COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 26 October 2016 CODEXTER (2016) 20rev1

COMMITTEE OF EXPERTS ON TERRORISM

(CODEXTER)

Discussion Paper

Proposed Public-Private Platform to Address the Abuse of the Internet for Terrorist Purposes

Secretariat of the Counter-Terrorism Division

Information Society and Action against Crime Directorate, DG I

codexter@coe.int - www.coe.int/terrorism

In order to follow-up on issues raised by the Discussion Paper on Terrorism and the Internet [CODEXTER (2016) 2], the Secretariat was instructed to examine the feasibility of establishing a forum within the framework of the Council of Europe for interested Member State governments and representatives from major private internet companies and other stakeholders to discuss topics relating to the abuse of the internet for terrorist purposes. The proposed platform would be established under the Council of Europe's Internet Governance Strategy for 2016-2019 [CM (2016)10-final], which calls for such a platform to be established in order to enable states to ensure respect for human rights online in synergy with the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its additional protocol (CETS No. 217), as well as the Convention on Cybercrime (ETS No. 185).

While the primary responsibility for preventing and combating terrorism-related offences online is incumbent upon states, there is a need to pursue partnerships and co-operative mechanisms with and between government entities and private sector internet companies with a view to facilitating an open dialogue and address common goals to combat terrorism and violent extremism on the internet.

In order to promote a fair and effective balance between the ability of all citizens to exercise their human rights and fundamental freedoms on a safe, secure, open and enabling online environment, the fight against terrorism, radicalisation and recruitment means certain online activity is subject to narrow restrictions. The effective protection and promotion of democracy, human rights and the rule of law involves many cross-sector stakeholders, but law enforcement powers shall not be delegated to private companies. Action against terrorism, violent extremism and radicalisation requires concrete collective measures in tandem with checks and balances that ensure such actions do not result in censorship or otherwise unlawfully interfere with human rights and fundamental freedoms for regular internet users.

The Council of Europe's Internet Governance Strategy strongly recommends interaction, co-operation and dialogue between public and private stakeholders in order to address relevant aspects of internet infrastructure and functionality vulnerable to abuse by terrorists and violent extremists. Internet communication platforms, messaging services, online content hosts and social media platforms are widely used by terrorists and violent extremists to advocate hate speech, radicalisation, propaganda and recruitment of foreign terrorist fighters. Alongside Member States and relevant international organisations, the proposed platform could include representatives from major internet companies, including social media and e-mail providers, website hosting companies, and internet registrars.

The topics for discussion would be those most conducive to coordinated international and cross-sectoral cooperative efforts to tackle terrorism-related use of the internet. Topics could include issues such as: 1) guidelines and standards for user agreements and terms of service for internet services, 2) facilitate law enforcement cooperation on legal and/or technical aspects of filtering/removing terrorist content and taking down identified user accounts, 3) guidelines on internet companies' means and methods of identifying, tracking and/or filtering of online terrorist content, 4) furthering counter-narratives to terrorism through techniques such as context-based search engine indexing, AI tools and targeted ads, 5) appropriate principles of openness and transparency regarding private companies' compliance with relevant laws on the collection, storage and analysis of information, personal data or other electronic evidence pertaining to terrorism-related offences, 6) principles, recommendations and/or guidelines for transparency reports provided by internet companies concerning requests for cooperation from law enforcement entities, or 7) effective remedies to address illegitimate restrictions or infringements of human rights and fundamental freedoms online.

The CODEXTER is invited to consider the above proposal for issues to be discussed on a possible platform and to make suggestions in this regard.