OSCE

MC.DEC/7/06
5 December 2006

Organization for Security and Co-operation in Europe
Ministerial Council
Brussels 2006

Original: ENGLISH

Second day of the Fourteenth Meeting
MC(14) Journal No. 2, Agenda item 8

DECISION No. 7/06
COUNTERING THE USE OF THE INTERNET FOR TERRORIST PURPOSES

The Ministerial Council,

Recalling its previous decision on this issue (MC.DEC/3/04),

Remaining gravely concerned with the growing use of the Internet for terrorist purposes as outlined in the aforementioned decision and beyond,

Reaffirming in this context the importance of fully respecting the right to freedom of opinion and freedom of expression, which include the freedom to seek, receive and impart information, which are vital to democracy and in fact are strengthened by the Internet (PC.DEC/633 of 11 November 2004) and the rule of law,

Recognizing that United Nations Security Council resolution 1624 (2005) calls upon States to take measures that are necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law incitement to commit a terrorist act or acts and to prevent such conduct,

Reaffirming our commitments under the United Nations Global Counter-Terrorism Strategy, in particular "to coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet" and "to use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard",

Noting the observation in the report by the UN Counter-Terrorism Committee (S/2006/737 of 15 September 2006) that several States reported they are studying the application of the prohibition on incitement in their national legislation to the Internet,

Noting recent developments, in particular the Council of Europe Convention on the Prevention of Terrorism, regarding the obligations of States parties to this Convention to criminalize public provocation to commit a terrorist offence and recruitment and training for terrorism,

Recalling the Council of Europe's Convention on Cybercrime (2001), the only legally binding multilateral instrument that specifically addresses cybercrime by, *inter alia*,

providing for a common legal framework for international co-operation between States parties to this Convention in combating cybercrime, and its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems,

Recognizing the commitment by the G8 Summit (St. Petersburg, Russian Federation, 16 July 2006) to effectively counter attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists, and in particular noting the role of the G8 24/7 Computer Crime Network for countering criminal conduct in cyberspace,

Recalling the results of the OSCE Special Meeting on the Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes (Paris, 15 and 16 June 2004), as well as the outcomes of the OSCE Expert Workshop on Combating the Use of the Internet for Terrorist Purposes (Vienna, 13 and 14 October 2005) and the OSCE-Council of Europe Expert Workshop on Preventing Terrorism: Fighting Incitement and Related Terrorist Activities (Vienna, 19 and 20 October 2006), and relevant work done by the OSCE Secretariat and institutions, in particular by the Representative on Freedom of the Media and the ODIHR,

Taking into account different national approaches to defining “illegal” and “objectionable” content and different methods of dealing with illegal and objectionable content in cyberspace, such as the possible use of intelligence collected from Internet traffic and content to closing websites of terrorist organizations and their supporters,

Concerned with continued hacker attacks, which though not terrorism related, still demonstrate existing expertise in the field and thus providing a possibility of terrorist cyber attacks against computer systems, affecting the work of critical infrastructures, financial institutions or other vital networks,

1. Decides to intensify action by the OSCE and its participating States, notably by enhancing international co-operation on countering the use of the Internet for terrorist purposes;

2. Calls on participating States to consider taking all appropriate measures to protect vital critical information infrastructures and networks against the threat of cyber attacks;

3. Calls on participating States to consider becoming party to and to implement their obligations under the existing international and regional legal instruments, including the Council of Europe’s Conventions on Cybercrime (2001) and on the Prevention of Terrorism (2005);

4. Encourages participating States to join the G8 24/7 Computer Crime Network and to nominate an appropriate unit/contact person for this network for the purpose of streamlining international law enforcement co-operation on combating the criminal misuse of cyberspace and in criminal cases that involve electronic evidence, as appropriate;

5. Calls on participating States, when requested to deal with content that is illegal under their national legislation and is hosted within their jurisdiction, to take all appropriate action against such content and to co-operate with other interested States, in accordance with their

national legislation and the rule of law, and in line with their international obligations, including international human rights law;

6. Invites participating States to increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information in the OSCE and other relevant fora on the use of the Internet for terrorist purposes and measures taken to counter it, in line with national legislation, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression, and the rule of law. Duplication of efforts with ongoing activities in other international fora should be avoided;

7. Recommends participating States to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes;

8. Encourages participating States to participate in the May 2007 "OSCE political conference on public-private partnership in countering terrorism" in Vienna that will focus on the vital role the private sector, including businesses, civil society and the media, can play in co-operating with governments to prevent and combat terrorism;

9. Tasks the Secretary General to promote, notably through the OSCE Counter-Terrorism Network, the exchange of information on the threat posed by the use of the Internet for terrorist purposes, including incitement, recruitment, fund raising, training, targeting and planning terrorist acts, and on legislative and other measures taken to counter this threat.