Parliamentary **Assembly**
Assemblée parlementaire

Parliamentary Assembly
Assemblée parlementaire
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Doc. 11325
26 juin 2007

Comment prévenir la cybercriminalité dirigée contre les institutions publiques des Etats membres et observateurs?

Rapport
Commission des questions juridiques et des droits de l'homme
Rapporteur : M. Kimmo SASI, Finlande, Groupe du Parti populaire européen

Résumé

La cybercriminalité est un danger réel qui doit être pris au sérieux à l'échelon le plus haut. Elle représente une véritable menace pour les Etats dont les infrastructures basées sur les technologies peuvent être paralysées ou même détruites. Cette question devrait être traitée avec la plus grande priorité.

L'Assemblée parlementaire souligne l'importance et la pertinence de la Convention sur la cybercriminalité (STE n° 185), seul instrument juridique contraignant en la matière à ce jour, et appelle les Etats membres et les Etats observateurs du Conseil de l'Europe à la signer, à la ratifier et à en mettre en œuvre les dispositions dans les meilleurs délais.

Consciente du fait que les cybercriminels comptent sur la possibilité d'opérer à travers les frontières et mettent à profit les différences de législation nationale d'un Etat à l'autre, l'Assemblée considère que la lutte contre la cybercriminalité nécessite le développement urgent de la coopération internationale.

Par ailleurs, les cyber-attaques ne représentent pas seulement un enjeu sur le plan juridique ; les pays devraient développer des politiques et des stratégies pour protéger effectivement leurs infrastructures vitales, ce qui exige d'allouer les ressources humaines, financières et techniques nécessaires à cette fin.

L'Assemblée attend avec beaucoup d'intérêt les conclusions du Comité d'experts sur le terrorisme (CODEXTER), qui examine actuellement la question de savoir si les lacunes des instruments actuels – y compris la Convention sur la cybercriminalité - nécessitent l'élaboration de nouveaux instruments, avant d'adresser ses recommandations au Comité des Ministres.

F – 67075 Strasbourg Cedex, e-mail: assembly@coe.int
tel : + 33 3 88 41 2000, fax + 33 3 88 41 2776

A. Projet de résolution

1. L'Assemblée parlementaire rappelle son Avis n°2 26 (2001) dans lequel elle considère la lutte contre la cybercriminalité comme un enjeu de toute première importance au regard des obstacles que peut poser cette forme de criminalité au développement des nouvelles technologies et, plus généralement, à la sécurité juridique et économique.

2. L'Assemblée considère que la cybercriminalité représente une véritable menace pour la démocratie, les droits de l'homme et l'Etat de droit, et que cette question devrait être traitée avec la plus grande priorité.

3. Pour la première fois, en effet, des cyber-attaques criminelles ont pris pour cible l'ensemble d'un Etat, en tentant de paralyser le fonctionnement d'infrastructures vitales de la République d'Estonie. D'autres attaques ont été constatées dans d'autres pays au même moment.

4. Ceci montre que la cybercriminalité est un danger réel qui doit être pris au sérieux à l'échelon le plus haut et qu'elle représente une véritable menace pour les Etats dont les infrastructures basées sur les technologies peuvent être paralysées ou même détruites.

5. Tous les Etats sont exposés à cette menace ; il est donc essentiel de développer un système de protection et de réponse efficace au niveau international.

6. L'Assemblée rappelle que la Convention sur la cybercriminalité, STE n° 185 (ci-après « la Convention ») contient des dispositions détaillées pour combattre les cyber-attaques dirigées contre des infrastructures vitales. Ce traité – le seul instrument contraignant sur le sujet à ce jour – a été très favorablement accueilli au niveau international et tous les Etats membres du Conseil de l'Europe, par conséquent, devraient le signer et le ratifier de toute urgence et, ce qui est le plus important, mettre en œuvre pleinement ses dispositions afin de lutter efficacement contre cette forme de criminalité.

7. L'Assemblée déplore le fait que de nombreux Etats membres n'aient pas encore ratifié cette importante Convention.

8. L'Assemblée note que la lutte contre la cybercriminalité nécessite le développement urgent de la coopération internationale car les cybercriminels comptent sur la possibilité d'opérer à travers les frontières et mettent à profit les différences de législation nationale d'un Etat à l'autre. L'absence de coopération entre les Etats membres expose ces derniers à des risques très graves.

9. L'Assemblée rappelle que la Convention est un traité ouvert et invite donc les Etats non membres à y adhérer le plus rapidement possible afin de renforcer la coopération internationale dans ce domaine important.

10. A cet égard, l'Assemblée se félicite des diverses initiatives mises en œuvre pour renforcer la coopération et la coordination internationale dans la lutte contre la cybercriminalité, notamment les points de contact 24/7 et le programme *« Check the web »* ; elle incite vivement les Etats membres à intensifier les efforts pour renforcer la coopération internationale et soutenir la coordination des mesures concrètes adoptées en vue d'une protection plus efficace.

11. Ce faisant, l'Assemblée souligne que les mesures adoptées pour combattre et prévenir la cybercriminalité doivent reposer sur une législation respectant pleinement les droits de l'homme et les libertés civiles.

12. Les législations pertinentes, en outre, devraient être standardisées ou, tout au moins, rendues mutuellement compatibles afin de permettre le degré requis de coopération internationale.

13. Les cyber-attaques ne représentent pas seulement un enjeu sur le plan juridique ; les pays devraient développer des politiques et des stratégies pour protéger effectivement leurs infrastructures vitales, ce qui exige d'allouer les ressources humaines, financières et techniques nécessaires à cette fin.

14. L'Assemblée invite en conséquence les Etats membres et observateurs à :

14.1. considérer la lutte contre la cybercriminalité et la prévention de ce type d'infractions comme une question prioritaire ;

14.2. signer et ratifier sans tarder la Convention sur la cybercriminalité et son Protocole additionnel et en assurer la pleine mise en oeuvre dès que possible ;

14.3. examiner leurs cadres juridiques respectifs afin d'établir s'ils prévoient des sanctions appropriées pour réprimer la cybercriminalité – en particulier les attaques terroristes effectuées par le biais de systèmes informatiques – et amender si nécessaire leur législation en assurant pleinement le respect des libertés individuelles, notamment la liberté d'expression et la liberté d'information ;

14.4. assurer la compatibilité de leur législation pertinente avec celle d'autres Etats afin de faciliter la coopération internationale et l'échange d'informations ;

14.5. développer, sur la base d'études techniques pertinentes, des politiques et des stratégies pour protéger efficacement les infrastructures vitales et allouer les ressources humaines, financières et techniques nécessaires à cette fin ;

14.6. prendre des mesures nationales efficaces en vue de prévenir les activités cybercriminelles.

15. L'Assemblée, tout en considérant que la Convention devrait faire l'objet d'un réexamen régulier à la lumière des progrès technologiques, attend avec beaucoup d'intérêt les conclusions du Comité d'experts sur le terrorisme (CODEXTER) – qui examine actuellement la question de savoir si les lacunes des instruments actuels (y compris la Convention sur la cybercriminalité) nécessitent l'élaboration de nouveaux instruments – avant d'adresser ses recommandations au Comité des Ministres.

B. Exposé des motifs par M. Kimmo Sasi, rapporteur

Table des matières

* * *

I. Introduction

1. Le 25 juin 2007, en réponse à une requête présentée par moi-même et d'autres parlementaires, le Bureau a décidé de demander à la Commission des questions juridiques et des droits de l'homme de préparer un rapport sur le thème « Comment prévenir la cybercriminalité dirigée contre les institutions publiques des Etats membres ».

2. Ce même jour, la Commission m'a nommé rapporteur.

3. Je voudrais présenter en quelques mots le contexte de cette initiative.

4. Pendant les dernières semaines, un Etat membre du Conseil de l'Europe – l'Estonie – a été l'objet de cyber-attaques de grande ampleur.[1] Ces attaques, qui ont culminé les 8 et 9 mai 2007, ont perturbé le fonctionnement de nombreux réseaux estoniens de transmission de données et pages web du secteur public. Les premières attaques ont visé les pages web des organes de l'Etat (gouvernement, ministres, cabinet du président, parlement, police, etc.) puis les médias, les systèmes basés sur l'Internet, les entreprises de télécommunication, les banques et d'autres infrastructures électroniques ont été à leur tour pris pour cibles. Les attaques étaient clairement intentionnelles et il existe de bonnes raisons de penser que leur lancement n'est pas sans relation avec les graves désordres qui se sont produits à Tallinn peu de temps auparavant, à la fin avril.

5. Comme il a déjà été indiqué dans la lettre du rapporteur et des autres parlementaires[2], ce qui fait de ces attaques un événement unique, particulièrement grave, est que, pour la première fois, l'ensemble d'un Etat en a été la cible et qu'elles ont cherché à paralyser le fonctionnement d'infrastructures vitales de la République d'Estonie.

6. La plupart de ces attaques provenaient apparemment de l'extérieur de l'Estonie, d'abord principalement de Russie[3] puis de diverses régions du monde. La plupart des sites Internet de langue russe ont publié des appels encourageant leurs lecteurs à lancer des cyber-attaques, accompagnés d'instructions explicites. D'autres Etats membres ont aussi été la cible de quelques attaques.

[1] Ces événements ont suscité un certain nombre de réactions. Bien que son mandat ne couvre pas la cybercriminalité, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié une déclaration sur les cyber-attaques en Estonie :
http://www.enisa.europa.eu/pages/02_01_press_2007_05_24_ENISA_commenting_on_massive_cyber_attacks_in_Estonia.html

[2] Voir lettre de Kimmo Sasi et autres, datée du 22.05.2007.

[3] Voir *Herald Tribune*, « Estonia says cyber-assault may involve the Kremlin », 17.06.2007 : http://www.iht.com/articles/2007/05/17/news/estonia.php.

7. La cybercriminalité représente un danger pour la démocratie, les droits de l'homme, l'Etat de droit et enfin et surtout la sécurité. Les menaces potentielles comprennent : le cyberterrorisme, c'est-à-dire la mise entièrement hors d'usage d'infrastructures essentielles, ou l'utilisation d'ordinateurs comme des armes afin de rendre inopérants des systèmes vitaux ou de menacer des populations entières.

8. Les événements récents en Estonie montrent que certaines conjectures qui pouvaient sembler paranoïaques sont maintenant devenues réalité. Aucun Etat n'est à l'abri d'un tel danger ; il est donc de la plus haute importance de développer un système efficace de protection et de réponse au niveau international.

II. Portée

9. Les actes de cyberterrorisme peuvent s'attaquer au réseau Internet lui-même (comme cela a été le cas en Estonie) et/ou être commis par le biais de l'Internet. Les attaques peuvent prendre les formes suivantes : cyber-attaques visant à mettre hors d'usage des systèmes électroniques par le biais de l'Internet; diffusion de contenus illégaux ; utilisation des systèmes de technologie de l'information par des terroristes ou d'autres organisations criminelles à des fins de communication ou de logistique.

III. Instruments actuels pertinents pour combattre et prévenir la cybercriminalité

i. Convention sur la cybercriminalité (STE n°185)

10. La Convention du Conseil de l'Europe sur la cybercriminalité (ci-après « la Convention »), datée du 23 novembre 2001, est à ce jour le seul instrument international contraignant sur le sujet ; il s'agit aussi du traité le plus détaillé. La Convention, qui est entrée en vigueur en juillet 2004, fournit des orientations à tous les gouvernements qui souhaitent mettre en place des outils législatifs détaillés pour combattre la cybercriminalité. Elle a été complétée par un Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STCE n°189).

11. La Convention sur la cybercriminalité incrimine – dans la Section 1 consacrée au droit pénal matériel – les « atteintes à l'intégrité des données » (article 4) et les « atteintes à l'intégrité du système » (article 5), qui couvrent les attaques contre les infrastructures essentielles. S'ils le souhaitent, les pays peuvent aller au-delà de ces dispositions en introduisant dans leur législation nationale des mesures plus spécifiques.

12. La Convention prévoit l'incrimination de certaines conduites (droit pénal matériel) telles que l'accès illégal, l'interception illégale, l'atteinte aux données, l'atteinte au système, l'abus de dispositifs, la falsification informatique, la fraude informatique, les infractions se rapportant à la pornographie enfantine et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes (articles 2 à 10).

13. Elle définit également des règles de procédure pour enquêter sur la cybercriminalité et d'autres infractions commises par le biais de systèmes informatiques (articles 16 à 21).

14. La Convention cherche aussi à favoriser le développement d'une coopération internationale efficace pour protéger la société de la cybercriminalité (articles 29 à 35).

15. Il importe de noter que la portée d'application des dispositions procédurales couvre toutes les infractions pénales commises à l'aide d'un système informatique ainsi que la collecte des preuves électroniques (voir article 14). Ces dispositions, par conséquent, s'appliquent non seulement aux conduites incriminées conformément aux dispositions de la Convention (Section 1) mais aussi à tous les actes incriminés par le droit interne de chaque pays. Ces actes comprennent le terrorisme, le blanchiment de capitaux et d'autres infractions commises par le biais de systèmes informatiques (y compris les téléphones portables modernes, par exemple).

16. Lors d'une réunion récente (13-14 juin 2007), le Comité de la Convention cybercriminalité (T-CY), qui tient régulièrement des consultations avec les Parties à la Convention, a examiné les

questions liées au terrorisme. De nombreux participants ont considéré que, bien que la Convention ne mentionne pas spécifiquement ces questions, il n'est pas nécessaire d'y introduire des dispositions spéciales sur le terrorisme. Le Comité d'experts sur le terrorisme (CODEXTER) examine lui aussi la question de savoir si les lacunes des instruments existants - y compris la Convention sur la cybercriminalité - justifient l'élaboration de nouveaux instruments.

ii. Autres instruments juridiques pertinents

17. La Convention pour la prévention du terrorisme (STE n° 196) exige des Etats parties qu'ils incriminent entre autres l'incitation publique à commettre une infraction terroriste ainsi que le recrutement et la formation de terroristes. L'utilisation de l'Internet est couverte puisque la Convention ne précise pas les moyens de communication employés à ces fins.

18. La Décision-cadre du Conseil de l'UE sur les attaques contre les systèmes d'information[4], qui est basée sur la Convention sur la cybercriminalité, a pour but de renforcer la coopération judiciaire en matière pénale dans les affaires d'attaques contre les systèmes d'information en développant des outils et des procédures efficaces. Les infractions pénales passibles de sanctions au titre de la décision-cadre sont : l'accès illicite à un système d'information, l'atteinte à l'intégrité d'un système (atteinte grave au fonctionnement d'un système informatique ou interruption de ce système par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, la modification, la suppression ou le fait de rendre inaccessibles des données informatiques) et l'atteinte à l'intégrité des données.

19. La question du cyberterrorisme est aussi abordée dans la Décision-cadre du Conseil de l'UE relative à la lutte contre le terrorisme.[5]

20. Un certain nombre de conventions et protocoles des Nations Unies conçus pour lutter contre des actes de terrorisme spécifiques peuvent aussi s'appliquer en cas d'attaques commises en manipulant un système informatique ou par le biais du courrier électronique.[6]

IV. Insuffisances du système de protection actuel : aux Etats d'agir

i. Nombre insuffisant des ratifications de la Convention sur la cybercriminalité

21. Le nombre peu élevé de ratifications des instruments légaux montre clairement l'insuffisance du système international actuel de protection contre la cybercriminalité.

22. Puisqu'il est clair que la lutte contre la cybercriminalité exige une action coordonnée au niveau international et l'harmonisation des dispositions légales, seule la pleine application des

---

[4] Voir Décision-cadre du Conseil 2005/222/JAI du 24.02.2005 relative aux attaques visant les systèmes d'information (JOCE L 69/67 du 16.03.2005).

[5] Voir Décision-cadre du Conseil 2002/474/JAI du 13.06.2002 relative à la lutte contre le terrorisme (JOCE L 164/3 du 22 juin 2002), notamment l'article 1 (d) : « *1. Chaque Etat membre prend les mesures nécessaires pour que soient considérés comme infractions terroristes les actes intentionnels visés aux points a) à i), tels qu'ils sont définis comme infractions par le droit national, qui, par leur nature ou leur contexte, peuvent porter gravement atteinte à un pays ou à une organisation internationale lorsque l'auteur les commet dans le but de :*
- gravement intimider une population ou
- contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque ou
- gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou d'une organisation internationale ;
(…)
*d) le fait de causer des destructions massives à une installation gouvernementale ou publique, à un système de transport, à une infrastructure, **y compris un système informatique**, à une plate-forme fixe située sur le plateau continental, à un lieu public ou une propriété privée susceptible de mettre en danger des vies humaines ou de produire des pertes économiques considérables* » (c'est moi qui souligne).

[6] Par exemple, la Convention sur la suppression de la saisie illégale des avions, la Convention pour la suppression des actes illégaux contre la sécurité de l'aviation civile, le Protocole pour la suppression des activités illégales (violence) dans l'environnement aéroportuaire (aviation civile), la Convention sur la prévention et la condamnation des activités criminelles contre les personnes protégées selon les normes internationales et la Convention internationale contre la prise d'otages.

instruments juridiques internationaux pertinents peut constituer une réponse efficace et satisfaisante à ce type de danger.

23. A ce jour, la Convention sur la cybercriminalité a été ratifiée par 21 pays (Etats membres du CdE[7] et Etats-Unis)[8] et signée par 22 autres (Etats membres[9] ainsi que le Canada, le Japon et l'Afrique du Sud). Le Costa Rica et le Mexique ont été invités à adhérer à la Convention. Dans le monde entier, de nombreux autres pays réforment actuellement leur législation en se servant de la Convention (Argentine, Brésil, Costa Rica, Égypte, Inde, Mexique, Philippines).

24. L'Assemblée devrait inviter les Etats membres qui ne l'ont pas encore fait à signer, ratifier et mettre en œuvre dès que possible la Convention et son Protocole additionnel.

ii. Besoin d'une coordination des mesures de lutte contre la cybercriminalité

25. La question de la cybercriminalité fait actuellement l'objet de discussions approfondies au niveau international. Les 11 et 12 juin, la Conférence Octopus Interface « Coopération contre la cybercriminalité »[10], qui s'est tenue à Strasbourg, a abordé les points suivants :

- l'identification des nouvelles menaces en matière de cybercriminalité ;
- l'efficacité de la législation adoptée pour combattre la cybercriminalité ;
- les initiatives d'autres organisations et parties prenantes ;
- les partenariats public-privé ;
- la coopération internationale et le fonctionnement des points de contact 24/7.[11]

26. La Convention sur la cybercriminalité met fortement l'accent sur les formes concrètes de coopération (voir notamment l'article 35). Comme le déclare le préambule de la Convention, la lutte contre la cybercriminalité requiert *« une coopération internationale en matière pénale accrue, rapide et efficace »*.[12]

27. La Présidence allemande du Conseil européen a lancé récemment une initiative appelée *« Check the web »* qui vise à favoriser l'adoption de mesures vigoureuses pour lutter contre l'utilisation de l'Internet par des organisations terroristes.[13] Le rapporteur attire à cet égard l'attention sur le futur portail d'information d'Europol qui devrait devenir une véritable plate-forme technique pour l'échange d'information entre les Etats membres.

28. A la suite des cyber-attaques en Estonie, la Commission européenne a aussi lancé un appel urgent à coordonner les efforts de lutte contre la cybercriminalité au niveau international.[14] Par

---

[7] Albanie, Arménie, Bosnie-Herzégovine, Bulgarie, Croatie, Chypre, Danemark, Estonie, Finlande, France, Hongrie, Islande, Lettonie, Lituanie, Pays-Bas, Norvège, Roumanie, Slovénie, « l'ex-République yougoslave de Macédoine », Ukraine (à la date du 22.06.2007).

[8] La Finlande a ratifié la Convention en mai 2007. Des discussions sont en cours avec la Fédération de Russie au sujet de l'interprétation d'un article particulier afin de permettre à la Fédération de Russie de signer et de ratifier ce traité dès que possible.

[9] Autriche, Belgique, République Tchèque, Allemagne, Grèce, Irlande, Italie, Luxembourg, Malte, Moldova, Monténégro, Pologne, Portugal, Serbie, Slovaquie, Espagne, Suède, Suisse, Royaume-Uni (à la date du 22.06.2007).

[10] Pour plus de détails, voir http://www.coe.int/t/dc/files/themes/cybercriminalité/default_en.asp.

[11] « Réseau 24/7 » : points de contact joignables 24 heures sur 24, 7 jour sur 7.

[12] La Convention européenne d'entraide judiciaire en matière pénale (STE n° 30) et ses deux protocoles additionnels fournissent un cadre légal à la coopération internationale mais prévoient aussi de nombreuses possibilités de refuser de coopérer.

[13] Voir Conclusions du Conseil sur la coopération pour combattre l'utilisation de l'Internet par des organisations terroristes (*« Check the web »*), 8457/3/07 REV 3, ENFOPOL 66, 29.05.2007.

[14] Voir http://www.infoworld.com/article/07/05/22/EC-urges-effort-against-cybercriminalité_1.html et *Business Week*, « Brussels to wage war on cybercriminalité », 23.05.2007 : http://www.businessweek.com/globalbiz/content/may2007/gb20070523_811592.htm?chan=globalbiz_europe+index+page_top+stories

ailleurs, lors de sa réunion des 21 et 22 juin 2007, le Conseil européen a préconisé l'élaboration d'un cadre d'action dans le domaine de la lutte contre la cybercriminalité[15].

29. La lutte contre la cybercriminalité requiert bien entendu, plus que la lutte contre d'autres formes de criminalité, une coopération internationale réelle et efficace. Des efforts ont été engagés pour renforcer cette coopération mais ils doivent être suivis de mesures concrètes. L'harmonisation de la législation pertinente doit être l'une des priorités, afin de supprimer tout obstacle législatif à la coopération.

iii. Nécessité de « sanctions effectives, proportionnées et dissuasives »

30. Comme l'exige l'article 13 de la Convention sur la cybercriminalité, les législations nationales doivent sanctionner les atteintes à l'intégrité des systèmes informatiques, y compris lorsque celles-ci sont le fait d'organisations terroristes. Les sanctions doivent être *« effectives, proportionnées et dissuasives »*.

31. Il est demandé aux Etats parties d'incriminer largement les attaques terroristes s'appuyant sur les technologies de l'information, ainsi que les attaques dirigées contre d'autres intérêts qui dépendent fortement des systèmes informatiques. Il convient de noter que la Convention sur la cybercriminalité ne fait pas de l'atteinte à des biens, à la vie ou au bien-être une condition préalable à l'imposition de sanctions.

32. La Décision-cadre du Conseil de l'UE stipule aussi que les Etats membres doivent prendre les mesures nécessaires pour que les infractions d'accès illicite à un système d'information, d'atteinte à l'intégrité d'un système et d'atteinte à l'intégrité des données soient passibles de sanctions effectives, proportionnées et dissuasives. Elle exige également que l'incitation, la complicité et la tentative de commettre l'une de ces infractions soient passibles de sanctions (article 5).

33. L'Assemblée, par conséquent, devrait inviter les Etats membres à examiner leurs cadres légaux respectifs afin d'établir s'ils sanctionnent de façon adéquate les infractions qui relèvent de la cybercriminalité – en particulier les attaques terroristes effectuées par le biais de systèmes informatiques – et à amender leur législation si nécessaire.

V. Conclusions

34. La coopération au niveau international est un facteur essentiel d'une protection et d'une prévention efficaces en matière de cybercriminalité. Les mesures prises par quelques Etats seulement sont vouées à l'échec car ce type de criminalité ignore les frontières. Les efforts qui sont engagés actuellement et seront engagés à l'avenir au niveau international devraient être axés en priorité sur la mise en place dans les différentes législations nationales de dispositions adéquates et harmonisées aux fins de la prévention et de la répression de la cybercriminalité. Cet objectif doit bien entendu être accompli dans le respect des libertés civiles.[16]

---

[15] Voir les conclusions de la présidence du Conseil de l'Europe de Bruxelles des 21 et 22.06.2007, § 31, http://europa.eu/rapid/pressReleasesAction.do?reference=DOC/07/2&format=PDF&aged=0&language=FR&guiLanguage=en.

[16] Voir, par exemple, *Weber et Saravia c. Allemagne* (requête n° 54934/00 du 29.06.2006) qui porte sur une affaire d'interception des télécommunications par les autorités publiques (en particulier § 95). Cette affaire est indirectement pertinente dans la mesure où la Cour n'a pas encore rendu d'arrêt sur un cas se rapportant directement à la cybercriminalité. Elle porte sur les dispositions de la loi allemande du 13.08.1968 qui définit les restrictions au secret de la correspondance postale et des télécommunications ; la requérante, dont plusieurs conversations téléphoniques avaient été interceptées, considérait que ses droits fondamentaux avaient été atteints. La question essentielle était celle de savoir si le gouvernement avait outrepassé ses pouvoirs en surveillant certaines communications afin de capturer des terroristes. On peut considérer que les « télécommunications » couvrent l'Internet puisque celles-ci sont définies en des termes assez généraux (« la transmission d'information, sous forme de mots, de sons ou d'images, généralement sur de grandes distances, par le biais de signaux électromagnétiques tels ceux employés par le télégraphe, le téléphone, la radio et la télévision »). Dans sa décision, la Cour évoque aussi en termes assez généraux la « transmission de données personnelles » et ne se réfère pas de façon spécifique aux seules communications téléphoniques. La Cour a considéré qu'il n'y avait pas eu violation de la Convention et a déclaré l'affaire irrecevable.

35. L'Assemblée devrait appeler les Etats membres à coordonner l'application des instruments existants. Naturellement, étant donnés la nature même de la cybercriminalité et ses liens étroits avec l'évolution constante des technologies, une certaine flexibilité est absolument nécessaire. La Convention sur la cybercriminalité devrait par conséquent faire l'objet d'un réexamen régulier afin d'évaluer sa capacité à répondre aux nouveaux défis résultant des avancées technologiques.

36. La protection offerte par les instruments internationaux existants apparaît assez détaillée et couvre toutes les cyber-attaques graves. D'autre part, le CODEXTER du Conseil de l'Europe examine actuellement les lacunes éventuelles de la protection. Par conséquent, l'Assemblée devrait s'abstenir à ce stade de recommander l'élaboration d'un projet de Protocole additionnel à la Convention sur la cybercriminalité et attendre les conclusions du CODEXTER.

Doc. 11325

Commission chargée du rapport: commission des questions juridiques et des droits de l'homme

Renvoi en commission: Demande de débat d'urgence, renvoi n°3365 du 25 juin 2007

Projet de résolution adopté à l'unanimité par la commission le 26 juin 2007

Membres de la commission: M. Dick **Marty** (Président), M. Erik **Jurgens**, M. György Frunda, Mme Herta Däubler-Gmelin (Vice-présidents), M. Athanasios **Alevras**, M. Miguel Arias (remplaçant : M. Miguel **Barceló Pérez**), Mme Aneliya Atanasova, M. Abdülkadir Ateş, M. Jaume **Bartumeu Cassany**, Mme Meritxell Batet, Mme Soledad Becerril, Mme Marie-Louise **Bemelmans-Videc**, M. Erol Aslan Cebeci, Mme Pia Christmas-Møller, Mme Ingrīda **Circene**, Mme Lydie Err, M. Valeriy **Fedorov**, M. Aniello Formisano, M. Jean-Charles Gardetto, M. József Gedei, M. Stef Goris, M. Valery Grebennikov, Mme Carina Hägg, M. Holger **Haibach**, Mme Gultakin Hajiyeva, Mme Karin Hakl, M. Nick Harvey, M. Andres **Herkel**, M. Serhiy **Holovaty**, M. Michel Hunault, M. Rafael Huseynov, Mme Fatme Ilyaz, M. Kastriot Islami, M. Željko Ivanji, Mme Kateřina Jacques, M. Karol Karski (remplaçante : Mme Ewa **Tomaszewska**), M. Hans Kaufmann, M. András Kelemen, Mme Kateřina Konečná, M. Nikolay Kovalev (remplaçant : M. Yuri **Sharandin**), M. Jean-Pierre Kucheida, M. Eduard Kukan, Mme Darja **Lavtižar-Bebler**, M. Andrzej Lepper (remplaçant : M. Krzysztof **Lisek**), Mme Sabine **Leutheusser-Schnarrenberger**, M. Tony Lloyd, M. Humfrey **Malins**, M. Andrija Mandic, M. Pietro Marcenaro, M. Alberto Martins, M. Andrew McIntosh, M. Murat Mercan, Mme Ilinka **Mitreva**, M. Philippe Monfils, M. João Bosco Mota Amaral, M. Philippe Nachbar, Mme Nino Nakashidzé, M. Tomislav Nikolić, Ms Ann Ormonde, M. Claudio Podeschi, M. Ivan **Popescu**, Mme Maria **Postoico**, Mme Marietta **de Pourbaix-Lundin**, M. Christos Pourgourides, M. Jeffrey Pullicino Orlando, M. Valeriy Pysarenko, M. François Rochebloine, M. Francesco Saverio Romano, M. Armen Rustamyan, M. Kimmo **Sasi**, M. Ellert Schram, M. Christoph **Strässer**, M. Mihai Tudose, M. Vasile Ioan Dănuț **Ungureanu**, M. Øyvind **Vaksdal**, M. Egidijus **Vareikis**, M. Miltiadis **Varvitsiotis**, Mme Renate **Wohlwend**, M. Marco Zacchera, M. Krysztof **Zaremba**, M. Vladimir Zhirinovsky, M. Miomir Žužul

*N.B. Les noms des membres qui ont participé à la réunion sont indiqués en **gras***

Secrétariat de la commission: M. Drzemczewski, M. Schirmer, Mme Maffucci-Hugel, Mlle Heurtin, Mme Schuetze-Reymann