Le tattiche tecnologiche di Israele e il futuro della guerra totale

geopolitika.ru/it/article/le-tattiche-tecnologiche-di-israele-e-il-futuro-della-guerra-totale

9 luglio 2025

Geopolitica

10.07.2025

Aleksandr Dugin

Dall'inizio del conflitto israelo-palestinese a Gaza – quasi immediatamente dopo l'attacco di Hamas contro Israele durante l'operazione Al-Aqsa Flood, che ha innescato una reazione a catena di eventi successivi – abbiamo assistito all'impiego da parte di Israele di tecnologie militari mai viste prima in azione. Queste tecnologie hanno svolto un ruolo

decisivo nel garantire il successo israeliano in diverse operazioni militari e politiche. Esse hanno comportato l'uso di dispositivi di comunicazione, computer, telefoni cellulari e persino cercapersone per infliggere perdite sensibili, se non addirittura critiche, al nemico. Questa tattica era strettamente intrecciata con attacchi missilistici e droni da combattimento. Inoltre, è ormai chiaro che Israele ha impiegato attivamente la tecnologia deepfake.

Insieme, questi fattori hanno trasformato radicalmente la natura della guerra moderna. Gli avversari di Israele in Medio Oriente erano completamente impreparati a questo cambiamento, che si è rivelato decisivo nello svolgersi del conflitto. In termini militari convenzionali, c'era stata una parità approssimativa tra Israele e i suoi avversari regionali e, nelle tattiche di guerriglia, gruppi come Hezbollah in Libano avevano persino avuto il sopravvento, come dimostrato durante la guerra del Libano del 2006. Tuttavia, l'introduzione di questo nuovo fattore tecnologico ha alterato drasticamente l'equilibrio di potere.

Quali erano queste nuove tecnologie e metodi? Il più importante tra questi era un software di sorveglianza di livello radicalmente avanzato. Gli israeliani sono riusciti a installare programmi di tracciamento praticamente in ogni dispositivo elettronico appartenente ai loro avversari. Movimenti, conversazioni, incontri e scambi di informazioni tra palestinesi, siriani, libanesi, iracheni e iraniani, chiunque avesse anche solo una rilevanza marginale per Israele, erano completamente visibili all'intelligence israeliana.

Nel suo libro del 2019 L'Impero e i Cinque Re, il globalista Bernard-Henri Lévy lamentava il graduale ritiro dell'Occidente dal Medio Oriente (in particolare dall'Iraq), sottolineando che l'unica compensazione per l'abbandono di tali posizioni strategiche era l'attuale capacità di sorveglianza iper-sofisticata dell'Occidente, in grado di rilevare anche il minimo dettaglio nei territori che venivano abbandonati. Lévy, un imperialista aggressivo, considerava questo insufficiente, un segno di debolezza e passività. Avrebbe preferito un controllo fisico diretto sul mondo islamico da parte dell'Occidente e di Israele (da qui il titolo del libro, che fa riferimento alla guerra dell'antico Israele contro una coalizione di cinque re cananei, che gli israeliti sconfissero e soggiogarono). Ma l'osservazione di Lévy sulla sorveglianza era acuta. Questo è diventato il fattore cruciale a partire dal 2023.

I sistemi di comunicazione e i dispositivi collegati in rete – elettronici, locali e di altro tipo – sono diventati armi letali nelle mani di Israele, determinando l'esito delle operazioni a Gaza, in Libano, in Siria e nella recente guerra di 12 giorni con l'Iran. L'assistenza degli Stati Uniti e dell'Occidente in generale è stata significativa, ma il vantaggio decisivo è venuto dalla nuova strategia. Israele è riuscito a ottenere il controllo completo sulle reti dei suoi nemici, trasformando telefoni, cercapersone e vari dispositivi elettronici in armi. Alcuni cercapersone destinati agli agenti di Hezbollah (che diffidavano dei telefoni cellulari) sono stati riempiti di esplosivo. Secondo i rapporti libanesi, non solo i cercapersone sono esplosi, ma anche i telefoni cellulari, gli scooter elettrici, i citofoni e i pannelli degli ascensori. La natura esatta di questa tecnologia rimane poco chiara, ma se esiste e se Israele la possiede, essa comporta rischi senza precedenti.

Un altro elemento coinvolto sono stati i droni lanciati sulla base dei dati di targeting acquisiti attraverso la sorveglianza, spesso dall'interno del territorio nemico. Questa tattica è stata resa nota per la prima volta nel luglio 2024, quando il leader di Hamas Ismail Haniyeh è stato eliminato in Iran. Metodi simili sono stati poi utilizzati per uccidere i leader di Hamas non solo a Gaza, ma anche in altri paesi. Grazie alla sorveglianza elettronica, gli israeliani avevano i loro obiettivi sotto controllo; il resto era solo una questione di esecuzione. I droni potevano essere lanciati da Israele o da nascondigli preparati in anticipo in paesi stranieri.

È persino possibile che l'operazione di sabotaggio che ha portato alla morte del presidente iraniano Ebrahim Raisi abbia coinvolto un cercapersone e una tecnologia di sorveglianza. Raisi era un conservatore e un convinto oppositore di Israele. Sebbene le autorità iraniane non siano riuscite a determinare la causa dell'incidente elicotteristico, gli eventi della guerra dei 12 giorni potrebbero spiegare il perché: semplicemente non disponevano della tecnologia necessaria e non avevano alcuna comprensione di come funzionassero tali sistemi.

Dopo aver eliminato la leadership di Hamas, Israele ha rivolto la sua attenzione a Hezbollah. Attacchi mirati hanno ucciso lo sceicco Hassan Nasrallah e praticamente tutta la leadership di Hezbollah, che un tempo rappresentava una seria minaccia per Israele. In combinazione con l'esplosione di cercapersone e dispositivi, questi omicidi e persino le uccisioni di massa dei membri di Hezbollah sono diventati straordinariamente efficaci. Sono seguiti attacchi precisi con droni e missili, non casuali ma basati su obiettivi identificati attraverso la sorveglianza elettronica. Gli israeliani hanno pianificato queste operazioni meticolosamente, iniziando lo sterminio dall'alto verso il basso: prima eliminando la leadership al vertice – religiosa e politico-militare – poi il secondo livello, il terzo e così via attraverso i ranghi.

In Siria, è stato il Mossad a portare al potere al-Sharaa, affiliato all'ISIS, orchestrando un cambio di regime e destituendo il presidente Bashar al-Assad utilizzando le stesse tecniche. Israele ha ottenuto il pieno controllo delle comunicazioni militari siriane. Sono stati ampiamente utilizzati i deepfake. Ordini e direttive – a volte contraddittori – sono stati inviati ai comandanti di rango inferiore, apparentemente dai vertici militari siriani, imitando persino la voce dello stesso Assad. Questi includevano ordini di ritirata, ridistribuzione in posizioni insensate o fuoco su obiettivi falsi. Il cambio di regime è stato ottenuto meno attraverso la forza militare convenzionale che attraverso le tecnologie di rete. Israele ha anche consolidato la sua presa sulle alture del Golan, ha ampliato la sua zona di controllo vicino alle aree druse più vicine a Damasco e ha distrutto, utilizzando droni e missili, ogni installazione militare siriana che rappresentasse anche solo una remota minaccia. In precedenza, le forze di Hezbollah e iraniane (in particolare le unità dell'IRGC) in Siria erano già state oggetto di attacchi mirati e costrette a ritirarsi una volta iniziata la rivolta di al-Sharaa.

Poi è stata la volta dell'Iran. Ancora una volta è stata utilizzata la stessa strategia. Nelle prime ore della guerra durata 12 giorni, Israele ha eliminato quasi tutto il vertice militare iraniano – il capo di Stato Maggiore, il comandante dell'IRGC e i principali scienziati

nucleari – insieme alle loro famiglie, compresi i bambini piccoli. Ciò è stato possibile in parte grazie a missili di precisione e in parte grazie a droni lanciati dall'interno dell'Iran, utilizzando depositi preposizionati. I droni sono stati lanciati fisicamente da migranti afghani seguendo le istruzioni israeliane, pagati con somme modeste e considerati sacrificabili dai pianificatori israeliani.

I successivi attacchi missilistici hanno preso di mira le infrastrutture nucleari iraniane, portando a un'operazione di cambio di regime. Affinché tutto questo avesse successo, Israele aveva bisogno del pieno controllo su ogni individuo iraniano ritenuto una potenziale minaccia o di interesse, e anche in questo caso attraverso dispositivi elettronici. La strategia è stata meno efficace contro gli Houthi dello Yemen, ma anche loro sono stati occasionalmente colpiti da attacchi di precisione che hanno causato gravi danni.

Abbiamo quindi assistito alla nascita di forme di guerra letali completamente nuove. Israele possiede tecnologie che gli hanno permesso di infliggere danni inimmaginabili ai suoi nemici. Siamo entrati in un'era completamente nuova della guerra.

Durante le prime fasi dell'Operazione Militare Speciale (SMO), ci siamo trovati inaspettatamente di fronte al problema dei droni e delle comunicazioni. Tuttavia, ciò che vediamo ora in Israele rappresenta un livello molto più avanzato. Se voi o i vostri familiari possedete un dispositivo elettronico e se entrate in conflitto con gli interessi di Israele, potete essere eliminati in modo chirurgico, efficiente e in qualsiasi momento. Questa è la terrificante conclusione di ciò a cui abbiamo appena assistito in Medio Oriente.

Un'altra preoccupazione è la neutralizzazione delle flotte nemiche e dei porti marittimi. Anche in questo caso, le tecnologie dei droni acquatici, non ancora completamente implementate, rappresentano un pericolo colossale, soprattutto se combinate con sistemi di sorveglianza avanzati.

Ci troviamo quindi di fronte a un intero blocco di nuove minacce. Il punto successivo: Israele è il più stretto alleato degli Stati Uniti e dell'Occidente collettivo. Alcuni vedono Israele come un proxy geopolitico degli Stati Uniti, mentre altri, in particolare gli israeliani, vedono gli Stati Uniti come un golem sottomesso al comando israeliano. In entrambi i casi, l'essenza è la stessa: le tecnologie che Israele ha utilizzato con tanta efficacia nella guerra contro i suoi avversari regionali sono senza dubbio note e accessibili agli Stati Uniti e all'Occidente. In effetti, non è chiaro se si tratti di invenzioni puramente israeliane. Forse hanno avuto origine dalla CIA, dal Pentagono, dalla Palantir o dall'MI6, oppure sono state sviluppate congiuntamente. Questo non ha molta importanza. Il punto è che l'Occidente possiede queste armi e ha imparato a padroneggiare queste strategie e tecnologie.

La Russia non è in guerra con Israele (anche se non dimentichiamo che l'Iran è nostro alleato), quindi si potrebbe pensare che siamo al sicuro da tali tattiche. Forse. Tuttavia, siamo innegabilmente in guerra con l'Occidente collettivo in Ucraina, e l'Ucraina è

inequivocabilmente un proxy, uno strumento, dell'Occidente collettivo. Da qui la semplice e terrificante conclusione: questa tecnologia letale può, in qualsiasi momento, essere rivolta contro la Russia.

Se guardiamo agli attacchi terroristici compiuti dai sabotatori ucraini in Russia – contro Daria Dugina (e me stesso), contro Vladlen Tatarsky e Zakhar Prilepin, contro generali russi come Moskalyok e Kirillov, e anche all'attacco al Crocus City Hall che ha coinvolto migranti reclutati da Kiev – allora il recente attacco con droni alla triade nucleare russa dal territorio russo deve essere visto in quel contesto. In una situazione critica, una tale strategia potrebbe essere pienamente implementata – o potrebbe già esserlo stata, anche se in forma limitata.

Sorgono domande logiche: possediamo sistemi d'arma simili? Abbiamo penetrato i dispositivi e i gadget nemici, non solo quelli dell'Ucraina, ma anche quelli degli Stati Uniti e della NATO? D'altra parte, disponiamo di difese adeguate contro tali attacchi e strategie? È chiaro che i nostri migliori specialisti stanno lavorando alacremente per garantire la sicurezza del presidente, la nostra risorsa chiave nella guerra contro l'Occidente. Ecco perché non possiede dispositivi elettronici, il che è prudente. Eppure continuiamo a digitalizzare ed elettrificare tutto, affidandoci all'intelligenza artificiale che, come altre tecnologie di rete, potrebbe già essere stata trasformata in arma o potrebbe facilmente diventarlo. L'IA può uccidere? La risposta è evidente dall'esperienza dei libanesi e degli iraniani: se i telefoni e i cercapersone possono uccidere, allora l'IA può certamente essere trasformata in arma in determinate condizioni. I deepfake, generati dall'IA, sono già diventati armi.

Inoltre, siamo pienamente consapevoli che le strutture di rete possono essere facilmente integrate nelle comunità di immigrati, in particolare tra gli immigrati illegali? Si tratta di operatori tecnici già pronti. Israele non avrebbe mai potuto integrare reti di sabotaggio così radicate nelle società senza una rete di agenti d'élite sul campo.

Infine: la Cina possiede tali tecnologie di rete militare? In questo momento, la Cina si trova di fronte a una decisione cruciale: se entrare in aperto conflitto con l'Occidente in Iran e nel Medio Oriente in generale, dove l'Occidente sta sferrando attacchi mirati contro i centri energetici e di trasporto cinesi. Probabilmente lo scopriremo presto.

In ogni caso, questa è ora la minaccia più grave che la Russia contemporanea deve affrontare. Tutto il resto possiamo gestirlo. Qui, invece, ci troviamo di fronte a qualcosa di completamente nuovo e, se ci troveremo impreparati in un momento critico, le conseguenze potrebbero essere davvero fatali.

Traduzione di Costantino Ceoldo