

La mappa dei cyber attacchi in tempo reale della russa Kaspersky, specializzata in software per la sicurezza informatica.



CYBERATTACK

Luglio è stato il mese delle manovre informatiche contro Teheran e Londra. Registi delle operazioni Israele e Russia. Si ruba di tutto. Dai dati personali a quelli sui vaccini, dai segreti militari ai conti correnti.

LA SPESA MONDIALE PER LA SICUREZZA RAGGIUNGERÀ I 133,7 MILIARDI DI DOLLARI NEL 2022

di Stefano Piazza e Luciano Tirinnanzi

Luglio è stato il mese dei grandi attacchi cibernetici contro Londra e Teheran. Autori? I soliti noti. La micidiale serie di hackeraggi contro obiettivi iraniani reca la «firma» di Israele, che non intende permettere agli ayatollah di minacciare la nazione ebraica con l'arma atomica. Questo ha comportato incendi alla flotta navale ancorata nel porto di Bushehr. Ma, soprat-

tutto, un rogo alle centrifughe di Natanz, principale struttura per l'arricchimento dell'uranio. Il danno è stato così serio che la ricerca iraniana è tornata indietro di oltre un anno sulla tabella di marcia per il nucleare.

Mentre, secondo la Nsa e il Ncsc, agenzie gemelle per la cybersecurity dei governi americano e britannico, la Russia avrebbe tentato di rubare nientemeno che il vaccino contro il Covid-19. O, per meglio dire, la formula creata dallo Jenner Institute di Oxford insieme all'italianissima Irbm di Pomezia (che potrebbe entrare in commercio già a novembre).

Sul banco degli imputati, per quanto riguarda Natanz, c'è la Unit 8200 israeliana, che può aver agito direttamente contro i terminali iraniani oppure sfruttando oppositori interni alla Repubblica islamica. Quest'ultima possibilità sarebbe confermata da una rivendicazione dell'incendio, inviata alla Bbc da un gruppo noto come i «Gheparidi della Madrepatria».

Il probabile sabotaggio contro l'Iran, del resto, è in linea con la strategia israeliana, che affonda le radici nella storia recente dello Stato ebraico. Fu il premier Menachem Begin il primo a rendere operativo questo sistema, attraverso una dottrina che consisteva nel ritenere legittimo qualsiasi intervento di Israele contro la corsa al nucleare di Paesi nemici. Accadde con l'operazione «Babilonia», con cui nel 1981 una squadra di F-16 israeliani bombardò il reattore iracheno di Osirak, bloccando definitivamente ogni velleità nucleare di Baghdad. E fu ripetuto in Siria nel 2007, quando jet israeliani rasero al suolo la centrale nucleare di Deir Ezzor.

Oggi la tecnologia permette sortite non meno efficaci, ma meno «rischiose». In questo è specializzato il gruppo di hacker russi denominato Apt-29 o «Cozy bear», braccio armato della Fsb (i servizi segreti russi) per il cyberspazio. L'Apt-29 è lo stesso ritenuto responsa-

