l'Unità

07-GIU-2016
pagina 16
foglio 1

Le regole del cybergioco

Michele Pierri

Tra le sfide della politica mondiale di oggi, la sicurezza informatica è senza dubbio tra le più importanti. Nonostante ciò gli Stati sono attori relativamente "nuovi" nel dominio cibernetico, che si configura sempre più come il nuovo terreno dove misurare la sicurezza, la competitività e dunque il benessere delle nazioni.

In questo quadro in continua evoluzione, cyberspazio e politica internazionale sono sempre più interconnessi e stanno entrambi cambiando rapidamente, influenzandosi a vicenda. Chi governerà queste nuove praterie virtuali? Come possono muoversi i governi per non restare in questo processo di cambiamento? E cosa comporta tutto ciò sul piano geopolitico?

Di questi e di altri temi legati tra loro si parlerà a Roma nei prossimi giorni grazie alla presenza di un'ospite d'eccezione proveniente dagli Stati Uniti: Nazli Choucri, consulente del Dipartimento della Difesa Usa e della Darpa, l'agenzia a stelle e strisce che si occupa dello sviluppo di nuove tecnologie per uso militare.

La professoressa del Massachusetts Institute of Technology, autrice del best seller mondiale "Cyberpolitics in International Relations", sarà nella Capitale per un ciclo di conferenze di alto livello.

L'8 giugno l'esperta parlerà assieme al ministro della Difesa Roberta Pinotti, in un evento organizzato da Ibm Italia in partnership con la Luiss Business School presso la Sala delle Colonne di Viale Pola.

Il giorno seguente, invece, la professoressa del Mit terrà con il sottosegretario alle Comunicazioni Antonello Giacomelli un intervento nel corso di un seminario realizzato alla Camera dei Deputati dall'Intergruppo parlamentare per l'innovazione.

In entrambe le occasioni la docente illustrerà l'attuale scenario e come le politiche di cyber security influenzino e stiano mutando radicalmente i rapporti tra Stati.

Parallelamente alle opportunità e agli investimenti nel settore, infatti, crescono anche il cyber crime e le minacce che da un lato toccano la vita dei singoli cittadini, dall'altro provengono spesso da nazioni nemiche o non alleate e sono mirate a colpire asset strategici dei sistemi-Paese, come le reti energetiche, finanziarie o di difesa.

In questo frangente, crede la Choucri, una parte rilevante sarà giocata dalla capacità degli Stati di difendere le proprie infrastrutture critiche implementando modelli di sicurezza efficaci (ad esempio quelli indicati dal Framework, come quello americano del Nist o quello italiano realizzato dal Cis-Sapienza e dal Laboratorio di cybersecurity del Cini); dare più risorse ai Cert per identificare, valutare i pericoli e scambiare informazioni sensibili con i propri partner; e rafforzare la collaborazione tra pubblico e privato.

Gestire questa complessità comporterà poi per i governi un ulteriore sforzo sul piano diplomatico. C'è bisogno di definire le "regole del gioco", con norme internazionali per regolare lo spazio cibernetico, ma anche di stipulare - sulla strada intrapresa da Washington con Mosca e Pechino - accordi tesi alla costruzione di misure di fiducia e di reciproca deterrenza come in campo nucleare. Anche l'Italia muove i suoi passi in questo settore: l'Osce, l'Organizzazione per la sicurezza e la cooperazione in Europa, ha da poco avviato un progetto in collaborazione con l'Università di Firenze e finanziato anche dal Ministero degli Esteri italiano. Obiettivo: ridurre il rischio di cyber conflitti tra Stati attraverso la costruzione di percorsi collaborativi tra Stati.