Organisation pour la sécurité et la coopération en Europe
Conseil ministériel
Bruxelles 2006

MC.DEC/7/06
5 décembre 2006

FRANÇAIS
Original : ANGLAIS

Deuxième jour de la quatorzième Réunion
MC(14) Journal No 2, point 8 de l'ordre du jour

DECISION No 7/06
LUTTE CONTRE L'UTILISATION DE L'INTERNET A DES FINS TERRORISTES

Le Conseil ministériel,

Rappelant sa décision précédente sur la question (MC.DEC/3/04),

Restant vivement préoccupé par l'utilisation croissante d'Internet à des fins terroristes, comme l'indiquent la décision susmentionnée et les documents ultérieurs,

Réaffirmant dans ce contexte qu'il est important de respecter pleinement le droit à la liberté d'opinion et d'expression, lequel englobe la liberté de rechercher, de recevoir et de communiquer des informations, qui sont vitales pour la démocratie et sont d'ailleurs renforcées par l'Internet (PC.DEC/633 du 11 novembre 2004) et la primauté du droit,

Sachant que la résolution 1624 (2005) du Conseil de sécurité des Nations Unies appelle les Etats à adopter toutes mesures nécessaires et appropriées et conformes aux obligations qui leur incombent en vertu du droit international, pour interdire par la loi l'incitation à commettre des actes de terrorisme et empêcher toute incitation à commettre de tels actes,

Réaffirmant nos engagements au titre de la Stratégie antiterroriste mondiale de l'Organisation des Nations Unies, en particulier « de coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et dans toutes ses manifestations sur l'Internet » et « d'utiliser l'Internet comme un outil pour faire échec au terrorisme, tout en reconnaissant que les Etats pourront avoir besoin d'une assistance à cet égard »,

Notant l'observation figurant dans le rapport du Comité des Nations Unies contre le terrorisme (S/2006/737 du 15 septembre 2006) selon laquelle plusieurs Etats ont informé le Comité qu'ils envisageaient dans leur législation nationale d'appliquer à l'Internet l'interdiction de l'incitation,

Prenant note des développements récents, en particulier la Convention du Conseil de l'Europe pour la prévention du terrorisme, concernant les obligations des Etats parties à la

Convention d'ériger en infractions pénales la provocation publique à commettre des infractions terroristes, ainsi que le recrutement et l'entraînement pour le terrorisme,

Rappelant la Convention du Conseil de l'Europe sur la cybercriminalité (2001), seul et unique instrument multilatéral juridiquement contraignant, qui traite spécifiquement de la cybercriminalité, notamment en fournissant un cadre juridique commun pour la coopération internationale entre les Etats parties à la Convention pour lutter contre la cybercriminalité, et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques,

Saluant l'engagement pris par le Sommet du G8 (Saint-Pétersbourg, Fédération de Russie, 16 juillet 2006) à contrer efficacement les tentatives d'utilisation abusive du cyberespace à des fins terroristes, y compris l'incitation à commettre des actes terroristes, à communiquer et planifier des actes terroristes, ainsi que le recrutement et l'entrainement de terroristes, et notant en particulier le rôle du réseau 24/7 sur la criminalité informatique établi par le G8 pour contrer le comportement délictueux dans le cyberespace,

Rappelant les résultats de la Réunion spéciale de l'OSCE sur la relation entre la propagande raciste, xénophobe et antisémite sur Internet et les crimes inspirés par la haine (Paris, 15-16 juin 2004), ainsi que les résultats de l'Atelier d'experts de l'OSCE sur la lutte contre l'utilisation d'Internet à des fins terroristes (Vienne, 13-14 octobre 2005) ainsi que l'Atelier d'experts conjoint de l'OSCE et du Conseil de l'Europe sur la prévention du terrorisme : lutte contre l'incitation et les activités terroristes connexes (Vienne, 19-20 octobre 2006) et les activités pertinentes réalisées par le Secrétariat et les institutions de l'OSCE, en particulier par le Représentant pour la liberté des médias et le BIDDH,

Prenant en considération les différentes approches nationales lors de la définition d'un contenu « illégal » et « répréhensible » ainsi que les différentes méthodes d'examen du contenu illégal et répréhensible dans le cyberespace, allant notamment de l'utilisation possible de renseignements recueillis en analysant le trafic et le contenu d'Internet à la fermeture de sites Web des organisations terroristes et de ceux qui les soutiennent,

Préoccupé par les attaques continues de pirates, qui bien qu'elles ne soient pas liées au terrorisme, n'en témoignent pas moins des connaissances existantes dans ce domaine et offrent de ce fait un risque de cyberattaques terroristes contre les systèmes informatiques, touchant les activités des infrastructures sensibles, des institutions financières ou d'autres réseaux vitaux,

1. Décide d'intensifier l'action de l'OSCE et de ses Etats participants, notamment en renforçant la coopération internationale pour contrer l'utilisation de l'Internet à des fins terroristes ;

2. Appelle les Etats participants à envisager de prendre toutes les mesures appropriées pour protéger les infrastructures et réseaux vitaux d'informations sensibles contre la menace de cyberattaques ;

3. Appelle les Etats participants à envisager de devenir parties aux instruments juridiques régionaux et internationaux existants, notamment aux Conventions du Conseil de l'Europe sur la cybercriminalité (2001) et pour la prévention du terrorisme (2005) et à mettre en œuvre leurs obligations relevant de ces instruments ;

4. Encourage les Etats participants à s'associer au réseau 24/7, établi par le G8, et à désigner une personne/unité appropriée de contact pour ce réseau afin de rationaliser la coopération internationale entre les services de détection et de répression pour contrer l'utilisation abusive du cyberespace à des fins criminelles ainsi que dans les affaires pénales qui impliquent des preuves électroniques, le cas échéant ;

5. Appelle les Etats participants, appelés à examiner un contenu qui est illégal selon leur législation nationale et relève de leur juridiction, à prendre toutes les mesures appropriées contre un tel contenu et à coopérer avec d'autres Etats intéressés, dans le respect de leur législation nationale et de la primauté du droit, et conformément à leurs obligations internationales, notamment au droit international relatif aux droits de l'homme ;

6. Invite les Etats participants à renforcer leur surveillance des sites Web des organisations terroristes/extrémistes violentes et de ceux qui les soutiennent et à accroitre leurs échanges d'information au sein de l'OSCE et d'autres instances pertinentes sur l'utilisation de l'Internet à des fins terroristes ainsi que sur les mesures prises pour la contrecarrer, conformément à leur législation nationale, tout en assurant le respect des obligations et des normes internationales en matière de droits de l'homme, notamment celles concernant les droits à la prie privée et à la liberté d'opinion et d'expression, et la primauté du droit. Les chevauchements avec les activités en cours dans d'autres instances internationales devrait être évitée ;

7. Recommande aux Etats participants d'envisager la possibilité d'un engagement plus actif de la part des institutions de la société civile et du secteur privé pour prévenir et contrer l'utilisation de l'Internet à des fins terroristes ;

8. Encourage les Etats participants à prendre part à la conférence politique de l'OSCE qui se déroulera en mai 2007 sur le partenariat public-privé dans la lutte contre le terrorisme, à Vienne, et qui sera axée sur le rôle vital que le secteur privé, notamment les milieux d'affaires, la société civile et les médias peuvent jouer en coopération avec les gouvernements pour prévenir et combattre le terrorisme ;

9. Charge le Secrétaire général de promouvoir, en particulier par l'intermédiaire du Réseau contre-terrorisme de l'OSCE, l'échange d'informations sur la menace que constitue l'utilisation de l'Internet à des fins terroristes, notamment l'incitation, le recrutement, la collecte de fonds, l'entraînement, et la planification ciblée d'actes terroristes, ainsi que sur des mesures législatives et autres prises pour contrer cette menace.