Doc. **XII-*quinquies***
N. **4**

CAMERA DEI DEPUTATI

ASSEMBLEA PARLAMENTARE DELL'OSCE

Sessione Annuale di Astana, Kazakistan
(29 giugno – 3 luglio 2008)

Risoluzione sulla cibersicurezza e la cibercriminalità

Trasmessa il 24 luglio 2008

1. *Ricordando* che nel mondo contemporaneo i conflitti armati non sono l'unico terreno fertile per le minacce contro gli Stati e i cittadini,

2. *Riconoscendo* il ruolo essenziale della cooperazione tra tutti i governi per affrontare in modo efficace i rischi per la sicurezza attuali,

3. *Sottolineando* il fatto che i ciberattacchi sono diventati una seria minaccia per la sicurezza, che non può essere sottovalutata,

4. *Riconoscendo* che i ciberattacchi possono essere una grande sfida per i governi, perché possono destabilizzare la società, mettere in pericolo la disponibilità di servizi pubblici e il funzionamento di infrastrutture statali vitali,

5. *Reiterando* che ogni paese che si affidi in ampia misura alle tecnologie di informazione e comunicazione può esser vittima della cibercriminalità,

6. *Accogliendo favorevolmente* le discussioni nelle sedi internazionali riguardo a come reagire efficacemente all'abuso del ciberspazio a fini criminali, in particolare a fini terroristici,

7. *Riconoscendo* che la cibersicurezza e la cibercriminalità sono diventate una questione di notevole preoccupazione per, *inter alia*, il Consiglio d'Europa, l'UE, la NATO e l'Assemblea Generale dell'ONU,

8. *Riaffermando* il ruolo dell'OSCE quale accordo regionale ai sensi del Capitolo VIII della Carta dell'ONU e quale strumento principale di preallarme, prevenzione dei conflitti, gestione delle crisi e riabilitazione post-conflittuale nella sua area,

9. *Ribadendo* la propria preoccupazione per la persistenza dei ciberattacchi in vari luoghi dell'area OSCE,

10. *Riconoscendo* la precedente attività svolta nell'ambito dell'OSCE per quanto

attiene ai vari aspetti della cibersicurezza e della cibercriminalità, legati in particolare all'uso di Internet da parte di terroristi,

11. *Sottolineando* l'urgente necessità che la comunità internazionale aumenti la cooperazione e lo scambio di informazioni nel campo della cibersicurezza e della cibercriminalità, perché solo con iniziative coordinate e congiunte è possibile rispondere efficacemente alle minacce che provengono dal ciberspazio,

12. *Sottolineando* che la Convenzione sulla Cibercriminalità del 2001 del Consiglio d'Europa è l'unico documento formale multilaterale giuridicamente vincolante che affronta in modo specifico la criminalità informatica, ma che è stata ratificata solo da 22 Stati,

13. *Accogliendo favorevolmente* le discussioni e le decisioni avviate dalla NATO, dall'Assemblea Parlamentare del Consiglio d'Europa e in altre sedi,

14. *Accogliendo favorevolmente* il fatto che numerosi Stati partecipanti dell' OSCE hanno già definito e adottato contromisure per contrastare vari tipi di minacce informatiche,

15. *Sottolineando* l'impegno degli Stati partecipanti dell'OSCE a rispettare e promuovere i principi di diritto internazionale,

L'Assemblea Parlamentare dell'OSCE:

16. *Esprime* il proprio rammarico per il fatto che la comunità internazionale non sia stata in grado sinora di concordare contromisure specifiche per contrastare le minacce informatiche;

17. *Invita* i parlamentari degli Stati partecipanti dell'OSCE a intensificare le loro iniziative nel convincere i parlamenti e i governi dei loro paesi che le minacce che provengono dal ciberspazio sono una delle sfide di sicurezza più preoccupanti di questi tempi, che può mettere in pericolo il modo di vivere delle società moderne e l'intera civiltà;

18. *Invita* i governi a condannare moralmente i ciberattacchi in quanto analoghi alla tratta di esseri umani o alla pirateria della proprietà intellettuale, e a creare regole di condotta universale nel ciberspazio;

19. *Sostiene* che i risultati di un ciberattacco ai danni di infrastrutture statali di vitale importanza non sono di natura diversa da quelli di un atto d'aggressione convenzionale;

20. *Invita* gli Stati partecipanti dell'OSCE e tutti gli altri membri della comunità internazionale a considerare la possibilità di aderire alla Convenzione sulla Cibercriminalità del Consiglio d'Europa e di seguirne le disposizioni incondizionatamente;

21. *Invita* gli Stati partecipanti dell'OSCE a considerare anche la possibilità di aderire alla Convenzione sulla prevenzione del terrorismo del Consiglio d'Europa che offre ulteriori strumenti per prevenire i ciberattacchi perpetrati da gruppi terroristici e impedire l'uso di Internet a scopi terroristici;

22. *Richiama l'attenzione* sulla necessità di emendare le leggi vigenti in materia di cibersicurezza e cibercriminalità e di trovare mezzi supplementari, inclusa l'armonizzazione delle legislazioni degli Stati in materia, e di rendere più efficiente la cooperazione internazionale nel campo della cibersicurezza e della cibercriminalità;

23. *Invita* tutte le parti interessate a ricercare, in buona fede, soluzioni negoziate nel campo della cibersicurezza e della cibercriminalità al fine di conseguire un compromesso globale e duraturo che deve essere basato sulle norme e i principi del diritto internazionale;

24. *Invita* tutte le parti ad utilizzare appieno i meccanismi e i formati disponibili per il dialogo in uno spirito costruttivo;

25. *Sostiene* tutte le iniziative volte a valorizzare lo scambio di informazioni

sulle esperienze e le prassi migliori in questo campo, coinvolgendo anche i soggetti interessati del settore privato e della società civile al fine di creare partnership pubblico-private in questo ambito;

26. *Incoraggia* gli Stati partecipanti dell'OSCE a definire, adottare ed attuare piani nazionali d'azione per la cibersicurezza e la cibercriminalità;

27. *Raccomanda* all'OSCE di fungere da meccanismo regionale che sostiene, coordina e verifica la definizione e l'attuazione delle attività nazionali in questo campo, prendendo spunto dalle attività precedenti relative ai vari aspetti della cibersicurezza e della cibercriminalità e portandole avanti;

28. *Sollecita* gli Stati partecipanti dell'OSCE ad adottare misure di prevenzione per impedire incidenti di sicurezza, per aumentare la consapevolezza rispetto alla sicurezza degli utenti delle tecnologie di informazione e comunicazione;

29. *Sottolinea* la necessità di analizzare l'adeguatezza delle misure esistenti e di integrarle in base all'esperienza acquisita;

30. *Accoglie favorevolmente* la proposta di tenere una conferenza o una tavola rotonda per i parlamentari dell'OSCE, considerando i precedenti eventi OSCE relativi ai vari aspetti della cibersicurezza e della cibercriminalità e prendendone spunto, per ottenere, con l'aiuto di esperti, informazioni dettagliate su tutti gli aspetti rilevanti della questione;

31. *Chiede* ai rappresentanti degli Stati partecipanti dell'OSCE di inoltrare questa risoluzione ai governi e ai parlamenti dei loro paesi.