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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 14055
04 May 2016

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

Reply to Recommendation[1]: Recommendation 2077 (2015)
Committee of Ministers

1. The Committee of Ministers has carefully examined Parliamentary Assembly Recommendation 2077 (2015) on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet." It has transmitted the recommendation to the Steering Committee on Media and Information Society (CDMSI), the Committee of Experts on Terrorism (CODEXTER) and the Cybercrime Convention Committee (T-CY), for information and possible comments.

2. The Committee of Ministers considers that large-scale attacks through computer systems represent a serious threat not only for national security, public safety, the economic well-being of societies and the integrity of the Internet's infrastructure, but also for the exercise and enjoyment of human rights on the Internet, in particular the right to freedom of expression, access to information and the right to privacy. The Committee welcomes the Assembly's efforts to strengthen international co-operation against cybercrime and the important role that it attributes to the Convention on Cybercrime (ETS No. 185) in this respect. It recalls that the Convention 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 are matters of public safety and thus fall within the scope of this treaty.

3. Regarding the Assembly's recommendation that a feasibility study be carried out for the elaboration of an additional protocol to the Convention on Cybercrime defining a common level of criminalisation of large scale cyberattacks (paragraph 3.1.1), the Committee of Ministers notes that in June 2013, the T-CY adopted Guidance Notes on Distributed Denial of Service Attacks, on Critical Infrastructure Attacks, on Botnets and on New Forms of Malware. These Notes provide guidance to the Parties to the Convention on Cybercrime on the use of already existing provisions 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. The questionnaire for the assessment of Article 13 explicitly asks whether aggravating circumstances are taken into account when criminalising and sanctioning offences against and by means of computer systems.

4. The Parliamentary Assembly also proposes a feasibility study for the drafting of an additional protocol on mutual assistance regarding investigative powers, extending the scope of Article 32 of the Convention (paragraph 3.1.2). In this respect, the Committee of Ministers refers to the Guidance Note on the scope of Article 32, adopted by the T-CY in December 2014, in which it concluded "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. At the same time, the T-CY noted, however, 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 will "follow

1. Adopted at the 1254th meeting of the Ministers Deputies (27 April 2016).

developments and reconsider the feasibility of a protocol on the specific question of transborder access to data in the future". The Committee of Ministers intends to follow this issue and will keep the Assembly informed about any developments in this respect.

5. Regarding a possible feasibility study for an additional protocol to the Convention on Cybercrime concerning criminal justice access to data on cloud servers (paragraph 3.2), the Committee of Ministers notes that the T-CY has established a working group on this subject. The option of an additional protocol to the Convention is being studied by the group, which is expected to complete its work by December 2016. The Committee of Ministers will keep the Assembly informed about any developments in this respect.

6. In respect of paragraph 3.3 of the Assembly's recommendation concerning legal standards on international responsibility for States for taking measures to prevent large-scale cyberattacks, the Committee of Ministers recalls its Recommendation CM/Rec(2011)8 to member States on the protection and promotion of the universality, integrity and openness of the Internet, which sets out core principles on international co-operation such as notification, information sharing, consultation and mutual assistance. It also recalls its Recommendation CM/Rec(2015)6 to member States on the free, transboundary flow of information on the Internet.

7. Finally, with respect to the proposal to increase assistance and monitoring activities (paragraph 3.4), the Committee of Ministers recalls that the 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 under way. The provisions covered by these assessments relate, *inter alia,* to "large-scale attacks". The Committee of Ministers also notes that extensive capacity building activities are carried out through the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania and that these activities contribute to strengthening capacities to respond to "large-scale attacks".