FASCICOLO FINALE

23 maggio 2012

SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Mozioni sulla sicurezza da minaccia cibernetica

(1-00405) (23 maggio 2012)
Approvata

RAMPONI, GASPARRI, FINOCCHIARO, BRICOLO, PISTORIO, D'ALIA, VIESPOLI, GRAMAZIO, DE ECCHER, DI STEFANO, RUTELLI (*). – Il Senato,

considerato che:

le tecnologie dell'informazione e della telecomunicazione costituiscono sempre di più una parte fondamentale per la vita della società;

la struttura aperta del sistema *Internet* è vulnerabile ad attacchi che possono avere origine: criminale (*cyber crime*), terroristica (*cyber terrorism*), per attività di spionaggio (*cyber espionage*) o, addirittura, dar vita ad una *cyber war*, cioè un vero e proprio conflitto tra nazioni combattuto attraverso la paralisi di tutti i gangli vitali per la vita delle società dei reciproci contendenti;

il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, all'articolo 7-*bis* , rubricato "Sicurezza telematica", dispone che "Ferme restando le competenze dei Servizi informativi e di sicurezza (...) l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Servizio Polizia Postale e delle Comunicazioni) assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno";

con decreto del Ministro dell'interno 9 gennaio 2008 sono state individuate le infrastrutture critiche informatizzate di interesse nazionale;

in ossequio allo stesso decreto, è stato istituito con decreto del Capo della Polizia, direttore generale della pubblica sicurezza, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC);

il nuovo concetto strategico della Nato e la dichiarazione finale del vertice di Lisbona hanno individuato come nuovo obiettivo la tutela della sicurezza del *cyber space*;

i principali governi europei, e in particolare, in ordine di tempo, il Regno Unito, la Francia, la Germania e l'Olanda, si sono dotati di una dottrina *cyber* sicurezza nazionale, grazie alla quale si individuano le priorità di intervento e si attribuiscono ruoli e responsabilità con l'obiettivo di

ridurre la frammentazione di competenze e di stimolare una più profonda collaborazione sul piano multilaterale;

nel convincimento che i *cyber attack*, oltre ad essere cresciuti in frequenza, siano divenuti oltremodo pericolosi per il mantenimento della prosperità dei singoli Paesi, l'Alleanza Atlantica ha avvertito la necessità di introdurre la dimensione informatica dei moderni conflitti nella propria dottrina strategica, nonché l'urgenza di potenziare la propria capacità nella prevenzione da un attacco, reagire ad esso, migliorando la resilienza e limitando i danni;

il decreto del Presidente del Consiglio dei ministri del 5 maggio 2010 ha dato vita al Nucleo interministeriale situazione pianificazione (NISP) quale organo di studio e supporto alle attività del Comitato politico strategico (COPS) in materia di organizzazione nazionale per la gestione della crisi;

le istituzioni nazionali hanno preso atto dei vari tipi di minaccia cibernetica ed hanno avviato iniziative di contrasto;

il quadro di difesa contro tali attacchi presenta in Italia una situazione diffusa di sistemi di protezione in via avanzata di completamento, nell'ambito dei diversi assetti pubblici e privati;

nelle conclusioni e raccomandazioni della relazione del COPASIR sulle possibili implicazioni e minacce per la sicurezza nazionale, derivanti dallo spazio cibernetico, si auspica un adeguato coordinamento di tutti i soggetti interessati alla messa a punto di un sistema di protezione di tutti gli assetti sensibili, riguardanti la vita economica, sociale e politica dello Stato,

impegna il Governo:

a porre in essere ogni idonea iniziativa per giungere alla costituzione presso la Presidenza del Consiglio dei ministri in tempi congrui, tenuto conto della specificità e tecnicità delle materia e della complessità e delicatezza delle valutazioni che essa comporta, di un Comitato interministeriale per l'indirizzo e il coordinamento strategico in materia di sicurezza dello spazio cibernetico, cui affidare l'adozione di una strategia nazionale per la sicurezza dello spazio cibernetico e l'approvazione degli indirizzi generali e delle direttive vincolanti da perseguire nel quadro della politica, nazionale ed internazionale, della sicurezza dello spazio cibernetico nonché l'individuazione degli interventi normativi conseguentemente necessari;

a individuare, tra le strutture già costituite presso la Presidenza del Consiglio dei ministri, quella cui attribuire le funzioni di Segreteria e di supporto al costituendo Comitato per lo svolgimento delle funzioni attribuitegli;

a mettere in atto appositi sistemi di difesa preventiva dalla minaccia, con strumenti, procedure e prescrizioni propri e/o multinazionali anche in aderenza con gli impegni assunti in ambito NATO e Unione euro-

pea, affidando ai Ministeri competenti, nel rispetto delle specifiche competenze, la protezione delle strutture e delle reti di comunicazione, in armonia con le direttive impartite dal Comitato interministeriale e tenendolo costantemente e preventivamente informato.

(*) Firma aggiunta in corso di seduta.

(1-00491) (23 maggio 2012)

Approvata

CASSON, CAROFIGLIO, CHIURAZZI, D'AMBROSIO, DELLA MONICA, GALPERTI, GARRAFFA, MARITATI, ADAMO, CECCANTI, INCOSTANTE, SANNA, SERRA, RUTELLI (*). – Il Senato,

premesso che:

uno dei presupposti essenziali della sicurezza delle reti è costituito dalla possibilità di identificare univocamente l'autore di condotte illecite;

in ragione dell'anonimato che caratterizza le comunicazioni in rete, tale possibilità dipende (quasi) esclusivamente dall'assegnazione a ciascun utente o abbonato al servizio di fornitura del collegamento Internet di un indirizzo di protocollo Internet (IP), ovvero – come lo definisce l'articolo 1, comma 1, lettera g), del decreto legislativo n. 109 del 2008, recante "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE"- di un indirizzo di protocollo che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica;

si tratta, in altri termini, di una sorta di targa che consente di identificare l'autore di ciascuna condotta tenuta in rete, oggi fondata sul sistema "IPv4" che, articolandosi sulla combinazione di 32 byte, può assegnare al massimo 232 indirizzi distinti;

considerato che:

tale numero massimo di indirizzi IP è prossimo all'esaurimento, in ragione dell'avvenuta assegnazione di quasi tutte le combinazioni disponibili e dell'assenza di investimenti finalizzati all'aggiornamento delle infrastrutture tecnologiche degli operatori di rete, che avrebbero potuto agevolare il passaggio al protocollo IPv6; sistema idoneo a garantire la disponibilità di nuovi indirizzi;

è evidente che la saturazione degli indirizzi IP disponibili renderà oltremodo difficili – se non impossibili – le indagini volte all'accertamento non solo di fenomeni quali *cyber-crime, cyber-espionage* e *cyber-terrorism*, ma più in generale di qualsiasi tipo di illecito per la cui realizzazione l'autore abbia fatto ricorso alla rete,

impegna il Governo:

ad adottare, con la massima urgenza – in ragione della gravità dei rischi conseguenti all'esaurimento degli indirizzi IPv4 – misure idonee a

consentire la disponibilità di nuovi indirizzi IP univoci, con il passaggio al V6 o con l'introduzione di dispositivi tecnici che consentano altrimenti l'identificazione dell'utente.

(*) Firma aggiunta in corso di seduta.