LA STAMPA

11-GEN-2017
pagina 1
foglio 1

QUANDO LA TALPA CI AGGREDISCE DAL CYBERSPAZIO

GIAMPIERO MASSOLO

Il rapporto delle agenzie di intelligence americane sulle presunte interferenze russe nel processo elettorale americano. L'inchiesta della nostra polizia postale sugli episodi di spionaggio cibernetico di cui sarebbero responsabili due fratelli romani. Nel molto grande e nel molto piccolo, nella macro dimensione delle relazioni internazionali come nella micro rete dei nostri rapporti quotidiani, due vicende che fanno riflettere.

Le accomuna lo stesso senso di impotenza e insufficienza di ogni forma di difesa che evocano entrambe, pur su scala diversa. Ma è davvero così? Siamo davvero vulnerabili, come Stati e come individui?

La minaccia purtroppo è reale. Si evolve di pari passo con il progresso tecnologico, si nutre delle nostre stesse consuetudini di comportamento, trova stimolo nella messe crescente di dati e notizie che affidiamo alla nostra presenza digitale. Inutile continuare a meravigliarci: carpire dati sensibili on line può essere reato, ma tecnologie avanzate e comportamenti inconsapevoli offrono possibilità virtualmente illimitate. A compiere illeciti, poi, è soprattutto una massa puntiforme, e per questo poco controllabile, di soggetti privati.

Molto più degli Stati e dei loro operatori, vincolati da perimetri giuridici definiti e dediti caso mai a pratiche e mezzi di influenza e di intelligence certamente non nuovi, pur se oggi molto più macroscopici, avanzati e efficaci.

Come difenderci? Fermo restando, ci piaccia o meno, che la sicurezza assoluta non esiste e che ogni muro è aggirabile, un efficace sistema di difesa non può che basarsi su di una combinazione di fattori: organi di prevenzione e repressione attrezzati, collaborazione internazionale, stretto rapporto tra autorità pubbliche e aziende private, più consapevolezza dei comportamenti individuali. Il loro insieme e le loro interazioni costituiscono in un Paese l'architettura nazionale di sicurezza cibernetica.

Sul piano degli organi preposti, è di cruciale importanza monitorare i segnali premonitori degli attacchi, mappare i rischi, individuare le falle più rilevanti del sistema, definire per tempo efficienti procedure in caso di attacco e ripartire con precisione ruoli e competenze, dotarsi di tempestivi e snelli sistemi di allarme, saper riparare con prontezza i danni per evitare che si allarghino a macchia d'olio. L'azione della polizia postale e della nostra intelligence di questi giorni dimostrano che in Italia progressi non sono mancati. Continuare ad investire, anche finanziariamente, nella sicurezza cibernetica rimane essenziale.

Si tratta, d'altra parte, di rischi dai quali nessuno Stato è al riparo e compiti che non possono essere svolti individualmente: di qui, l'importanza della collaborazione internazionale, sia tra Paesi che condividano le stesse alleanze e tradizioni, sia nel quadro dei principali organismi multilaterali. Non esiste, sotto il profilo della vulnerabilità cibernetica e malgrado varie ambizioni, un vero primo della classe nel mondo e questo dovrebbe indurre a rafforzare quello scambio di esperienze e buone pratiche, che ancora stenta a decollare.

Segno distintivo di ogni sistema di sicurezza è poi la qualità del rapporto tra autorità preposte e aziende private, molte delle quali gestiscono direttamente infrastrutture critiche e servizi di pubblico interesse. La collaborazione, nelle nostre economie di mercato, non può essere imposta per legge. È dunque indispensabile sviluppare un clima di fiducia reciproca che consenta di scambiarsi informazioni su attacchi informatici subiti e sulle modalità di riparazione dei danni. Molto è stato fatto in Italia e nell'Ue sotto questo profilo, ma è un processo destinato a continuare.

E infine l'aspetto dei nostri comportamenti individuali. Nessun sistema di sicurezza è efficace se non si basa sulla stretta collaborazione tra chi tutela e chi viene tutelato. La protezione della nostra privacy - è giusto aspettarselo - dipende dal livello di sicurezza informatica dell'ambiente che ci circonda. Anche il più sofisticato dei sistemi, tuttavia, non può esimerci dall'uso responsabile della rete. Nella consapevolezza che, se molti sono i guardiani, molti più potrebbero essere i male intenzionati.