Israele inaugura l'epoca in cui tutto è un'arma

ariannaeditrice.it/articoli/israele-inaugura-l-epoca-in-cui-tutto-e-un-arma

di Pino Cabras - 18/09/2024

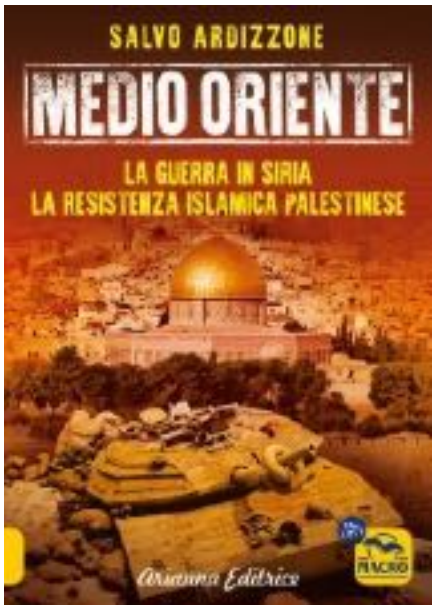
Fonte: Pino Cabras

L’inedita forma dell’atto di guerra con cui oggi Israele ha improvvisamente colpito il Libano causando decine di morti e migliaia di feriti è da considerare già adesso una pietra miliare dei conflitti del XXI secolo. Non c’è più un posto sicuro. Ogni forma di connessione incastonata negli oggetti della vita quotidiana e attivabile da remoto con intenti maligni è pronta a essere usata come un’arma.
Abbiamo visto centinaia di esplosioni contemporanee partite da dei cercapersone usati da militanti di Hezbollah – paradossalmente usati per essere meno connessi e meno aggredibili rispetto all’uso dei telefoni cellulari – hackerati, manomessi fino a usare le loro batterie come innesco. Molti innocenti che si trovavano vicino alle persone colpite sono stati coinvolti in modo massiccio e indiscriminato. Restano da chiarire alcune circostanze misteriose sull’abnorme portata dei danni (c’è chi ipotizza che molti dispositivi avessero addirittura grammi di esplosivo inseriti da qualche “talpa” che avrebbe intercettato e alterato la fornitura). Ma già adesso – oltre il singolo episodio - possiamo riflettere su quel che è implicato da questo caso.
In teoria, un numero enorme di oggetti connessi all'Internet delle Cose (IoT), inclusi dispositivi di domotica, impianti di produzione distribuita di energia, automobili altamente elettroniche e altri dispositivi intelligenti, sono vulnerabili ad attacchi informatici. Gli attacchi potrebbero avere potenzialmente effetti devastanti. Termostati intelligenti, telecamere di sicurezza, serrature elettroniche, luci e elettrodomestici connessi possono essere hackerati. Un attacco sufficientemente sofisticato rivolto a sistemi iper-connessi potrebbe riguardare in

un domani abbastanza vicino milioni di famiglie immerse nell'entusiasmo della crescente digitalizzazione delle loro chincaglierie elettroniche.
Le tecniche possono risultare persino "banali" nella loro linearità. Oggi il server del cercapersone è stato violato, provocando l'installazione di uno script che ha generato un sovraccarico. Questo sovraccarico potrebbe aver causato il surriscaldamento della batteria al litio, la quale è successivamente esplosa. Conseguenze: decine di ospedali costretti a chiedere urgenti donazioni di sangue. Caos, sgomento.
Domani – e non solo in Libano - possiamo immaginare un attacco diffuso su più dispositivi che potrebbe creare in ogni casa numerosi punti di stress, da termostati sovraccaricati a elettrodomestici lasciati in funzione troppo a lungo, che insieme potrebbero aumentare esponenzialmente il rischio di incendi.
O automobili portate a causare incidenti di massa. O mille altri scenari che sfruttano la vulnerabilità della nostra epoca.
Fino a oggi, ogni invenzione è stata anche l'invenzione del suo cattivo funzionamento. Per capirci: inventi l'elettricità, che prima non c'era? Bene, hai inventato anche il problema del black out, che pure prima non c'era. Adesso scopriamo che ci sono forze potenti che considerano ogni invenzione anche l'invenzione di una nuova arma in grado di essere usata sulle masse. Il test libanese è ampiamente scalabile.
C'è anche un corollario, per tutto questo: ci sarà una corsa a dire che le "cyber-minacce" richiedono contromisure adeguate. Un po' come il discorso dei virus informatici che creano il business degli antivirus. Solo che sarà moltiplicato su una scala incomparabilmente più estesa che abbraccia ogni oggetto connesso alla Rete.
Ricordiamoci che la strategia della tensione a livello planetario che ha avuto l'impronta iniziale della mega-operazione terroristica dell'11 settembre 2001 ha creato l'immenso indotto di una nuova e ossessiva economia "securitaria". Negli ultimi vent'anni è tutto un proliferare di imprese, agenzie, nuove professioni che ci promettono più sicurezza, ma che hanno divorato pezzi significativi dei bilanci con una tendenza a espandersi indefinitamente e con una vocazione al controllo che ha eroso le libertà dei cittadini.
Molte imprese del settore della cybersicurezza sono israeliane. È una specializzazione mondiale che vede molti politici di tutto il mondo stendere loro tappeti rossi con totale negligenza rispetto alla propria sicurezza nazionale. Vero Gasparri?
Possiamo vedere l'episodio libanese di oggi come un macabro spot pubblicitario: "vedete come tutti sono esposti ai pericoli? C'è bisogno di protezione! Abbiamo giusto alcune aziende che farebbero al caso vostro. E non tirate fuori quell'esempio trito e ritrito della volpe nel pollaio, su, per favore!"

Israele - Libro

Dialogo impossibile con un rabbino - Libro



Medio Oriente - Volume III