L'ANALISI

Dagli Usa alla Russia: la guerra 3.0 che agita il pianeta

Fausto Biloslavo

L'ombra degli hacker russi sulle elezioni americane, l'allarme dei servizi segreti per il voto in Francia e Germania nel 2017 e la Ue che chiede aiuto alla Nato sono tutti esempi della nuova «guerra», la 3.0, che si combatte con attacchi cibernetici sempre più sofisticati.

In Italia, dove è appena stato scoperto a Roma la punta dell'iceberg dello spionaggio digitale, i crimini informatici nel 2016 hanno raggiunto il picco più elevato degli ultimi tre anni.

Ieri, per la prima volta, il nuovo presidente americano, Donald Trump, ha ammesso che «forse gli attacchi informatici sono stati compiuti dalla Russia, ma credo anche da altri Paesi» riferendosi al rapporto dell'intelligence sulle intrusioni digitali durante le elezioni.

Trump ha sempre sostenuto che gli hacker non hanno influenzato il risultato, ma la Cia è convinta che il gruppo di pirati russi «Orsi fantasiosi» abbia preso di mira soprattutto i democratici. E *Wikileaks* ha reso pubblici 19mila messaggi di posta elettronica di Hillary Clinton e altri big del partito.

L'8 dicembre l'allarme è rimbalzato in Europa con un inusuale comunicato dei servizi segreti tedeschi, che hanno denunciato l'impennata di attacchi «aggressivi di cyber spionaggio» contro i politici tedeschi. Il vero timore, come ha lasciato capire la stessa cancelliera Angela Merkel, è che le cruciali elezioni politiche di settembre possano diventare il campo di battaglia della nuova «guerra» 3.0.

Anche per le presidenziali francesi di aprile si teme un'offensiva cyber. Il ministro della Difesa, Jean-Yves Le Drian, lo ha ammesso pubblicamente.

«Sarebbe ingenuo - ha avvertito - pensare che la Francia, dove gli attacchi informatici l'anno scorso sono raddoppiati, possa restare immune da questo rischio».

L'obiettivo non è solo il mero spionaggio informatico, ma la manipolazione delle informazioni collegata ad un evoluto modello di *disinformazia* di sovietica memoria. La tattica, come nel caso scoperto a Roma, è infilarsi nei computer o nei cellulari di politici e autorità grazie ad un cavallo di Troia digitale, che copia tutti i dati senza che le vittime se ne accorgono. Poi si stabilisce se e come divulgarle. L'evoluzione della minaccia è la manipolazione delle informazioni piratate, che vengono trasformate in notizie false, parzialmente vere o divulgate ad arte per poi venire ingigantite dalla cassa di risonanza dei social. Nella campagna per la Casa Bianca è stato calcolato che le 20 notizie false più forti sono state riprese su Facebook 8,7 milioni di volte.

La campagna cyber in vista delle elezioni in Europa nel 2017, comprese quelle olandesi e forse italiane, è già iniziata. Lo scorso anno i server della Commissione nel quartier generale Ue di Bruxelles hanno subito 110 attacchi di pirateria informatica, il 20% in più rispetto al 2015. Ed in novembre c'è stato il culmine con un'offensiva cyber su larga scala. Bruxelles conserva i dati sensibili dei 28 stati membri. I funzionari europei hanno ricevuto l'ordine di usare messaggi di posta elettronica criptati.

La Commissione ha chiesto aiuto alla Nato per rafforzare le misure anti hacker, ma è curioso che i più insidiosi sistemi di intrusione dello spionaggio cibernetico, come Sauron, si sospetta siano stati sviluppati dai governi.