Il Messaggero
19-LUG-2016
pagina 22
foglio 1

L'intervento

Antiterrorismo, l'arma in più della "Cyber security"

Paolo De Angelis

La crescente minaccia terroristica velocemente costringe i governi di tutto il pianeta ad aggiornare l'agenda alla voce sicurezza, per prevenire i rischi di attentati che, con drammatica cadenza, vengono realizzati in ogni latitudine. Non ci possono essere falle, la prevenzione è indispensabile di fronte ad un fenomeno sempre più violento e diffuso. Gli scenari mondiali sono in continuo aggiornamento per stabilire standard comuni di coordinamento antiterrorismo. In questo quadro, oltre agli interventi sul versante della sicurezza fisica dei cittadini, assume sempre maggior rilievo lo scenario informatico e la sicurezza dello spazio cibernetico. I maggiori analisti del mondo sono al lavoro per individuare i rischi che la rete informatica può correre in caso di attacco terroristico, per attuare strategie di prevenzione e risposta. C'è la consapevole certezza che un'azione terroristica informatica sia in grado di causare danni e conseguenze non meno devastanti di quelli tradizionali, per il rischio di completa paralisi di servizi e settori essenziali. L'antiterrorismo non è più solo di tipo militare o di controllo del territorio ma di tipo informatico, contro i rischi della cyber war, lessico anglosassone che evoca scenari di crimini cibernetici di altissimo livello, in grado di mettere in ginocchio lo Stato aggredito, contro i quali la risposta deve essere efficace e pronta. L'Italia ha adottato il Piano strategico nazionale per la sicurezza cibernetica e la protezione informatica, un testo normativo della Presidenza del Consiglio dei Ministri che detta le linee guida di prevenzione e di reazione in caso di attacco ai sistemi informatici sia pubblici che privati; è la prima volta che la sicurezza del comparto industriale e produttivo viene messa sullo stesso piano di quella dei sistemi telematici militari o della pubblica amministrazione in genere. È un salto culturale nella strategia della sicurezza perché considera il problema non solo nei tradizionali ambiti istituzionali ma in ogni aspetto della rete economica, organizzativa e strutturale del sistema Paese. L'impostazione del quadro strategico nazionale della cyber security risente positivamente delle influenze e delle esperienze di altri paesi che ci hanno preceduto, a volte di anni, nella visione della sicurezza informatica come priorità nazionale. Una normativa con molte luci, prima fra tutte l'individuazione e la previsione di azioni di prevenzione e di contrasto; infatti, dal primo testo in materia dell'anno 2013, che ha disegnato l'assetto istituzionale della sicurezza cibernetica, si è passati, nel dicembre 2015, ad un testo molto più completo ed operativo, anche grazie al significativo stanziamento di 150 milioni di euro destinato a realizzare concretamente il piano. Ci sono però anche le ombre, specie nella ripartizione dei ruoli e nella gerarchia dei protagonisti della strategia di sicurezza informatica: l'eccesso di organismi coinvolti e la suddivisione delle competenze tra i diversi ministeri (ben 6) e centri di coordinamento tecnico (ulteriori 7 soggetti istituzionali oltre agli operatori privati che gestiscono reti telematiche) rischia di burocratizzare l'azione, a discapito dell'efficienza e della immediatezza della risposta in caso di attacco, anche se il piano assegna il ruolo centrale nella gestione del sistema di sicurezza alla Presidenza del Consiglio, con funzioni di vertice sul piano decisionale ed organizzativo; tutto il piano strategico ruota attorno alle informazioni che devono transitare da un soggetto ad un altro in tempo reale, per le immediate contromisure in caso di attacco informatico e più è lunga la catena di comando, più lungo è il percorso delle informazioni prima di giungere al livello delle azioni. Ma anche se il meccanismo avrà necessità di essere regolato per garantire la massima efficienza, è già positivo che ci sia una struttura in grado di operare in caso di rischi di sicurezza della rete informatica e telematica italiana; la filosofia di fondo è che le politiche di Cyber Strategy non siano solo una mera tecnica, per le sofisticate conoscenze che richiedono, quanto una vera e propria strategia, intesa come risposta globale ed articolata, in cui la sicurezza sia un valore assoluto da tutelare, anche in un contesto non tradizionale ed in continua evoluzione come il crimine informatico. La parola chiave è quindi cultura: della sicurezza dei dati, delle informazioni e, in generale, delle risorse di cui i soggetti, pubblici o privati, dispongono; poi, cultura della protezione del patrimonio di conoscenza dei singoli, privati o pubblici, e degli interessi superiori dello Stato; infine, cultura informatica, per lo sviluppo della consapevolezza che il mondo web oramai coincide col mondo reale e la violazione delle reti informatiche non ha solo dimensione virtuale ma ha riflessi significativi anche sui rapporti giuridici ed economici concreti. È il momento di agire, allora: il terrorismo non aspetta.

Sostituto procuratore presso il Tribunale di Cagliari