**Organizzazione per la sicurezza e la cooperazione in Europa**
**Consiglio dei ministri**
**Bruxelles 2006**

MC.DEC/7/06
5 dicembre 2006

ITALIANO
Originale: INGLESE

**Secondo giorno della quattordicesima Riunione**
Giornale MC(14) N.2, punto 8 dell'ordine del giorno

# DECISIONE N.7/06
# LOTTA ALL'USO DI INTERNET PER SCOPI TERRORISTICI

Il Consiglio dei ministri,

richiamando la sua precedente decisione su tale materia (MC.DEC/3/04),

continuando a nutrire profonda preoccupazione per il crescente uso di Internet per scopi terroristici come espresso nella summenzionata decisione e in altre occasioni,

ribadendo in tale contesto l'importanza del pieno rispetto del diritto alla libertà di opinione e di espressione, che comprende la libertà di cercare, ricevere e divulgare informazioni, che sono vitali per la democrazia e che sono di fatto rafforzate da Internet (PC.DEC/633 dell'11 novembre 2004) e dallo stato di diritto,

riconoscendo che la risoluzione 1624 (2005) del Consiglio di sicurezza delle Nazioni Unite esorta gli Stati ad adottare misure necessarie ed appropriate e, in conformità ai loro obblighi di diritto internazionale, a vietare per legge l'istigazione a commettere atti di terrorismo e a prevenire tale condotta,

ribadendo il nostro impegno conformemente alla Strategia globale delle Nazioni Unite contro il terrorismo, in particolare "di coordinare gli sforzi a livello internazionale e regionale per contrastare il terrorismo in Internet in tutte le sue forme e manifestazioni " e "di usare Internet come strumento per contrastare la diffusione del terrorismo, riconoscendo nel contempo agli Stati la possibilità di richiedere assistenza a tale riguardo",

prendendo nota del rapporto del Comitato antiterrorismo delle Nazioni Unite (S/2006/737 del 15 settembre 2006) in cui si rileva che numerosi Stati stanno esaminando l'applicazione a Internet del divieto di istigazione previsto dalla loro legislazione nazionale,

rilevando i recenti sviluppi, in particolare la Convenzione del Consiglio d'Europa sulla prevenzione del terrorismo, riguardanti gli obblighi degli Stati Parte di tale convenzione di considerare come reato l'istigazione pubblica a commettere un atto terroristico, nonché il reclutamento e l'addestramento a scopi terroristici,

richiamando la Convenzione del Consiglio d'Europa sulla cibercriminalità (2001), l'unico strumento multilaterale giuridicamente vincolante che affronta specificatamente la

cibercriminalità, fornendo tra l'altro un quadro giuridico comune per la cooperazione internazionale fra gli Stati Parte della Convenzione nella lotta alla cibercriminalità, nonché il suo Protocollo aggiuntivo relativo all'incriminazione di atti di natura razzista e xenofoba commessi tramite mezzi informatici,

riconoscendo l'impegno espresso al Vertice del G8 (San Pietroburgo, Federazione Russa, 16 luglio 2006) di contrastare efficacemente i tentativi di sfruttare il ciberspazio a scopi terroristici, inclusa l'istigazione a commettere atti di terrorismo, a comunicare e pianificare atti di terrorismo, ivi compreso il reclutamento e l'addestramento di terroristi, e rilevando in particolare il ruolo del "24/7 Computer Crime Network" del G8 per contrastare gli atti criminali nel ciberspazio,

richiamando i risultati della Riunione speciale dell'OSCE sul rapporto tra propaganda razzista, xenofoba e antisemita in Internet e i crimini ispirati dall'odio (Parigi, 15 e 16 giugno 2004), nonché gli esiti del Seminario OSCE di esperti sulla lotta all'uso di Internet a scopi terroristici (Vienna, 13 e 14 ottobre 2005) e del Seminario di esperti OSCE-Consiglio d'Europa sulla prevenzione del terrorismo: lotta all'incitamento al terrorismo ed alle attività correlate (Vienna, 19 e 20 ottobre 2006), nonché dell'importante attività svolta dal Segretariato e dalle istituzioni dell'OSCE, in particolare dal Rappresentante per la libertà dei mezzi di informazione e dall'ODIHR,

tenendo conto dei differenti approcci nazionali per definire "illegale" e "deplorevole" un contenuto, nonché dei differenti metodi di trattare un contenuto illegale e deplorevole nel ciberspazio, come ad esempio l'eventuale uso di informazioni riservate raccolte dal traffico e dai contenuti Internet al fine di chiudere siti web di organizzazioni terroristiche e di loro sostenitori,

preoccupato dai continui attacchi di pirateria informatica che, benché non connessi al terrorismo, dimostrano l'esistenza di una competenza in tale campo, creando in tal modo la possibilità di lanciare attacchi terroristici cibernetici contro sistemi informatici, che colpiscono l'attività di importanti infrastrutture, istituzioni finanziarie e altre reti vitali,

1. decide di intensificare l'azione dell'OSCE e dei suoi Stati partecipanti potenziando in particolare la cooperazione internazionale nella lotta all'uso di Internet per scopi terroristici;

2. invita gli Stati partecipanti a considerare la possibilità di adottare tutte le misure necessarie a proteggere importanti infrastrutture e reti informatiche vitali dalla minaccia di attacchi di pirateria informatica;

3. invita gli Stati partecipanti a considerare la possibilità di aderire a strumenti giuridici internazionali e regionali esistenti e di attuarne gli obblighi, incluse le Convenzioni del Consiglio d'Europa sulla cibercriminalità (2001) e sulla prevenzione del terrorismo (2005);

4. incoraggia gli Stati partecipanti a aderire al "24/7 Computer Crime Network" del G8 e a nominare un'unità/persona di contatto appropriata per tale rete al fine di accelerare la cooperazione internazionale delle forze di polizia in materia di lotta allo sfruttamento a fini criminali del ciberspazio e in casi di reati dimostrabili con prove elettroniche, a seconda del caso;

5. invita gli Stati partecipanti, qualora sia loro richiesto di intervenire in caso di contenuti considerati illegali ai sensi della loro legislazione nazionale e ospitati da siti che rientrano nella loro giurisdizione, ad adottare tutte le misure appropriate contro tali contenuti e a cooperare con altri Stati interessati, conformemente alla loro legislazione nazionale e allo stato di diritto, nonché ai loro obblighi internazionali, incluso il diritto umanitario internazionale;

6. invita gli Stati partecipanti a intensificare il monitoraggio dei siti web di terroristi e/o di organizzazioni estremiste violente e di loro sostenitori e a potenziare lo scambio di informazioni in seno all'OSCE e ad altri fori pertinenti sull'uso di Internet a scopi terroristici e sulle misure adottate per contrastarlo, in conformità alla legislazione nazionale, assicurando nel contempo il rispetto degli obblighi e degli standard di diritto umanitario internazionale, inclusi quelli concernenti i diritti alla riservatezza e alla libertà di opinione e di espressione, nonché dello stato di diritto. Si dovranno evitare duplicazioni di sforzi con attività in corso in altri fori internazionali;

7. raccomanda agli Stati partecipanti di esplorare la possibilità di un più attivo coinvolgimento delle istituzioni della società civile e del settore privato nella prevenzione e nella lotta all'uso di Internet per scopi terroristici;

8. incoraggia gli Stati partecipanti a partecipare alla "Conferenza politica dell'OSCE sul partenariato pubblico-privato nella lotta al terrorismo" che si terrà a Vienna nel maggio 2007 e che sarà incentrato sul ruolo vitale che il settore privato, incluse le imprese, la società civile e i mezzi di informazione, può svolgere nella cooperazione con i governi al fine di prevenire e combattere il terrorismo;

9. incarica il Segretario generale di promuovere, in particolare tramite la Rete antiterrorismo dell'OSCE, lo scambio di informazioni sulla minaccia posta dall'uso di Internet per scopi terroristici, inclusi l'istigazione, il reclutamento, lo stanziamento di fondi, l'addestramento, la scelta degli obiettivi e la pianificazione di atti terroristici, nonché su misure legislative e di altro genere adottate per contrastare tale minaccia.