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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 14055
04 mai 2016

Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet

Réponse à Recommandation[1]: Recommandation 2077 (2015)
Comité des Ministres

1. Le Comité des Ministres a procédé à un examen approfondi de la Recommandation 2077 (2015) de l'Assemblée parlementaire intitulée «Renforcer la coopération contre le bioterrorisme et d'autres attaques de grande ampleur sur internet». Il a communiqué la recommandation au Comité directeur sur les médias et la société de l'information (CDMSI), au Comité d'experts sur le terrorisme (CODEXTER) et au Comité de la Convention sur la cybercriminalité (T-CY), pour information et éventuelles observations.

2. Le Comité des Ministres estime que les attaques de grande ampleur commises par l'intermédiaire de systèmes informatiques représentent une menace grave non seulement pour la sécurité nationale, la sûreté publique, le bien-être économique des sociétés et l'intégrité de l'infrastructure d'internet, mais aussi pour l'exercice et la jouissance sur internet des droits de l'homme, en particulier la liberté d'expression, l'accès à l'information et le respect de la vie privée. Le Comité salue les efforts que déploie l'Assemblée pour renforcer la coopération internationale contre la cybercriminalité et se félicite de l'importance de la place qu'elle accorde à la Convention sur la cybercriminalité (STE n° 185) à cet égard. Il rappelle que la Convention est un traité de justice pénale qui s'applique à la cybercriminalité et aux preuves électroniques dans le cadre d'une infraction pénale quelle qu'elle soit. Les «attaques de grande ampleur» contre les systèmes informatiques et l'utilisation de ces systèmes à des fins terroristes sont des questions de sûreté publique; elles entrent donc dans le champ d'application de ce traité.

3. Pour ce qui est de la recommandation de l'Assemblée de réaliser une étude de faisabilité concernant l'élaboration d'un protocole additionnel à la Convention sur la cybercriminalité qui définisse un niveau commun d'incrimination des cyberattaques de grande ampleur (paragraphe 3.1.1), le Comité des Ministres observe qu'en juin 2013, le T-CY a adopté des Notes d'orientation sur les attaques par déni de service distribué, sur les attaques visant les infrastructures critiques, sur les Botnets et sur les nouvelles formes de logiciels malveillants. Ces Notes donnent aux Parties à la Convention sur la cybercriminalité des indications sur l'utilisation des dispositions figurant déjà dans ladite convention pour faire face aux «cyberattaques de grande ampleur». Les Notes d'orientation appellent ainsi les Parties «à faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques soient passibles de sanctions effectives, proportionnées et dissuasives». Le troisième cycle d'évaluations du T-CY a été lancé en juillet 2015; il porte sur l'article 13 de la Convention. Dans le questionnaire relatif à l'évaluation de l'article 13, il est expressément demandé s'il est tenu compte de circonstances aggravantes dans l'incrimination et la sanction des infractions commises contre les systèmes informatiques et au moyen de ceux-ci.

4. L'Assemblée parlementaire propose également une étude de faisabilité concernant l'élaboration d'un protocole additionnel sur l'entraide en matière de pouvoirs d'investigation qui étende le champ d'application de l'article 32 de la Convention (paragraphe 3.1.2). A cet égard, le Comité des Ministres renvoie à la Note d'orientation sur le champ d'application de l'article 32, adoptée par le T-CY en décembre 2014, dans laquelle il a indiqué en conclusion «qu'un protocole additionnel sur l'accès transfrontalier aux données serait nécessaire» compte tenu, entre autres, du coût que représentent ces crimes pour les droits de l'homme et les

1. Adoptée à la 1254e réunion des Délégués des Ministres (27 avril 2016).

libertés fondamentales, dont le droit au respect de la vie privée, et de leurs conséquences pour les victimes. Toutefois, dans le même temps, le T-CY a observé qu'un tel protocole ferait polémique dans le contexte actuel et qu'«il n'y a pas de consensus raisonnable pour commencer les travaux sur un protocole». Le T-CY a décidé d'«être attentif à la suite des événements et [de] réexaminer à l'avenir la faisabilité d'un protocole consacré à la question spécifique de l'accès transfrontalier aux données». Le Comité des Ministres a l'intention de suivre la question de près et tiendra l'Assemblée informée des développements en la matière.

5. En ce qui concerne une éventuelle étude de faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité concernant l'accès de la justice pénale aux dossiers stockés sur des serveurs d'hébergement dans le nuage (paragraphe 3.2), le Comité des Ministres relève que le T-CY a mis en place un groupe de travail sur la question. Ce groupe étudie l'opportunité d'un protocole additionnel à la Convention et devrait achever ses travaux en décembre 2016. Le Comité des Ministres tiendra l'Assemblée informée des développements en la matière.

6. En ce qui concerne le paragraphe 3.3 de la recommandation de l'Assemblée sur l'élaboration de normes juridiques sur la responsabilité internationale qui revient aux Etats de prendre des mesures visant à prévenir des cyberattaques de grande ampleur, le Comité des Ministres rappelle sa Recommandation CM/Rec(2011)8 aux Etats membres sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet qui énonce les principes fondamentaux régissant la coopération internationale, tels que la notification, le partage d'informations, la consultation et l'assistance mutuelle. Il rappelle également sa Recommandation CM/Rec(2015)6 aux Etats membres sur la libre circulation transfrontière des informations sur internet.

7. Enfin, en ce qui concerne la proposition de renforcer les actions d'assistance et de suivi (paragraphe 3.4), le Comité des Ministres rappelle que l'évaluation de la mise en œuvre de la Convention sur la cybercriminalité est une mission essentielle du T-CY. Deux cycles d'évaluation ont été menés depuis 2012 et un troisième (sur les sanctions et les mesures) est en cours. Les dispositions couvertes par ces évaluations concernent, entre autres, «les attaques de grande ampleur». Le Comité des Ministres relève également que des activités approfondies de renforcement des capacités sont menées via le Bureau du Conseil de l'Europe pour le programme sur la cybercriminalité (C-PROC) à Bucarest, Roumanie et que ces activités concourent au renforcement des capacités pour faire face aux «attaques de grande ampleur».