Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Résolution 1565 (2007)[1]

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

Assemblée parlementaire

1. L'Assemblée parlementaire rappelle son Avis no 226 (2001) sur le projet de convention sur la cybercriminalité 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 stabilité démocratique et la sécurité nationale, et qu'elle pose des problèmes fondamentaux quant au respect des droits de l'homme et de l'Etat de droit; par conséquent, cette question devrait être traitée avec une priorité absolue.

3. Les attaques à motifs politiques contre des sites militaires ou gouvernementaux de plusieurs Etats membres et observateurs du Conseil de l'Europe sont de plus en plus fréquentes et sophistiquées. Pour la première fois, en effet, des cyberattaques criminelles ont pris pour cible l'ensemble d'un Etat, en tentant de paralyser le fonctionnement d'infrastructures vitales de la République d'Estonie. Quelques attaques ont été constatées dans d'autres pays au même moment.

4. Cela montre que la cybercriminalité est un danger réel, qui doit être pris au sérieux à l'échelon le plus élevé, et qu'elle représente une véritable menace pour les Etats dont les infrastructures fondées sur les technologies peuvent être paralysées ou même détruites. Cette menace peut provenir de particuliers, de groupes organisés ou d'Etats.

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 no 185, ci-après «la convention») contient des dispositions détaillées pour combattre les cyberattaques 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 devraient donc 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 rappelle aussi qu'avec la Convention du Conseil de l'Europe pour la prévention du terrorisme (STCE no 196) on dispose d'un instrument supplémentaire dans la lutte contre le cyberterrorisme, ainsi que contre l'utilisation de l'internet à des fins terroristes.

8. L'Assemblée déplore le fait que de nombreux Etats membres et observateurs n'aient pas encore ratifié ces importantes conventions.

---

1. Discussion par l'Assemblée le 28 juin 2007 (25e séance) (voir Doc. 11325, rapport de la commission des questions juridiques et des droits de l'homme, rapporteur: M. Sasi; Doc. 11335, avis de la commission des questions politiques, rapporteur: M. Agramunt; et Doc. 11333, avis de la commission des questions économiques et du développement, rapporteur: Mme Lilliehöök). Texte adopté par l'Assemblée le 28 juin 2007 (25e séance).

9. L'Assemblée note que la lutte contre la cybercriminalité requiert d'urgence une coopération internationale entre les gouvernements, le secteur privé et les organisations non gouvernementales, car les cybercriminels comptent sur leur aptitude à opérer à travers les frontières et mettent à profit les différences entre les législations nationales. L'absence de coopération entre les Etats membres expose ces derniers à des risques très graves.

10. 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.

11. A cet égard, l'Assemblée se félicite des diverses initiatives mises en œuvre pour renforcer la coopération et la coordination internationales 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 leurs efforts pour renforcer la coopération internationale et soutenir la coordination des mesures concrètes adoptées en vue d'une protection plus efficace.

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

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

14. Les cyberattaques 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. Ce faisant, ils devraient faire participer à cet effort des acteurs privés, y compris les industries des ordinateurs, des réseaux et des logiciels.

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

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

15.2. à signer et à ratifier sans tarder la Convention du Conseil de l'Europe pour la prévention du terrorisme, ainsi que la Convention sur la cybercriminalité et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE no 189), et à en assurer la pleine mise en œuvre dès que possible;

15.3. à 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 à amender si nécessaire leur législation en assurant pleinement le respect des libertés individuelles, notamment la liberté d'expression et la liberté d'information;

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

15.5. à élaborer un cadre destiné à faciliter les consultations politiques et l'échange d'informations en urgence, à tous les niveaux nécessaires des pays concernés, en cas de cyberattaque de grande ampleur;

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

15.7. à associer plus étroitement le secteur privé, notamment en instaurant des partenariats entre les secteurs public et privé en vue d'une coopération transsectorielle internationale plus efficace contre la cybercriminalité;

15.8. à prendre des mesures nationales efficaces en vue de prévenir les activités cybercriminelles;

15.9. à apporter toute l'assistance nécessaire au Gouvernement de l'Estonie pour garantir qu'il puisse réaliser une enquête complète et exhaustive sur les récentes cyberattaques survenues dans ce pays, et afin de soutenir par les informations ainsi obtenues les efforts futurs de lutte internationale contre la cybercriminalité.

16. L'Assemblée, tout en considérant que la convention devrait faire l'objet d'un réexamen régulier à la lumière des progrès technologiques et des nouveaux défis, 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. L'Assemblée entend revenir sur cette question dès que possible.