La guerra elettronica contro Starlink di Iran, Russia e Cina

ariannaeditrice.it/articoli/la-guerra-elettronica-contro-starlink-di-iran-russia-e-cina

di Giacomo Gabellini - 19/01/2026

Fonte: Analisi Difesa

Lo scorso 11 gennaio, il quotidiano israeliano «Ma'ariv» ha riportato le valutazioni formulate in merito ai disordini che attraversavano l'Iran ormai da diversi giorni dallo specialista in questioni di sicurezza Ehud Ya'ari.

A suo avviso, «*non si vedono crepe evidenti nei meccanismi del regime, dal governo ai suoi due eserciti, quello regolare e le Guardie Rivoluzionarie, né in seno ai Basij. Vediamo segni di esitazione qua e là, niente di più».*

Anche perché già allora non si registrava «*una continua espansione della rivolta. Non c'è aumento nel volume delle manifestazioni: proseguono ma non si espandono, non assumono dimensioni nuove e più ampie, come accaduto nel 1978-1979, prima che Khomeini arrivasse a Teheran».*

Per la precisione, fino a poche ore prima «c'erano 60 centri di protesta, non di più. Prima ne avevamo 300 o più. Di questi, 36 erano a Teheran, principalmente nella zona est della città. La maggior parte delle proteste sono di medie dimensioni, non grandi».

Uno dei fattori determinanti a depotenziare l'ondata di destabilizzazione e ricondurre a situazione sotto il controllo delle autorità di Teheran è consistito indubbiamente nella disattivazione della rete internet, disposta, stando a quanto affermato dal ministro degli Esteri iraniano Abbas Araqchi, «*dopo che abbiamo affrontato operazioni terroristiche e ci siamo resi conto che gli ordini provenivano dall'esterno del Paese».*

Più specificamente, il passaggio cruciale va individuato nella capacità iraniana di "neutralizzare" Starlink, sistema internet a banda larga sorretto da una rete di migliaia di satelliti in orbita bassa prodotto dalla Space-X di Elon Musk, e impiegato sistematicamente dai contestatori iraniani.

Come funziona Starlink

Concepito ufficialmente come sistema satellitare a fini civili e commerciali, Starlink si è prestato immediatamente a impieghi di carattere militare perché i satelliti in orbita bassa di cui si avvale trasmettono segnali di velocità di gran lunga superiore a quelli emessi dai satelliti che gravitano in orbita geosincrona attorno all'equatore.

I segnali trasmessi ai terminali terrestri dai circa 10.000 satelliti Starlink che gravitano a una velocità orbitale di oltre 27.000 km/h risultano molto più difficili da localizzare e interrompere rispetto a quelli emessi dai tradizionali sistemi satellitari che fanno capo a singole unità geostazionarie.

I piani orbitali di Starlink sono mutevoli, così come le traiettorie di movimento della costellazione satellitare, generando una incertezza spaziotemporale che pone enormi problemi a qualsiasi attore eterno intenzionato a sabotare il sistema.

Ogni singolo terminale può "saltare" da un satellite all'altro in caso di interruzione del segnale che riceve in origine. Impiega per di più antenne phased-array e tecniche di frequency hopping modulabili da remoto da personale di Space-X, garantendo una straordinaria capacità di adattamento in tempo reale.

Nel marzo 2022, a seguito di una serie di test, il 388° Fighter Wing dell'Aeronautica degli Stati Uniti (USAF) ha confermato che Starlink applicato alla guida dei caccia F-35A garantiva una velocità di connessione di circa 30 volte superiore rispetto ai satelliti militari, offrendo una connessione internet a bassa latenza e ad ampia larghezza di banda cruciale per lo sviluppo dei futuri sistemi di comando e controllo.

Starlink in Ucraina

Starlink è stato prontamente messo a disposizione delle forze armate ucraine, che se ne sono avvalse per manovrare droni e guidare proiettili di artiglieria e missili contro le postazioni russe.

Nel corso di un'audizione dinnanzi alla Commissione Forze del Senato degli Stati Uniti risalente sempre al marzo 2022, il generale James Dickinson dello Us Space Command ha riconosciuto di esser rimasto colpito dalla capacità di Starlink di resistere alla guerra elettronica e fornire accesso a internet nelle zone dell'Ucraina devastate dal conflitto. L'impiego di Starlink in Ucraina «*ci sta davvero dimostrando quali risultati sono in grado di conseguire le megacostellazioni di satelliti»,* ha aggiunto Dickinson.

Nella primavera del 2024, la situazione stava già cambiando sensibilmente. Nel corso di alcune operazioni militari portate avanti in quel periodo nell'oblast di Kharkiv, le forze armate russe misero in campo disturbatori elettronici in grado di compromettere il corretto funzionamento di Starlink.

Lo rivelò il ministro per i Servizi Digitali ucraino Mykhailo Fedorov, secondo cui i russi stavano affinando con successo le proprie capacità tecnologiche contro Starlink. Le esternazioni di Fedorov furono confermate al New York Times da Ajax, nome di battaglia del comandante di un'unità ucraina specializzata nell'impiego dei droni inquadrata nel 92° Reggimento. A detta di Ajax, l'Ucraina stava «*perdendo la battaglia contro la guerra elettronica*» russa.

A pochi mesi di distanza, il Ministero della Difesa russo annunciò che il Kalinka, congegno elettronico concepito per identificare segnali emanati da sistemi di comunicazione satellitare come Starlink, si trovava ormai in fase di test di combattimento bell'ambito dello sviluppo e aggiornamento dei sistemi di guerra elettronica.

Andreij Bezrukov, amministratore delegato del Center for Unmanned Systems and Technologies, spiegò che Kalinka risultava particolarmente adatto a rilevare la presenza di droni aerei e marini senza pilota, ma anche per «*individuare i nodi di comunicazione Starlink fissati a terra in zone di guerra».*

Starlink in Iran

Da quando, nel 2022, l'amministrazione Biden concesse alle aziende statunitensi dell'alta tecnologia un'esenzione alle sanzioni per autorizzarle a vendere agli iraniani apparecchiature per la comunicazione, migliaia di terminali Starlink sono stati introdotti clandestinamente all'interno della Repubblica Islamica dall'Armenia e dal Kurdistan iracheno.

La diffusione su vasta scala di Starlink che ne è conseguita si è rivelata determinante ai fini dell'allargamento a macchia d'olio delle proteste scoppiate per la morte sotto custodia di Mahsa Amini.

Nel giugno dello scorso anno, il Parlamento di Teheran proibì l'utilizzo di Starlink, dopo che Elon Musk ne aveva disposto l'attivazione per aggirare lo spegnimento della rete internet nazionale disposto dal governo durante la guerra dei 12 giorni con Israele.

Nonostante il divieto, implicante pene detentive da sei mesi a dieci anni, alcune stime ipotizzavano che, all'inizio di luglio, tra i 20.000 e i 40.000 terminali Starlink introdotti attraverso canali di contrabbando funzionassero regolarmente in Iran.

Secondo quanto affermato da Ahmad Ahmadian, direttore esecutivo del gruppo statunitense Holistic Resilience, che collabora con gli iraniani per garantire l'accesso a internet all'interno della Repubblica Islamica, Starlink ha rinunciato al canone di abbonamento in Iran.

Una fonte anonima a conoscenza della questione ha confermato a Bloomberg che Starlink ha iniziato a fornire servizi gratuiti all'interno del Paese dopo lo scoppio delle rivolte.

Mehdi Yahyanejad, un iraniano la cui organizzazione no-profit Net Freedom Pioneers ha contribuito a far entrare clandestinamente unità Starlink in Iran, ha richiamato l'attenzione sull'importanza cruciale del sistema satellitare rispetto all'espansione delle proteste, perché ha consentito la condivisione di informazioni e il coordinamento tra i vari gruppi di contestatori anche dopo la disattivazione della rete internet disposta dal governo di Teheran l'8 gennaio e mantenuta in vigore per 168 ore.

Senonché, ha rivelato il direttore dei diritti digitali e della sicurezza presso il Miaan Group Amir Rashidi, proprio quel giorno si è registrata una perdita del circa il 30% del traffico uplink e downlink di Starlink, rapidamente salita all'80%.

Un calo notevolissimo, attribuito da Nariman Gharib, attivista dell'opposizione iraniana e investigatore indipendente di spionaggio informatico con sede in Gran Bretagna, alla trasmissione di falsi segnali Gps volta a confondere e disabilitare i terminali Starlink tramite jammer satellitari come il russo Murmansk-Bn, o il sistema di guerra elettronica iraniano Cobra-V8, simile al Krasukha-4 1RL257E di fabbricazione russa, o di altre apparecchiature prodotte internamente.

Rashidi formula invece un'osservazione più allarmata. «*Ho monitorato e studiato l'accesso a Internet negli ultimi 20 anni e non ho mai visto una cosa del genere in vita mia. Credo che il governo iraniano stia facendo qualcosa di più che disturbare il segnale Gps, come accade in Ucraina dove la Russia è regolarmente impegnata a disturbare Starlink*» attraverso la diffusione di onde radio di disturbo, ha affermato Rashidi.

"Interferenza attiva"

Lo specialista di informatica Kave Salamatian ha parlato in proposito di "interferenza attiva" finalizzata alla disconnessione dei terminali Starlink, implicante la saturazione del canale di trasmissione di un satellite attraverso la diffusione di segnali fittizi per un lasso di tempo sufficientemente ampio.

Teoricamente, questo modus operandi «potrebbe rendere il satellite inutilizzabile [per il terminale]. Quindi si possono semplicemente bloccare, uno dopo l'altro, tutti i satelliti Starlink visibili», afferma Radim Badsi, amministratore delegato della società francese Ground Space.

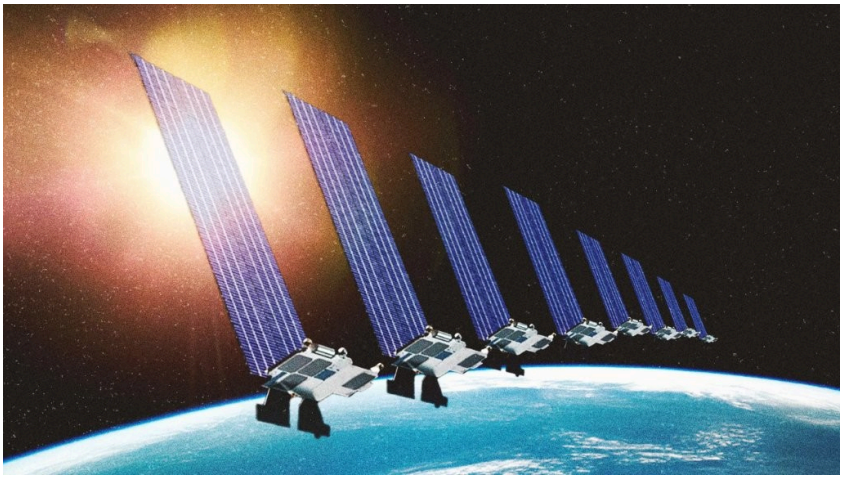
Il punto è che è *«tecnicamente piuttosto difficile bloccare il canale principale di Starlink perché la sua rete è composta da una moltitudine di satelliti in movimento*», sostiene l'ingegnere ucraino Oleg Kutkov.

Il quale rileva inoltre che *«dirigere un potente fascio di "rumore" direttamente verso il satellite nel cielo richiede più antenne paraboliche di grandi dimensioni che tracciano costantemente i satelliti. I russi hanno tentato questo approccio [in Ucraina], ma i jammer sono stati colpiti da droni e missili vista l'estrema difficoltà a nasconderli*».

Per Yair Kleinbaum di «J-Feed» (testata focalizzata su Israele e mondo ebraico), il risultato conseguito dalle autorità iraniane rispetto a Starlink scaturirebbe gli sforzi concertati di Pechino, Mosca e Teheran, nell'ambito di una netta divisione del lavoro in cui la Russia fornisce l'hardware, la Cina mette a disposizione l'apparato tecnologico e l'Iran funge da banco di prova.

Fino ad ora, Space-X contrastava il jamming russo in Ucraina grazie a rapidi aggiornamenti software, ma la situazione delineatasi in Iran presenta una sfida diversa: *«l'attuale interruzione è frutto di un attacco "brute force" basato sull'hardware che le patch software non riescono a eludere facilmente».*

Più specificamente, il modus operandi messo in campo in Iran rifletterebbe il modello teorico sviluppato dai ricercatori cinesi lo scorso novembre, che identifica nella disattivazione di Starlink una delle chiavi di volta per portare a compimento un'ipotetica invasione di Taiwan.



Come riporta il «South China Morning Post», *«per l'Esercito Popolare di Liberazione, prepararsi a una potenziale campagna su Taiwan significa risolvere una questione cruciale: come ottenere il predominio elettromagnetico quando il nemico può accedere a una costellazione di oltre 10.000 satelliti che interagiscono, si adattano e resistono alle interferenze in tempo reale?».*

Il piano d'azione elaborato dagli specialisti cinesi prevede la saturazione della banda di frequenza di cui si avvalgono i terminali Starlink per interagire con i satelliti mediante onde radio emanate sincronicamente da centinaia o migliaia di jammer distribuiti sia a terra che in cielo – su droni, palloni aerostatici e/o aerei.

Taiwan verrebbe così circondata e sovrastata da uno "scudo elettromagnetico" in grado di interdire ai terminali Starlink l'accesso ai satelliti.

Utilizzando dati satellitari Starlink, gli studiosi cinesi hanno simulato il posizionamento dinamico dei satelliti per un periodo di 12 ore sopra la Cina orientale e modellato la potenza del segnale di downlink dai satelliti Starlink, il paradigma di ricezione dei terminali utente, la propagazione delle interferenze e l'effetto cumulativo di una moltitudine di jammer che colpiscono lo stesso terminale da diverse angolazioni.

Hanno poi introdotto una griglia di jammer virtuali, che volavano a 20 km (12 miglia) di altitudine, distanziati tra loro di 5 e 9 km, delineando nel cielo una specie di scacchiera. Ogni jammer emetteva rumore a vari livelli di potenza, imitando realistici carichi utili per la guerra elettronica.

Sono state testate antenne a fascio ampio, capaci di coprire aree più vaste maggiore ma di distribuire l'energia in modo sottile, e a fascio stretto, più focalizzate e potenti ma bisognose di orientamento.

Risultato: «*in condizioni ottimali, utilizzando una potente ma costosa sorgente di jamming da 26 decibel-watt (400 watt), un'antenna a fascio stretto e una spaziatura di 7 km, ogni nodo jammer ha soppresso la ricezione Starlink su un'area media di 38,5 km^2».*

Taiwan, però, si estende per circa 36.000 km^2. Ne discende che, per coprire interamente l'isola, *«sarebbero necessari almeno 935 nodi di interferenza coordinati, e questo numero non include la ridondanza in caso di guasti, la compensazione di terreni come le montagne che bloccano i segnali e la capacità di contrastare i futuri aggiornamenti anti-jamming di Starlink».*

Si tratta comunque di risultati da prendere con le dovute cautele, dal momento che Starlink *«ha mantenuto la riservatezza su alcune tecnologie chiave».* Non è attualmente verificabile se Pechino abbia condiviso o meno con Teheran le tecnologie necessarie alla realizzazione del sofisticato piano di oscuramento di Starlink ideato per Taiwan.

Di certo, l'Iran ha tratto ispirazione dal Great Firewall cinese per costruire il National Information Network (NIN).

Si tratta di una rete internet interna parallela a quella globale, basata su piattaforme "alternative" come quelle riconducibili a Huawei, sviluppata a partire dal 2012 in risposta ai devastanti attacchi informatici sferrati dal Mossad e dalla Cia e giunta, dopo oltre un decennio, alla fase operativa.

Il NIN ha posto Teheran nelle condizioni di mantenere regolarmente in attività i servizi di base (banche, canali di informazione statali, ecc.) scollegando allo stesso tempo da internet il resto del Paese.

Nel 2023, il presidente Ebrahim Raisi aveva incaricato il Ministero delle Comunicazioni di aumentare la quota di traffico interno, affinché il 70% circa del traffico internet del Paese venisse assorbito dalla rete nazionale entro i cinque anni successivi, in modo da lasciare soltanto il 30% del traffico utilizzabile per accedere alla rete internet globale.

L'anno precedente, l'ex direttore dell'emittente statale iraniana Abdol-Ali Asgari aveva invocato il potenziamento della rete internet nazionale, citando come esempio la Cina che aveva notevolmente «ridimensionato l'influenza della rete americana» all'interno del Paese.