www.coe.int/TCY

Strasbourg, le 15 octobre 2015 T-CY (2015)19 F

Comité de la Convention cybercriminalité (T-CY)

Avis du T-CY sur la Recommandation 2077 (2015) de l'Assemblée parlementaire du Conseil de l'Europe Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet

Adopté par le T-CY le 13 octobre 2015 par procédure écrite

Avis du T-CY sur la
Recommandation 2077 (2015) de l'Assemblée parlementaire du Conseil de l'Europe « Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet »[1]

1. A leur 1233e session (8 juillet 2015), les Délégués des Ministres ont décidé de communiquer la Recommandation 2077 (2015) de l'Assemblée parlementaire intitulée « Accroître la coopération contre le cyber terrorisme et d'autres attaques de grande ampleur sur Internet » entre autres au Comité de la Convention cybercriminalité (T-CY) pour commentaires avant le 22 octobre 2015[2].

2. Le T-CY salue les efforts accomplis par l'Assemblée parlementaire pour renforcer la coopération internationale contre la cybercriminalité et se félicite de la place importante qu'elle accorde à la Convention sur la cybercriminalité (STE 185) à cet égard.

3. Le T-CY rappelle que la Convention sur la cybercriminalité 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[3] sont des questions de sécurité publique ; elles entrent donc dans le champ d'application de ce traité.

4. S'agissant de la recommandation 3.1.1 (étude de faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité (STE 185) définissant un niveau commun d'incrimination des cyberattaques de grande ampleur), le T-CY souhaite formuler les commentaires suivants :

- En juin 2013, le T-CY a adopté des Notes d'orientation[4] 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 apportent aux Parties à la Convention sur la cybercriminalité des orientations utiles sur l'utilisation des dispositions existantes de la Convention pour faire face aux « cyberattaques de grande ampleur ». Ces documents appellent 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, comprenant des peines privatives de liberté. »
- Le troisième cycle d'évaluation du T-CY, lancé en juillet 2015, couvre l'article 13 de la Convention intitulé « Sanctions et mesures ». Dans le questionnaire relatif à l'évaluation de l'article 13, il est expressément demandé si les circonstances aggravantes sont bien prises en compte dans l'incrimination la sanction des infractions contre les systèmes informatiques et au moyen de ces systèmes. Les résultats sont attendus pour la mi-2016.
- La mise en œuvre de l'article 13 garantit que les « cyberattaques de grande ampleur » sont traitées de façon proportionnée.

---

[1] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21976&lang=fr

[2] https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/Dec%282014%291198/3.1&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

[3] Le T-CY n'a pas connaissance d'une définition admise du terme « cyberterrorisme ».

[4] http://www.coe.int/fr/web/cybercrime/guidance-notes

5. S'agissant de la recommandation 3.1.2 (étude de faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité (STE 185) en vue d'étendre le champ d'application de l'article 32), le T-CY souhaite formuler les commentaires suivants :

- S'agissant du champ d'application de l'article 32, le T-CY a adopté une Note d'orientation en décembre 2014[5].
- Le T-CY réfléchit intensément depuis 2010 au problème de l'accès transfrontalier des données et à d'autres solutions qui dépasseraient le cadre de l'article 32, notamment via un groupe de travail spécifique (le « groupe sur l'accès transfrontalier »), qui a achevé ses travaux en décembre 2014.
- En décembre 2014, le T-CY a conclu « 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 , notamment en ce qui concerne le droit à la vie privée, et des conséquences de l'infraction sur les victimes[6].
- Parallèlement, le T-CY est arrivé à la conclusion 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 donc 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 ».

6. S'agissant de la recommandation 3.2 (étude de faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité (STE 185) concernant l'accès de la justice pénale aux données stockées sur des serveurs d'hébergement dans le nuage), le T-CY souhaite formuler les commentaires suivants :

- En décembre 2014, le T-CY a créé un nouveau groupe de travail sur l'accès de la justice pénale aux preuves stockées dans le nuage, notamment par le biais d'une entraide judiciaire (le « Groupe sur les preuves dans le nuage »).
- Ce groupe s'appuie sur les travaux du groupe sur l'accès frontalier et sur les résultats de l'évaluation des dispositions relatives à l'entraide judiciaire figurant dans la Convention sur la cybercriminalité. Ces résultats ont été adoptés par le T-CY en décembre 2014[7].
- Le groupe étudie l'opportunité d'un rapport additionnel à la Convention sur la cybercriminalité. Il devrait achever ses travaux d'ici à décembre 2016. Un document de réflexion sur les problèmes rencontrés par les autorités de justice pénale[8] a été publié en mai 2015.

---

[5] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297F_REV_GN3_transborder_V13.pdf

[6] « [...] De nombreux interlocuteurs ont tendance à négliger le coût de ce type de criminalité pour les droits de l'homme, notamment en ce qui concerne la vie privée, les conséquences de l'infraction sur la victime et l'obligation positive de l'Etat de protéger les personnes contre la criminalité, y compris la cybercriminalité. Le manque de considération pour les droits des victimes a été une révélation pénible pour le groupe sur l'accès transfrontalier ».

http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282014%2916F_TBGroupReport_v16.pdf

[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

[8] https://rm.coe.int/CoERMPublicCommonSearchServices/sso/SSODisplayDCTMContent?documentId=09000016803053cb&ticket=ST-84466-pJVl5gH0BUzsAMpfrXGO-cas

7. S'agissant de la recommandation 3.4 (renforcer les actions d'assistance et de contrôle relatives à la Convention sur la cybercriminalité (STE 185) dans le droit et la pratique internes), le T-CY souhaite formuler les commentaires suivants :

- Evaluer la mise en œuvre de la Convention sur la cybercriminalité est une mission essentielle du T-CY. Deux cycles d'évaluation ont été achevés depuis 2012 et un troisième (sur les sanctions et les mesures) est en cours. Les dispositions couvertes par ces évaluations concernent également les « attaques de grande ampleur ». Des ressources supplémentaires sont nécessaires pour renforcer « les actions d'assistance et de contrôle relatives à la mise en œuvre de la Convention sur la cybercriminalité (STE 185) dans le droit et la pratique internes », notamment au vu du nombre croissant de Parties.
- Des activités approfondies de renforcement des capacités sont menées avec efficacité et à moindre coût par le bureau du Conseil de l'Europe pour le Programme sur la cybercriminalité (C-PROC), à Bucarest, en Roumanie. Ces activités permettent aussi de renforcer les capacités pour répondre aux « attaques de grande ampleur ».

Annexe: PACE Recommandation 2077 (2015)

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

Auteur(s) : Assemblée parlementaire

Origine - *Discussion par l'Assemblée* le 26 juin 2015 (27e séance) (voir Doc. 13802, rapport de la commission de la culture, de la science, de l'éducation et des médias, rapporteur: M. Hans Franken). *Texte adopté par l'Assemblée* le 26 juin 2015 (27e séance).

1. L'Assemblée parlementaire se réfère à sa Résolution 2070 (2015) «Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet».

2. Elle souligne qu'il est important que le Conseil de l'Europe apporte des réponses au problème croissant que posent, pour la sécurité des réseaux informatiques à l'échelle mondiale, le cyberterrorisme et d'autres formes d'attaques de grande ampleur commises contre les systèmes informatiques ou au moyen de ces derniers, lesquels constituent une grave menace pour la sécurité nationale, la sécurité publique ou le bien-être économique des Etats.

3. L'Assemblée recommande au Comité des Ministres:

3.1. d'inviter les Parties à la Convention sur la cybercriminalité (STE no 185) et à son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE no 189) à étudier s'il est faisable:

3.1.1. d'élaborer un protocole additionnel définissant un niveau commun d'incrimination des cyberattaques de grande ampleur, y compris pour ce qui est des circonstances aggravantes de ces attaques, ainsi que sur des normes minimales pour les peines applicables à ces attaques;

3.1.2. d'élaborer un autre protocole additionnel sur l'entraide en matière de pouvoirs d'investigation, qui étende en particulier le champ d'application de l'article 32 de la convention, conformément à la note d'orientation correspondante du Comité de la Convention sur la cybercriminalité qui représente les Parties à la convention;

3.2. d'inviter le Groupe sur les preuves dans le nuage établi par le Comité de la Convention sur la cybercriminalité à étudier la faisabilité d'un protocole additionnel à la Convention sur la cybercriminalité relatif à l'accès de la justice pénale aux données stockées sur des serveurs d'hébergement dans le nuage;

3.3. d'élaborer des normes juridiques sur la responsabilité internationale qui revient aux Etats de prendre toutes les mesures raisonnables pour prévenir que des cyberattaques de grande ampleur soient lancées par des personnes relevant de leur juridiction ou à partir de leur territoire national contre des systèmes informatiques dans un autre Etat;

3.4. de renforcer les actions d'assistance et de contrôle relatives à l'application de la Convention sur la cybercriminalité dans le droit et la pratique internes, ainsi que la coopération et les mesures pratiques contre les cyberattaques de grande ampleur, en particulier au bénéfice des Etats membres dans lesquels la mise en œuvre pratique de la Convention sur la cybercriminalité est confrontée à des difficultés;

3.5. d'appeler l'Autriche, la Bosnie-Herzégovine, la République tchèque, la Grèce, la Hongrie, l'Islande, l'Irlande, l'Italie, Malte, Monaco, le Portugal, Saint-Marin, la Suède et le Royaume-Uni à signer et/ou à ratifier sans délai le Protocole de 2003 portant amendement à la Convention

européenne pour la répression du terrorisme (STE no 190), ce qui est nécessaire pour que ce protocole entre en vigueur;

3.6. de transmettre à leurs autorités et ministères nationaux compétents cette recommandation et la Résolution 2070 (2015) «Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet».