

Continuano gli eventi Nato in Italia per la sensibilizzazione sui rischi cyber e sulle nuove forme di terrorismo

Date : 16 giugno 2017



Si è svolto ieri, 15 giugno, alla Camera presso la Nuova aula dei Gruppi parlamentari, la conferenza “Il pericolo corre in rete. La nuova frontiera della minaccia cibernetica”, evento promosso dalla Delegazione italiana presso l'Assemblea parlamentare della Nato, in collaborazione con il Centro studi americani. Alla conferenza hanno partecipato circa 500 persone rappresentative del mondo cyber italiano.

L'evento rientra nell'ambito di un ciclo di incontri inaugurato dalla Delegazione Nato già nel 2015 per stimolare il dibattito italiano sui temi della sicurezza cibernetica. La discussione si è articolata in tre parti ed ha visto la partecipazione, tra gli altri di **Alessandro Armando**, professore del Dipartimento di Informatica, bioingegneria, robotica e ingegneria dei sistemi (Dibris) dell'Università di Genova; **Arije Antinori**, del Cri.Me.Lab della Sapienza e **Kieran L. Ramsey**, Attaché legale dell'Fbi dell'Ambasciata americana a Roma.

Tra i presenti anche l'onorevole **Andrea Manciuoli**, Presidente della Delegazione italiana alla Nato, che nel suo intervento ha spiegato: “La nuova frontiera della minaccia cibernetica rappresenta una priorità per la sicurezza internazionale, come numerosi fatti recenti hanno dimostrato, dall'attacco in Estonia di dieci anni fa al caso “wannacry” del mese scorso. La capacità di provocare danni, anche molto significativi, da parte di soggetti diversi e anche di piccole dimensioni, alle nostre infrastrutture, al sistema economico, alle nostre istituzioni, fino ad interferire i processi elettorali, è ormai evidente e deve spingere tutti i paesi dell'Alleanza ad aggiornare sempre di più gli strumenti di contrasto e prevenzione nella dimensione cibernetica. Non è un caso che quello cibernetico sia stato riconosciuto dalla Nato come il nuovo dominio operativo”.

Il ministro della Difesa, **Roberta Pinotti**, nel suo intervento a chiusura dei lavori, si è invece soffermata sul bisogno di conoscere il mondo virtuale che costituisce il “sistema nervoso della società mondiale del ventunesimo secolo”. “Il cosiddetto virtuale - ha aggiunto - è diventato più reale del reale, sempre più centrale per la nostra quotidianità. La vastità e pervasività delle tecnologie informatiche ci danno la misura del problema: dai rischi più direttamente percepiti dagli individui, come la tutela della privacy, alle minacce di eventi persino catastrofici, come il sabotaggio informatico delle infrastrutture critiche, passando per la dimensione immateriale

della conoscenza e della percezione degli eventi". Per tale motivo, ha poi chiosato "se nella rete sembra esserci sempre meno spazio di manovra per i tradizionali stati nazionali, proprio lo Stato è un attore fondamentale per la sicurezza cibernetica e sarà sempre più cruciale la definizione dei rapporti tra Stati e soggetti non statuali".

Le difficoltà per la Difesa che nell'ambito della sicurezza cibernetica si trova ad operare in un nuovo teatro di operazioni non esclusivamente ad appannaggio delle componenti militari, ma in cui trovano spazio anche organizzazioni ed individui non necessariamente riconducibili ad entità statuali è invece stato il tema dell'intervento del capo di Stato maggiore della Difesa, generale **Claudio Graziano**.

"La minaccia cibernetica – ha spiegato il generale Graziano - sta assumendo un crescente rilievo in forma direttamente proporzionale alla 'dipendenza informatica' da parte dei paesi tecnologicamente più avanzati e costituisce oggi uno dei più efficaci metodi di lotta asimmetrica".

Entrando poi nello specifico delle implicazioni della minaccia cyber in ambito militare, il capo di Stato maggiore della Difesa ha evidenziato che "l'elevato livello tecnologico che caratterizza anche gli assetti delle nostre Forze armate, ci espone ad attacchi cyber che possono avere una diretta incidenza in molteplici aspetti delle attività militari, come la gestione dei sistemi d'arma e le comunicazioni tattiche ed operative durante operazioni militari". "Ormai il 60 per cento della nostra attività è cyber. Il Comando interforze per le operazioni cibernetiche (Cioc) sta già operando e raggiungerà la piena capacità nel 2019", ha concluso il generale Graziano.

A cura di: **Fabrizio Di Ernesto**