www.coe.int/TCY

Strasbourg, 15 October 2015 T-CY (2015)19 E

Cybercrime Convention Committee (T-CY)

Opinion of the T-CY on Recommendation 2077 (2015) of the Parliamentary Assembly of the Council of Europe on Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet

Adopted by the T-CY on 13 October 2015 through written procedure

Opinion of the T-CY on
Recommendation 2077 (2015) of the Parliamentary Assembly of the Council of Europe on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet"[1]

1. The Deputies of the Ministers decided at their 1233rd session (8 July 2015) to communicate Recommendation 2077 (2015) of the Parliamentary Assembly on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet", inter alia, to the Cybercrime Convention Committee (T-CY) for comments by 22 October 2015.[2]

2. The T-CY welcomes the efforts of the Parliamentary Assembly to strengthen international cooperation against cybercrime and the important role that it attributes to the Convention on Cybercrime (ETS 185) in this respect.

3. The T-CY recalls that the Convention on Cybercrime is a criminal justice treaty which is applicable to cybercrime and electronic evidence of any criminal offence. "Large-scale attacks" against computer systems and the use of computer systems for terrorist purposes[3] are matters of public safety and thus fall within the scope of this treaty.

4. Regarding the specific recommendation 3.1.1 (study feasibility of an additional protocol to the Convention on Cybercrime (ETS 185) defining a common level of criminalisation of large-scale cyberattacks), the T-CY has the following comments:

- The T-CY adopted, in June 2013, Guidance Notes[4] on Distributed Denial of Service Attacks, on Critical Infrastructure Attacks, on Botnets and on New Forms of Malware. They provide guidance to Parties to the Convention on Cybercrime on the use of already existing provisions of the Convention to address "large-scale cyberattacks". The Guidance Notes call on Parties "to ensure, pursuant to Article 13, that criminal offences related to such attacks are punishable by effective, proportionate and dissuasive sanctions".
- The 3rd round of T-CY assessments was launched in July 2015 and covers Article 13 of the Convention on sanctions and measures. The questionnaire for the assessment of Article 13 explicitly asks whether aggravating circumstances are taken into account when criminalizing and sanctioning offences against and by means of computer systems. Results are expected to be available by mid-2016.
- Implementation of Article 13 ensures that "large-scale cyberattacks" are proportionately addressed.

5. Regarding the specific recommendation 3.1.2 (study feasibility of an additional protocol to the Convention on Cybercrime (ETS 185) extending the scope and application of Article 32), the T-CY has the following comments:

- Regarding the scope of Article 32, the T-CY adopted a Guidance Note in December 2014.[5]

---

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

[2] https://wcd.coe.int/ViewDoc.jsp?id=2184085&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

[3] The T-CY is unaware of an accepted definition of the term "cyberterrorism".

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

[5] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a

- The T-CY studied additional solutions to the problem of transborder access to data beyond Article 32 extensively since 2010, including through a specific working group ("Transborder Group") which completed its work in December 2014.
- The T-CY concluded in December 2014 "that an additional Protocol on transborder access to data would be needed", among other things given the cost of such crime to human rights and fundamental freedoms, including the right to private life, and the impact of crime on victims[6].
- At the same time, the T-CY came to the conclusion that such a Protocol would be controversial in the current context and that "a reasonable consensus to commence work on a Protocol was lacking".
- The T-CY, therefore, decided to "follow developments and reconsider the feasibility of a Protocol on the specific question of transborder access to data in the future".

6. Regarding the specific recommendation 3.2 (study feasibility of an additional protocol to the Convention on Cybercrime (ETS 185) regarding criminal justice access to data on cloud servers), the T-CY has the following comments:

- The T-CY in December 2014 established a new working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance ("Cloud Evidence Group").
- The Cloud Evidence Group is following up on the work of the Transborder Group as well as on the results of the assessment of the mutual legal assistance provisions of the Convention on Cybercrime adopted by the T-CY in December 2014.[7]
- The option of an additional Protocol to the Convention on Cybercrime is being studied by the Group. The Group is expected to complete its work by December 2016. A discussion paper on challenges encountered by criminal justice authorities[8] was published in May 2015.

7. Regarding the specific recommendation 3.4 (increase the assistance and monitoring activities regarding the implementation of the Convention on Cybercrime in domestic law and practice), the T-CY has the following comments:

- Assessment of the implementation of the Convention on Cybercrime is a core function of the T-CY. Two rounds of assessments have been completed since 2012 and a third one (on sanctions and measures) is underway. The provisions covered by these assessments are also related to "large-scale attacks". Additional resources are required to increase "the assistance and monitoring activities regarding the implementation of the Convention on Cybercrime in domestic law and practice", in particular considering the increasing number of Parties.
- Extensive capacity building activities are carried out in an efficient and cost-effective manner through the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania. These activities also strengthen capacities to respond to "large-scale attacks".

---

[6] "… the cost of such crime to human rights, including privacy, the impact of crime on victims and the positive obligation of governments to protect individuals against crime, including cybercrime, tends to be disregarded by many interlocutors. The lack of concern for the rights of victims has been a distressing revelation for the Transborder Group;"
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e

[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

[8] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

Appendix: PACE Recommendation 2077 (2015)

Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet

Author(s): Parliamentary Assembly

Origin - *Assembly debate* on 26 June 2015 (27th Sitting) (see Doc. 13802, report of the Committee on Culture, Science, Education and Media, rapporteur: Mr Hans Franken). *Text adopted by the Assembly* on 26 June 2015 (27th Sitting).

1. The Parliamentary Assembly refers to its Resolution 2070 (2015) on increasing co-operation against cyberterrorism and other large-scale attacks on the Internet.

2. It emphasises the importance for the Council of Europe to address the globally growing challenge to the security of computer networks posed by cyberterrorism and other forms of large-scale attacks on and through computer systems, which represent a serious threat to the national security, public safety or economic well-being of States.

3. The Assembly recommends that the Committee of Ministers:

3.1. invite the Parties to the Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) to study whether it is feasible to:

3.1.1. draft an additional protocol defining a common level of criminalisation of large-scale cyberattacks, including aggravating circumstances of those attacks as well as minimum standards for penalties for such attacks;

3.1.2. draft another additional protocol on mutual assistance regarding investigative powers, extending in particular the scope and application of Article 32 of the convention, in accordance with the respective guidance note of the Cybercrime Convention Committee which represents the parties to the convention;

3.2. invite the Cloud Evidence Group established by the Cybercrime Convention Committee to study the feasibility of drafting an additional protocol to the Convention on Cybercrime regarding criminal justice access to data on cloud servers;

3.3. draft legal standards on the international responsibility of States for taking all reasonable measures to prevent large-scale cyberattacks from being launched by persons under their jurisdiction or emanating from their national territory against computer systems in another State;

3.4. increase the assistance and monitoring activities regarding the implementation of the Convention on Cybercrime in domestic law and practice, as well as practical measures and co-operation against large-scale cyberattacks, in particular for the benefit of member States where the practical implementation of the Convention on Cybercrime faces difficulties;

3.5. call on Austria, Bosnia and Herzegovina, the Czech Republic, Greece, Hungary, Iceland, Ireland, Italy, Malta, Monaco, Portugal, San Marino, Sweden and the United Kingdom to sign and/or ratify without further delay the 2003 Protocol amending the European Convention on the Suppression of Terrorism (ETS No.190), which is necessary for its entry into force;

3.6. transmit to their competent national ministries and authorities this recommendation and Resolution 2070 (2015) on increasing co-operation against cyberterrorism and other large-scale attacks on the Internet.