SENATO DELLA REPUBBLICA
XVII LEGISLATURA

Doc. XII-*quinquies*
n. 10

ASSEMBLEA PARLAMENTARE DELL'OSCE

Sessione annuale di ISTANBUL, Turchia

(29 giugno - 3 luglio 2013)

Risoluzione sulla sicurezza informatica

Trasmessa alla Presidenza il 10 luglio 2013

RISOLUZIONE SULLA

SICUREZZA INFORMATICA

1. Ricordando che nel mondo contemporaneo le società moderne dell'informazione dipendono notevolmente dallo spazio informatico – un ambiente elettronico che comprende prodotti, servizi e informazioni,

2. Riconoscendo il fatto che gli attacchi informatici, in qualsiasi forma, sono diventati una minaccia grave per la sicurezza che non può essere ignorata o sottovalutata,

3. Sottolineando che l'insicurezza nel nostro spazio informatico comune impedisce l'ulteriore sviluppo economico, l'innovazione e la prosperità sociale,

4. Riconoscendo che gli attacchi informatici possono essere una sfida per tutta la società, ivi compresi i governi, le società private, le organizzazioni non governative e gli utenti privati di Internet, perché possono destabilizzare la società, compromettere la disponibilità dei servizi pubblici e il funzionamento delle infrastrutture vitali di uno Stato,

5. Ribadendo che tutti i paesi che fanno ampio ricorso allo spazio informatico possono subire gli effetti di attacchi informatici nello stesso modo in cui subiscono le conseguenze di attacchi convenzionali,

6. Sottolineando che far fronte alle nuove esigenze create del mutato ambiente di sicurezza non è solo una sfida per i paesi direttamente interessati dalla nuova situazione, ma è una sfida per ogni singolo paese del mondo,

7. Riconoscendo che il continuo processo di globalizzazione e interoperabilità dei sistemi di informazione renderà lo spazio informatico ancora più vulnerabile e che le nuove tecniche e strategie di sicurezza potrebbero non essere in grado di rispondere in modo adeguato a tale maggiore vulnerabilità,

8. Costatando che Internet è sempre stato alimentato da politiche che promuovono il libero flusso delle informazioni e che proteggono i diritti umani e incoraggiano l'innovazione, la creatività e la crescita economica,

9. Convinta che l' OSCE possa svolgere un ruolo utile offrendo una piattaforma ai decisori, agli esperti del settore e agli altri soggetti interessati ampliando il dibattito sulla sicurezza informatica,

10. Riconoscendo che per far fronte alle minacce informatiche sarebbe necessario aumentare significativamente le risorse migliorando la consapevolezza, la formazione e gli investimenti in tecnologia, oltre che migliorando gli approcci concettuali e dottrinali,

11. Guardando con favore ai dibattiti in seno ai forum internazionali che vertono su come rispondere efficacemente all'uso improprio dello spazio informatico per attività di spionaggio e a fini criminali, terroristici e militari e ai dibattiti e alle decisioni avviate dalla NATO, dall'Assemblea Parlamentare del Consiglio d'Europa e in altre sedi,

12. Riconoscendo che la sicurezza informatica è diventata, tra l'altro, una questione di notevole interesse per il Consiglio d'Europa, la UE, la NATO e l'Assemblea Generale dell'ONU,

13. Riaffermando il ruolo dell'OSCE quale accordo regionale ai sensi del Capitolo VIII della Carta delle Nazioni Unite e strumento essenziale di preallarme, prevenzione dei conflitti, gestione delle crisi e riassetto postconflittuale nella sua regione,

14. Ribadendo la sua preoccupazione per la persistenza degli attacchi informatici in diversi luoghi dell'area dell'OSCE,

15. Riconoscendo le precedenti attività svolte nell'OSCE riguardo a vari aspetti della sicurezza informatica, in particolare il Gruppo di lavoro informale dell'OSCE istituito dalla decisione N. 1039 della Commissione permanente, incaricata di elaborare una serie di misure di rafforzamento della fiducia (CBM) per migliorare la collaborazione tra gli Stati, la trasparenza, la capacità di prevedere e la stabilità e per ridurre i rischi di un errore di valutazione, di un'intensificazione e di un conflitto che potrebbero derivare dall'uso delle tecnologie dell'informazione e della telecomunicazione (TIC),

16. Sottolineando l'urgente necessità che la comunità internazionale aumenti la cooperazione e lo scambio di informazioni nel campo della sicurezza informatica, perché solo iniziative congiunte e concertate consentiranno di reagire efficacemente alle minacce che provengono dallo spazio informatico,

17. Sottolineando che la Convenzione del Consiglio d'Europa sulla criminalità informatica è l'unico strumento multilaterale giuridicamente vincolante che affronta specificamente la criminalità informatica, ma che solo trentanove Stati l'hanno ratificata o vi hanno aderito,

18. Guardando con favore al fatto che numerosi Stati partecipanti dell'OSCE hanno elaborato e adottato misure per contrastare vari tipi di minacce informatiche, e osservando tuttavia che le misure di contrasto sono state prevalentemente di natura interna e non possono essere efficaci nell'ambiente di una rete che si estende al mondo intero,

19. Sottolineando l'impegno degli Stati partecipanti dell'OSCE a rispettare e a promuovere i principi del diritto internazionale,

L'Assemblea Parlamentare dell'OSCE:

20. Raccomanda che l'OSCE possa funzionare come meccanismo regionale che sostiene, coordina e verifica l'elaborazione e l'attuazione di attività nazionali in questo campo, prendendo spunto dalle precedenti attività concernenti vari aspetti della sicurezza informatica e promuovendole;

21. Deplora che la comunità internazionale non sia stata in grado sinora di concordare misure specifiche di contrasto alle minacce informatiche,

22. Sostiene che i risultati di un attacco informatico contro le infrastrutture vitali dello Stato non siano di natura diversa da quelli di un atto di aggressione convenzionale;

23. Osserva che lo spazio informatico è stato un ambiente per promuovere il libero flusso delle informazioni, per incoraggiare l'innovazione e la crescita economica e dovrebbe rimanere tale;

24. Invita gli Stati partecipanti dell'OSCE a promuovere e facilitare l'accesso a Internet e la cooperazione internazionale che mira allo sviluppo dei mezzi di informazione e delle strutture dell'informazione e della comunicazione in tutti i paesi;

25. Esorta i parlamentari degli Stati partecipanti dell'OSCE a intensificare le iniziative per convincere i parlamenti e i governi dei loro paesi del fatto che le minacce che provengono dallo spazio informatico costituiscono una delle sfide più gravi cui la sicurezza è ora esposta, che può compromettere il modo in cui vivono le società moderne e la civiltà nel suo complesso;

26. Esorta i governi a svolgere un ruolo di guida nel difendere uno spazio informatico libero e sicuro, a condannare senza mezzi termini gli attacchi informatici e a ricercare soluzioni comuni efficaci per proteggere lo spazio informatico da usi impropri e attività dolose;

27. Prende atto delle iniziative intraprese dall'OSCE per aumentare la trasparenza e la stabilità e per ridurre i rischi derivanti dallo spazio informatico;

28. Esorta gli Stati partecipanti dell'OSCE a utilizzare il suo approccio globale e interdimensionale alla sicurezza e a proseguire le iniziative per la definizione di misure di rafforzamento della fiducia nell'ambito della sicurezza informatica;

29. Sottolinea la necessità di affrontare le minacce informatiche senza compromettere i diritti e le libertà fondamentali, e che gli stessi diritti di cui le persone godono quando non sono collegate telematicamente (*offline*) devono essere tutelati anche quando sono collegate (*online)*, in particolare la libertà di espressione;

30. Esorta gli Stati partecipanti dell'OSCE e tutti gli altri membri della comunità internazionale a considerare l'adesione alla convenzione del Consiglio d'Europa sulla criminalità informatica e a seguirne le disposizioni;

31. Esorta gli Stati partecipanti dell'OSCE a considerare l'adesione anche alla Convenzione del Consiglio d'Europa sulla prevenzione del terrorismo, che offre ulteriori strumenti per prevenire attacchi informatici da parte di gruppi terroristici e l'uso di Internet a scopi terroristici;

32. Richiama l'attenzione sulla necessità di studiare le leggi in vigore che disciplinano la sicurezza informatica e di trovare mezzi supplementari, quali l'armonizzazione delle leggi in materia degli Stati, per rendere più efficiente la cooperazione internazionale nel campo della sicurezza informatica;

33. Esorta tutte le parti interessate a ricercare, in buona fede, soluzioni negoziate nel campo della sicurezza informatica al fine di giungere a un accordo globale e duraturo che sia basato sulle norme e sui principi del diritto internazionale;

34. Invita tutte le parti ad avvalersi appieno, con spirito costruttivo, dei meccanismi e dei formati di dialogo disponibili;

35. Sostiene tutte le iniziative finalizzate a migliorare lo scambio di informazioni sulle esperienze e le buone prassi in materia, anche coinvolgendo gli attori competenti del settore privato e della società civile, e a creare partenariati tra il settore pubblico e il settore privato in quest' ambito;

36. Incoraggia gli Stati partecipanti dell'OSCE a definire, adottare e attuare piani d'azione nazionali sulla sicurezza informatica;

37. Esorta gli Stati partecipanti dell'OSCE ad adottare misure di natura previsionale per prevenire incidenti alla sicurezza e a sensibilizzare maggiormente rispetto alla sicurezza gli utenti delle tecnologie di informazione e comunicazione;

38. Accoglie favorevolmente la proposta di organizzare una conferenza o una tavola rotonda per i parlamentari dell'OSCE, che tenga presente gli eventi dell'OSCE svoltisi in precedenza sui vari aspetti della sicurezza informatica e ne prenda spunto, e di acquisire, attraverso l'aiuto di esperti, informazioni dettagliate su tutti gli aspetti pertinenti della questione;

39. Chiede ai rappresentanti degli Stati partecipanti dell'OSCE di far pervenire questa Risoluzione ai governi e ai parlamenti dei loro paesi.