusieurs États membres et lorsque chacun des États membres concernés peut valablement engager des poursuites sur la base des mêmes faits, les États membres concernés coopèrent pour décider lequel d'entre eux poursuivra les auteurs de l'infraction en vue, si possible, de contraindre la procédure dans un seul d'entre eux. À cette fin, les États membres peuvent avoir recours à tout organe ou mécanisme établi au sein de l'Union européenne pour faciliter la coopération entre leurs autorités judiciaires et la coordination de leurs actions.

6. Les États membres informent le Secrétariat général du Conseil et la Commission lorsqu'ils décident d'appliquer le paragraphe 3, en précisant, le cas échéant, les cas ou circonstances particuliers dans lesquels s'appliquent la décision.

Échange d'informations

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3, 4 et 5, et conformément aux règles régissant la protection des données, les États membres désignent des points de contact opérationnels disponibles 24 heures sur 24 et 7 jours sur 7.

2. Chaque État membre communique au Secrétariat général du Conseil et à la Commission le nom des points de contact désignés en vue de l'échange d'informations sur les infractions relatives aux attaques contre les systèmes d'information. Le Secrétariat général transmet ces informations aux autres États membres.

Article 13

Mise en œuvre

1. Les États membres adoptent les mesures nécessaires pour se conformer à la présente décision-cadre pour le 31 décembre 2003 au plus tard.

2. Ils communiquent au secrétariat général du Conseil et à la Commission le texte de toute disposition qu'ils adoptent, ainsi que des informations sur toutes autres mesures qu'ils prennent pour se conformer à la présente décision-cadre.

3. Sur cette base, la Commission soumet, pour le 31 décembre 2004, un rapport au Parlement européen et au Conseil sur l'application de la présente décision-cadre, accompagné, si nécessaire, de propositions législatives.

4. Le Conseil évaluera si les États membres ont arrêté les mesures nécessaires pour se conformer à la présente décision-cadre.

Article 14

Entrée en vigueur

La présente décision-cadre entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel des Communautés européennes*.