CENTRO ANALISI E STUDI ITALUS

REPORT

Aprile 2026

WARFARE DATA-DRIVEN: LA NUOVA ARCHITETTURA DEL POTERE

Tra sorveglianza totale e fusione civile-militare: come gli algoritmi stanno ridisegnando i confini della sovranità nazionale.

A CURA di:
Matteo Moschetti
Donatello D'Andrea
Vittorio Iacopini

Abstract

Questo report analizza la metamorfosi del conflitto moderno, in un'epoca in cui il campo di battaglia non è più solo fisico, ma si espande in uno spazio dominato dalla superiorità informativa, dalla sorveglianza totale e dalla fusione definitiva tra mondo civile e militare. Dopo aver delineato il valore vitale del dato come nuovo pilastro della sovranità, l'analisi si immerge nei profili di giganti tecnologici e attori d'ombra — Palantir, Paragon Solutions e l'architettura statale cinese — rivelando come l'intelligenza artificiale, i software di intrusione e le costellazioni satellitari stiano riscrivendo i confini dell'autonomia nazionale. Un focus cruciale è dedicato al potere delle tecnologie esogene, dove i sistemi analitici d'avanguardia e la 'diplomazia della sorveglianza' diventano i nuovi strumenti con cui le grandi potenze plasmano gli equilibri globali e decidono il destino dei Paesi nei teatri di crisi.

Il lavoro esplora la 'geografia del dominio digitale', interpretando le infrastrutture digitali non come semplici strumenti, ma come veri e propri dispositivi di potere: vengono messi a nudo i conflitti per il controllo della crittografia e le silenziose battaglie nello spettro elettromagnetico, dove si gioca la vera partita per il dominio. Il report espone, infine, lo scontro epocale tra il modello d'innovazione occidentale e la dottrina della fusione civile-militare di Pechino, valutando le opportunità e i rischi di una competizione tecnologica che deciderà la stabilità e il futuro della sicurezza globale.

Abstract

This report analyzes the metamorphosis of modern conflict, in an era in which the battlefield is no longer only physical, but expands into a space dominated by information superiority, total surveillance, and the definitive fusion between the civilian and military worlds. After outlining the vital value of data as the new pillar of sovereignty, the analysis dives into the profiles of technological giants and shadow actors — Palantir, Paragon Solutions, and the Chinese state architecture — revealing how artificial intelligence, intrusion software, and satellite constellations are rewriting the boundaries of national autonomy. A crucial focus is dedicated to the power of exogenous technologies, where cutting-edge analytical systems and 'surveillance diplomacy' become the new tools with which great powers shape global balances and decide the fate of countries in crisis theaters.

The work explores the "geography of digital dominance," interpreting digital infrastructures not as simple tools, but as true devices of power: it lays bare the conflicts for the control of encryption and the silent battles in the electromagnetic spectrum, where the true game for dominance is played. Finally, the report exposes the epochal clash between the Western innovation model and Beijing's doctrine of civil-military fusion, evaluating the opportunities and risks of a technological competition that will decide the stability and future of global security.

Key Words: #WarfareDataDriven #GeopoliticaDigitale #CyberSecurity #Palantir #SorveglianzaTotale #IntelligenzaArtificiale #SovranitàDigitale #DifesaModerna #TecnologiaMilitare #SicurezzaGlobale

Indice

Introduzione

Il dominio digitale è oggi uno di quegli spazi in cui la tecnologia e la politica di potenza si fondono, innescando meccanismi di influenza che determinano cambiamenti sostanziali nella sovranità dei Paesi contemporanei. Collocato all'intersezione tra innovazione civile e sicurezza nazionale, l'ecosistema dei dati concentra in poche righe di codice capacità di sorveglianza, interessi economici, vulnerabilità cibernetiche e competizioni strategiche. Gli Stati sono oggi costretti a destreggiarsi in un ambiente dove la protezione delle informazioni e le dipendenze tecnologiche sono altamente instabili e incidono direttamente sulle reali possibilità di difesa.

Negli ultimi anni, la gestione del dato si è trasformata in un vero crocevia strategico: da un lato perché le piattaforme di analisi aumentano il valore delle informazioni come strumento decisionale, dall'altro perché la natura invisibile delle minacce rende fragile qualsiasi equilibrio. In questo contesto, i software e le infrastrutture critiche, più che semplici supporti logistici, diventano zone di pressione e strumenti di controllo, capaci di influenzare la stabilità interna e la sicurezza globale.

A complicare ulteriormente il quadro è il ruolo dei nuovi attori della forza: colossi privati come Palantir, fornitori di strumenti di intrusione come Paragon e la potenza sistemica della Cina agiscono con modalità differenti, ma convergono nel considerare la superiorità informativa l'area decisiva per la propria profondità strategica. Da questo derivano dinamiche d'influenza che si esprimono attraverso algoritmi predittivi, sistemi di spionaggio mirato e architetture satellitari. Parallelamente, l'attenzione delle democrazie occidentali cresce, consapevoli che il controllo sulle tecnologie emergenti ha ricadute dirette sull'autonomia politica nazionale.

Questo report propone una lettura integrata della trasformazione del warfare moderno, con una prospettiva tecnologica e geopolitica. Dopo un inquadramento della rilevanza strategica della "All-Domain Awareness", l'analisi si concentra su tre casi studio cruciali, evidenziando le leve d'influenza e i vincoli che condizionano le scelte degli attori in campo. Si esaminano i nuovi giganti del settore e le modalità di intrusione digitale, fino ad arrivare alla dottrina della fusione civile-militare cinese, interpretata come il nodo centrale per comprendere le sfide alla stabilità internazionale nel XXI secolo.

Capitolo 1 – Palantir Technologies: Il Sistema Operativo della Difesa Occidentale

A cura di Matteo Moschetti

Il concetto di **warfare data-driven** trova in Palantir Technologies la sua massima espressione operativa e dottrinale. Fondata nel 2003 con il supporto di In-Q-Tel (il braccio venture capital della CIA), l'azienda nasce con una missione dichiarata che la distingue nettamente dal resto della Silicon Valley: **fornire alle democrazie liberali e ai loro alleati la superiorità tecnologica necessaria per proteggere le istituzioni occidentali**[1]. La sua **vision** non si limita alla fornitura di strumenti analitici, ma punta a diventare il "sistema operativo" centrale della difesa moderna, trasformando il software da semplice supporto logistico a pilastro della sovranità nazionale.

Attraverso l'integrazione di sistemi avanzati come **Gotham** e l'**Artificial Intelligence Platform (AIP)**, la difesa contemporanea si sposta dal piano della mera potenza di fuoco a quello della superiorità informativa. In questo capitolo si analizza come la trasformazione del dato grezzo in "oggetto ontologico" e l'accelerazione della kill chain abbiano ridefinito gli standard della **All-Domain Awareness**. Palantir emerge così come un partner strategico insostituibile, capace di sincronizzare intelligence e azione cinetica per garantire una capacità di risposta rapida nei teatri di crisi più complessi, dal fronte ucraino alla gestione delle minacce asimmetriche globali.

1.1 Cos'è la "All-Domain Awareness": Gotham

La **All-Domain Awareness** rappresenta l'evoluzione della consapevolezza situazionale: non si tratta più solo di vedere il campo di battaglia, ma di comprenderlo in tempo reale attraverso ogni dimensione (terra, mare, aria, spazio e cyberspazio). Al centro di questa visione si pone **Gotham**, una piattaforma di integrazione dati progettata per trasformare oceani di informazioni frammentate in un'unica verità operativa condivisibile[2]. A differenza dei database tradizionali, Gotham non organizza le informazioni in righe e colonne, ma attraverso un **modello ontologico**[3].[4] Ogni dato proveniente da fonti disparate (satelliti, droni, segnali radio) viene trasformato in "Oggetti" (es. un veicolo, una persona, un'installazione) e "Relazioni" (es. "di proprietà di", "visto vicino a").

- **Normalizzazione semantica:** Il software agisce come un "tessuto connettivo" (**data fabric**[5]) che traduce i linguaggi tecnici di sensori incompatibili tra loro in un linguaggio comune.[6]
- **Ingestione Multi-Sorgente:** Gotham aggrega flussi **SIGINT** (segnali elettronici), **GEOINT** (immagini satellitari e mappe), **MASINT** (firme radar) e **HUMINT**[7] (rapporti di intelligence umana) in un unico ambiente di lavoro.[8]

[1] Moschetti M.; *La macchina che sa tutto di tutti: cos'è davvero Palantir?;* Centro Analisi e Studi Italus – C.A.S.I.*; 2025;* Link.
[2] Palantir Platforms; *Gotham*; Palantir Platforms; 2026; Link.
[3] A differenza dei database tradizionali che leggono i dati come tabelle, un **modello ontologico** mappa i dati come 'oggetti' e 'relazioni' logiche. Questo permette all'IA di capire il contesto: non vede solo 'Veicolo A' e 'Persona B', ma comprende che 'Persona B sta guidando il Veicolo A'.
[4] Palantir Technologies ltd.; *The Ontology system*; Palantir Foundry Documentation; 2026; Link.
[5] In informatica, il **Data Fabric** è un'architettura che facilita l'accesso e la condivisione dei dati in un ambiente eterogeneo, agendo come uno strato unificante che permette a sistemi diversi di 'parlarsi' senza dover riscrivere i database originali.
[6] Strout N.; *Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up*; C4isrnet; 2021;Link.
[7] L'intelligence si divide in discipline basate sulla fonte: **SIGINT** (intercettazione di segnali elettromagnetici), **GEOINT** (analisi di immagini e dati geografici), **MASINT** (identificazione di bersagli tramite firme fisiche come radar o calore) e **HUMINT** (informazioni raccolte da fonti umane dirette).
[8] Palantir Technologies UK, ltd.; *Palantir Platform: Gotham*; Digital Marketplace; 2024; Link.

Il risultato di questa integrazione è la **Common Operational Picture (COP)**, una mappa dinamica che rappresenta la "verità singola" del campo di battaglia. Per gestire l'enorme mole di dati visivi, Gotham integra algoritmi di *Computer Vision* avanzata e, tramite l'impiego di tecnologie sviluppate in programmi come **Project Maven**, il sistema analizza automaticamente migliaia di ore di filmati da droni e costellazioni satellitari. Questo permette di identificare e "taggare" sulla mappa obiettivi nemici in tempo reale, eliminando i colli di bottiglia dell'analisi umana manuale.[9]

Gotham permette, attraverso la **sincronizzazione Terra-Spazio** di assegnare compiti ai sensori direttamente dalla mappa. Un operatore può cliccare su un'area sospetta e il sistema, tramite Application Programming Interface (API), può richiedere un nuovo passaggio satellitare o il reindirizzamento di un drone per confermare l'obiettivo[10].

Palantir è diventata l'infrastruttura software centrale per il concetto di **Joint All-Domain Command and Control (JADC2)** del Pentagono, che mira a connettere ogni sensore a ogni tiratore (*sensor-to-shooter*) in tutte le forze armate. [11]Grazie alla capacità di **Edge Computing**[12], il sistema processa i dati direttamente sui sensori periferici (come i veicoli blindati TITAN), inviando al comando centrale solo le informazioni rilevanti. Questo trasforma la consapevolezza situazionale in un vantaggio decisionale immediato, riducendo i tempi di reazione da ore a minuti. [13]

La differenza tra Project Maven ed Edge Computing è sottile ma sostanziale: mentre l'IA di **Maven** agisce come un "occhio intelligente" che riconosce automaticamente i nemici nelle immagini, l'**Edge Computing** permette a questo occhio di funzionare direttamente sul campo (sui droni o sui mezzi corazzati) senza dover inviare gigabyte di dati a basi lontane, rendendo la risposta militare quasi istantanea.

1.2 Il targeting accelerato: AIP

Se Gotham rappresenta l'occhio che osserva il campo di battaglia, l'**Artificial Intelligence Platform (AIP)** ne costituisce il sistema nervoso decisionale. Lanciata ufficialmente nel 2023, questa piattaforma ha segnato un punto di svolta integrando i Large Language Models (LLM) [14]in un ambiente militare protetto e isolato. L'obiettivo non è sostituire il comandante, ma permettergli di dialogare con la massa di dati operativi usando il linguaggio naturale, abbattendo drasticamente i tempi della cosiddetta *kill chain* (la sequenza che va dall'individuazione dell'obiettivo alla sua neutralizzazione)[15]. L'apporto di AIP nella compressione della *kill chain* a favore di Kiev ha svolto un ruolo cruciale, e ci aiuta davvero a capire come opera il software sviluppato da Palantir.

L'esperienza in Ucraina ha dimostrato che la velocità di reazione è spesso l'unico fattore che separa il successo dal fallimento. In un contesto bellico tradizionale, il processo di targeting è lineare e lento: un satellite scatta una foto, un analista la esamina, il comando valuta la minaccia e infine invia le coordinate all'artiglieria. **Palantir ha trasformato questo ciclo in un processo quasi istantaneo**.[16] Attraverso la "fissione dei dati",

[9] Hitchens T.; *Pentagon's flagship AI effort, Project Maven, moves to NGA*; Breaking Defense; 2022; Link.
[10] Strout N.; *Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up*; C4isrnet; 2021; Link.
[11] Ibidem.
[12] L'**Edge Computing** consiste nell'elaborare i dati il più vicino possibile a dove vengono generati (es. direttamente sul drone) invece di inviarli a un server centrale. Questo riduce il ritardo e permette di operare anche quando le connessioni internet sono deboli o disturbate.
[13] Strout N.; *Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up*; C4isrnet; 2021; Link.
[14] I **LLM** sono algoritmi di intelligenza artificiale (come quello alla base di ChatGPT) addestrati su enormi quantità di testo per comprendere e generare linguaggio naturale. Nel contesto militare, permettono all'operatore di interrogare i dati complessi come se stesse parlando con un assistente umano.
[15] Palantir Technologies ltd.; *AIP for Defense*; Palantir Solutions; 2026; Link.
[16] Glosselin-Malo E.; *Ukraine feeds sensitive military data to Palantir AI for training*; Defense News; 2026; Link.

AIP incrocia in tempo reale le immagini dei droni con le segnalazioni dei civili e i dati satellitari commerciali, come quelli di MetaConstellation[17]. Un operatore può letteralmente "chiedere" al sistema: *"Quali unità nemiche si trovano nel raggio di 10km da questo punto?"* oppure *"Suggerisci tre opzioni per neutralizzare questo mortaio nemico minimizzando i danni collaterali"*; in questo modo AIP genera piani d'attacco basandosi su modelli logistici e tattici in tempo reale.

L'Ucraina quindi non rappresenta solo un utente, ma si trasforma in un vero e proprio laboratorio di addestramento per l'IA. Attraverso la partnership **Brave1**, il governo ucraino e Palantir hanno creato un "Dataroom" sicuro dove i dati reali del conflitto vengono usati per allenare nuovi algoritmi. [18]Questa simbiosi tecnica sta spingendo l'IA verso nuove frontiere, come lo sviluppo di droni capaci di navigare e riconoscere obiettivi in totale autonomia, superando gli ostacoli della guerra elettronica russa che spesso oscura i segnali GPS[19]. Ogni scontro diventa così una lezione per il software, creando un ciclo di apprendimento continuo che ridefinisce costantemente la dottrina della guerra digitale.

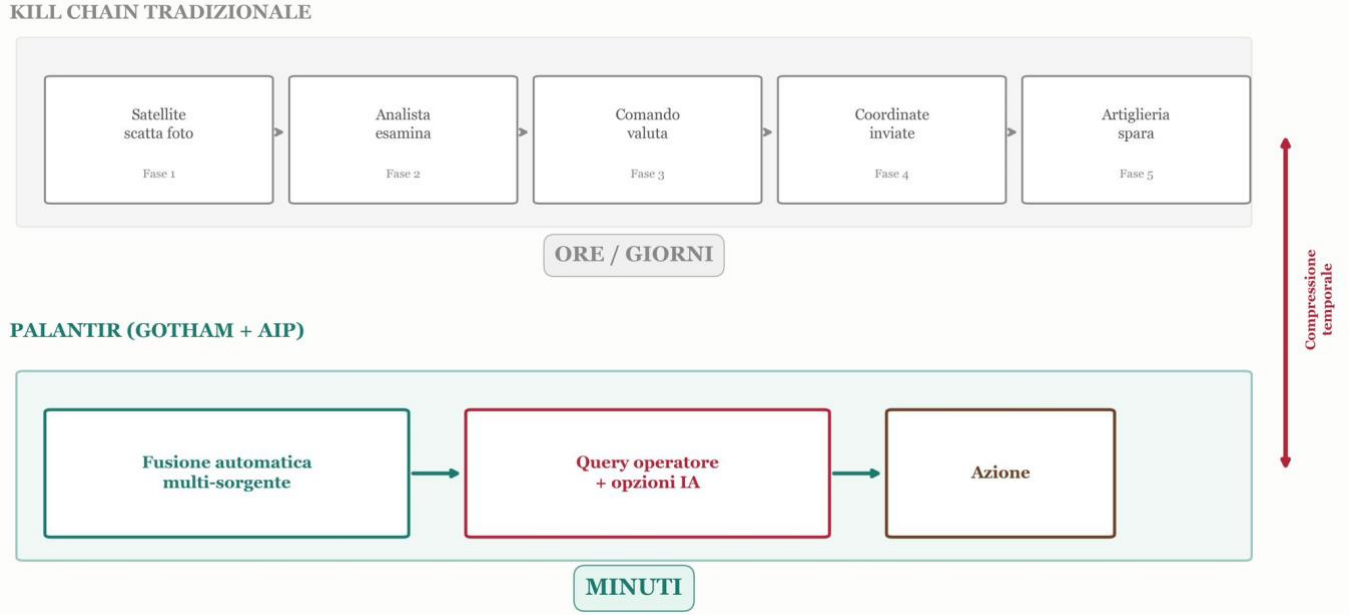

Figura 1. Confronto esplicativo-illustrativo della kill chain tradizionale e Palantir.

Fonte: elaborazione dell'autore.

Tuttavia, l'impatto di **AIP non si limita alla fase cinetica dell'attacco**. La capacità dell'IA di processare variabili infinite viene sfruttata per **compiti strategici** di vitale importanza, come la gestione dei colli di bottiglia logistici in territori contesi, assicurando che i rifornimenti arrivino dove il sistema prevede che avverrà il prossimo scontro. Un esempio significativo è la collaborazione con il Ministero dell'Economia ucraino per lo sminamento del territorio: AIP analizza dati geografici, storici ed economici per dare priorità alle aree che, una volta bonificate, possono garantire la più rapida ripresa agricola ed economica del paese, trasformando uno strumento di guerra in un motore di ricostruzione.[20]

1.3 Sovranità e dipendenza

L'ascesa di Palantir come pilastro tecnologico della difesa moderna ha innescato un dibattito profondo che va oltre la semplice efficienza del software: la questione della sovranità nazionale. Quando uno Stato affida la gestione dei propri segreti militari e dei dati sensibili a una piattaforma privata, il confine tra "fornitore di

[17] Kosoy D.; *Palantir, the Secretive Tech Giant Shaping Ukraine's War Effort*; United 24 Media; 2025; Link.
[18] Kosoy D.; *Palantir, the Secretive Tech Giant Shaping Ukraine's War Effort*; United 24 Media; 2025; Link.
[19] Mosley L.; *Ukraine at "bleeding edge" of military tech, says Palantir executive*; Bloomberg Technology; 2025; Link.
[20] Jaura R.; *"Software on the Front Line": How Palantir Is Aiding Ukraine in Its War with Russia*; InDeptNews; 2025; Link.

servizi" e "partner strategico indispensabile" svanisce. Questo solleva interrogativi critici su quanto potere un governo sia disposto a cedere in cambio di una superiorità tecnologica che non possiede internamente.

Uno dei timori più sentiti dai governi, specialmente in Europa, è il rischio di rimanere intrappolati in un ecosistema chiuso, il cosiddetto *vendor lock-in*.[21] [22]Una volta che l'intera infrastruttura di intelligence di un Paese viene costruita sull'architettura e sull'ontologia di Palantir, cambiare fornitore diventa un'impresa titanica, quasi impossibile. Sebbene Palantir dichiari esplicitamente che i dati appartengono al cliente e che l'azienda fornisce solo i "tubi" per farli scorrere, la realtà tecnica è più complessa: la capacità di leggere, interpretare e dare un senso a quei dati dipende interamente dal codice proprietario dell'azienda. Si crea così una forma di dipendenza strutturale in cui lo Stato, pur essendo proprietario delle informazioni, non può operare senza le chiavi fornite da un ente privato. Inoltre, a differenza dei vecchi contratti di difesa dove si acquistava un mezzo fisico, qui si parla di abbonamenti (Software as a Service): se la licenza scade o il rapporto si incrina, la capacità operativa di un esercito potrebbe teoricamente essere compromessa da una decisione commerciale.[23]

A differenza della Silicon Valley tradizionale, che spesso ha cercato di mantenere una neutralità di facciata (si pensi ai dipendenti di Google che protestarono contro la collaborazione con il Pentagono), Palantir ha fatto del suo posizionamento ideologico una bandiera. Il CEO Alex Karp ha dichiarato apertamente che l'azienda "sceglie da che parte stare"[24], ovvero quella delle democrazie occidentali e dei loro alleati. Questa trasparenza, se da un lato rassicura i partner della NATO, dall'altro trasforma Palantir in un attore politico globale. Un'azienda che può decidere a chi fornire, o a chi negare, la capacità di vedere il campo di battaglia in tempo reale, possiede un'influenza che solitamente appartiene solo ai governi. Il dibattito sulla sovranità si estende anche all'uso civile: nel Regno Unito, l'accordo per gestire i dati del servizio sanitario nazionale (NHS) ha scatenato accese proteste sulla privacy, poiché molti cittadini temono che una tecnologia nata per scopi bellici possa essere applicata in modo opaco sulla vita quotidiana, senza un controllo pubblico trasparente sugli algoritmi.[25]

1.4 L'impatto tattico e strategico: la guerra della previsione e della logistica

L'analisi predittiva sta trasformando la condotta bellica da un esercizio di reazione a una sfida di gestione proattiva. Non si tratta di avere una "sfera di cristallo", ma di utilizzare la potenza di calcolo per identificare schemi invisibili all'occhio umano, cambiando radicalmente il modo in cui i comandi pensano alla logistica e alla prevenzione delle minacce.

Storicamente, le guerre si vincono o si perdono sulle linee di rifornimento. Palantir ha applicato i modelli analitici già testati nel mondo civile (con colossi come Airbus) al contesto del combattimento. [26]Attraverso il software, la logistica smette di essere un semplice inventario e diventa un sistema predittivo dinamico. Il sistema analizza costantemente variabili come l'usura dei componenti dei carri armati, il consumo di carburante e la percorribilità delle strade. In Ucraina, questo ha permesso di prevedere le necessità di un'unità prima ancora che i soldati lanciassero l'allarme, ottimizzando le catene di distribuzione in territori costantemente sotto il fuoco. La logistica diventa così un vantaggio tattico: chi sa dove e quando mancherà un pezzo di ricambio può mantenere la pressione sul nemico senza interruzioni. [27]

[21] Il **Vendor Lock-in** è una situazione di dipendenza in cui un cliente non può passare a un altro fornitore senza sostenere costi di transizione proibitivi o perdere l'accesso ai propri flussi di lavoro, diventando di fatto ostaggio tecnologico del fornitore iniziale.
[22] Booth R.; *MPs urge UK government to halt contract giving Palantir FCA data access*; The Guardian; 2026;Link.
[23] Shone E.; *The great Ministry of Defence-to-Palantir pipeline* ;Progressive International; 2026;Link
[24] Bienvenue E., Kelton M., Rogers Z., Sullivan M., Ford M.; *Private Tech Companies, the State, and the New Character of War*; Carnegie Endowment; 2025; Link.
[25] Booth R.; *NHS deal with AI firm Palantir called into question after officials' concerns revealed*; The Guardian; 2026; Link;
[26] Gordon L.; *Palantir and Airbus Extend Strategic Collaboration*; Business Wire; 2026; Link;
[27] Palantir Technologies ltd.; *Palantir Supply Chain Solutions*; Palantir Solutions; 2026; Link.

L'impatto strategico più profondo risiede nella capacità di prevenire le imboscate attraverso l'analisi dei segnali deboli[28]. Gotham e AIP sono in grado di incrociare anni di dati storici con i movimenti attuali per identificare anomalie che precedono un attacco. [29]Se un sensore rileva un insolito movimento di truppe e, contemporaneamente, si registra una variazione nei prezzi dei mercati locali o un silenzio radio sospetto, il sistema lancia un'allerta su un'imminente offensiva.[30] A livello tattico, i soldati possono visualizzare sui propri tablet le aree a più alto rischio di ordigni improvvisati (**IED**), basandosi sulla "memoria" del software che mappa ogni incidente passato e ogni caratteristica del terreno favorevole a un'imboscata. Questa capacità di "mappare il rischio" trasforma ogni movimento in una decisione basata sui dati, riducendo drasticamente le perdite umane.

A livello di alto comando, Palantir permette di eseguire "giochi di guerra" digitali in tempo reale. I generali possono simulare migliaia di scenari, come l'impatto della distruzione di un ponte o di tre giorni di pioggia incessante, ricevendo stime probabilistiche sui risultati di un'operazione. In questo scenario, il baricentro della strategia si sposta dalla forza bruta all'efficienza informativa: il vantaggio non appartiene più necessariamente a chi ha il cannone più grande, ma a chi possiede l'algoritmo capace di elaborare la realtà più velocemente dell'avversario. [31]

1.5 Applicazione pratica sul campo: Il "miracolo" di Kharkiv e la guerra algoritmica

Per capire se queste tecnologie funzionino davvero, non bisogna guardare i manuali, ma i fatti del settembre 2022. Durante la controffensiva ucraina nelle regioni di Kharkiv e Kherson, il mondo ha assistito a una velocità di manovra che ha spiazzato l'intelligence russa. In questo contesto, Palantir non è stato un semplice fornitore, ma il cuore di quello che gli analisti definiscono ora "Guerra Algoritmica".[32]

In quelle settimane, l'esercito ucraino si trovava in inferiorità numerica di uomini e mezzi. La chiave del successo è stata la capacità di colpire esattamente dove il nemico era più fragile, un risultato ottenuto grazie all'integrazione di dati in Gotham. Il software ha permesso di incrociare istantaneamente le immagini dei satelliti commerciali (come Maxar e Planet) con i segnali intercettati dai droni e le segnalazioni dei partigiani sul territorio tramite bot di messaggistica. Questo mosaico informativo ha rivelato che la linea difensiva russa a Kharkiv era una "crosta" sottile: dietro le prime linee non c'erano riserve pronte. Gli ucraini, vedendo questa vulnerabilità sulla loro mappa digitale, hanno concentrato la forza in un unico punto di rottura, provocando il collasso dell'intero fronte nemico in pochi giorni. [33]

Un ulteriore esempio pratico e documentato riguarda l'efficacia del "ciclo di fuoco". Prima dell'arrivo di queste piattaforme, confermare la posizione di un quartier generale nemico nascosto e dare l'ordine di tiro poteva richiedere ore. In Ucraina, grazie ad AIP e alla connessione satellitare Starlink, gli operatori hanno ridotto questo tempo a meno di 10 minuti. Durante la ritirata russa da Kherson, il sistema ha permesso di tracciare i movimenti dei convogli russi che tentavano di attraversare il fiume Dnipro. Non appena l'IA identificava un raggruppamento di mezzi ai traghetti, le coordinate venivano inviate automaticamente alle unità HIMARS. Il risultato non è stato solo la distruzione di mezzi, ma la paralisi psicologica del nemico, consapevole di essere osservato e puntato in ogni istante da un occhio invisibile e infallibile. [34]

[28] In ambito di intelligence, i **segnali deboli** sono frammenti di informazioni apparentemente insignificanti o scollegati che, se analizzati collettivamente da un algoritmo, possono rivelare l'imminenza di un evento critico o un cambiamento di strategia nemica.
[29] Horowitz M. C.; *Artificial Intelligence and the Future of Strategic Stability*; Texas National Security Review; 2026; Link.
[30] Bergengruen V.; *How Tech Giants Turned Ukraine Into an AI War Lab*; Time Magazine; 2024; Link.
[31] Palantir Technologies ltd.; *AIP for Defense*; Palantir Solutions; 2026; Link.
[32] Bergengruen V.; *How Tech Giants Turned Ukraine Into an AI War Lab*; Time Magazine; 2024; Link.
[33] Ignatius D.; *How the algorithm tipped the balance in Ukraine*; The Washington Post; 2022; Link.
[34] Jaura R.; *Come Palantir sta aiutando l'Ucraina nella sua guerra con la Russia*; L'Indro; 2025; Link.

L'applicazione pratica continua anche oggi, lontano dai colpi di cannone. Il governo ucraino utilizza Palantir per gestire la logistica degli aiuti umanitari e, soprattutto, per il "Digital Demining". L'IA analizza i dati storici dei combattimenti per prevedere dove sia più probabile la presenza di mine antiuomo, permettendo alle squadre di bonifica di lavorare con priorità scientifica, riaprendo strade e campi agricoli che altrimenti rimarrebbero abbandonati per decenni.[35]

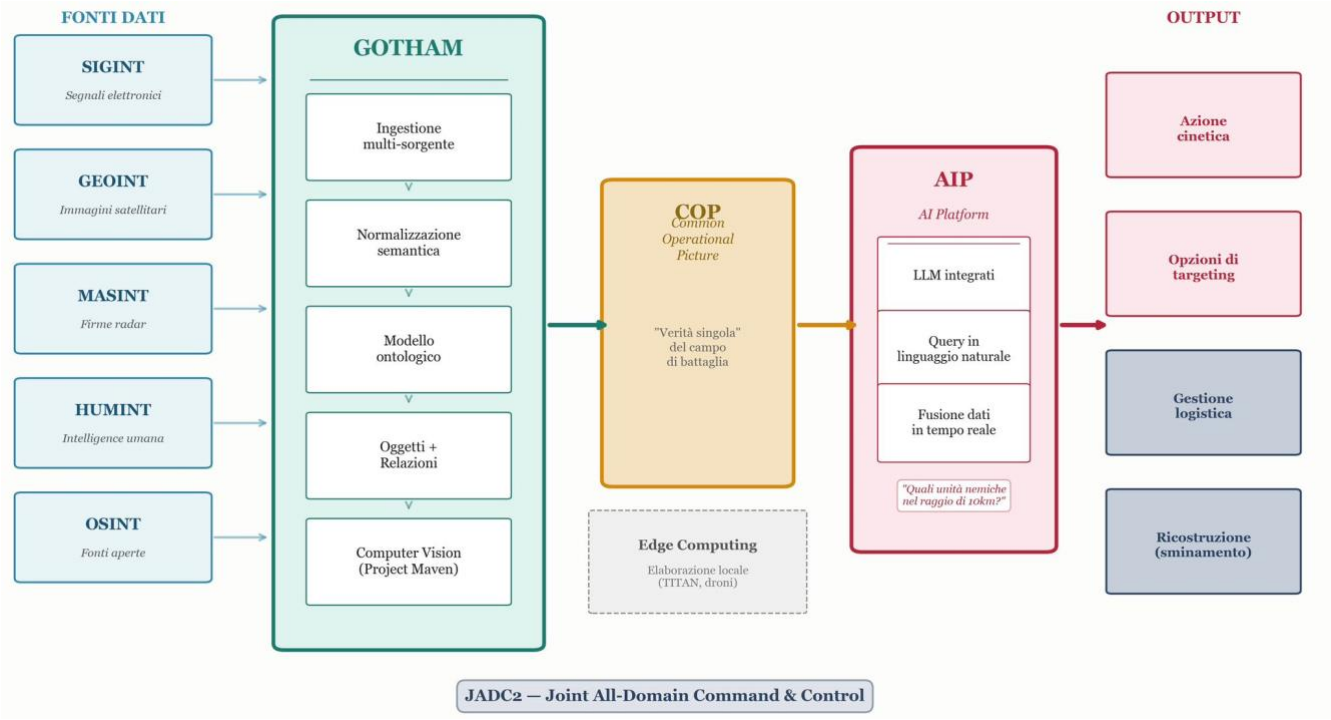

Figura 2. Come si muove Palantir: dalle fonti di dati all'output.

Fonte: elaborazione dell'autore

[35] Jaura R.; *Come Palantir sta aiutando l'Ucraina nella sua guerra con la Russia*; L'Indro; 2025; Link.

Capitolo 2 – I sistemi di intrusione nella sicurezza nazionale: il caso Paragon

A cura di Donatello D'andrea

La digitalizzazione delle comunicazioni ha profondamente ridefinito il contesto operativo di riferimento per la sicurezza nazionale. La diffusione capillare di dispositivi mobili e servizi cloud, e di piattaforme di messaggistica cifrata, ha reso sempre più robusta la tutela delle comunicazioni e al contempo introdotto nuove sfide per l'esercizio delle attività di intelligence e del contrasto alle minacce. Organizzazioni terroristiche, reti criminali transnazionali e Stati ostili utilizzano infatti infrastrutture digitalizzate di grande complessità e basate su protocolli di **crittografia end-to-end** che rendono sempre più difficile l'intercettazione delle comunicazioni.

In questo nuovo scenario di riferimento è emersa una nuova categoria di strumenti tecnologici: il **software di intrusione mirata**, sviluppato appositamente per ottenere l'accesso al dispositivo del soggetto investigato aggirando il sistema di crittografia e di cifratura delle informazioni tramite l'infiltrazione del terminale del dispositivo utilizzato. Queste tecnologie sono spesso sviluppate da aziende private a stretto contatto con il settore difesa/intelligence e rappresentano oggi una delle capacità più evolute a disposizione degli Stati per la raccolta di informazioni nel dominio digitale e per il contrasto di attività ostili prima che si traducano in azioni concrete.

Il caso di **Paragon Solutions**, società israeliana fondata nel 2019 e produttrice dello spyware **Graphite**, può essere considerato un esempio altamente emblematico di questa tendenza. L'analisi della società pone dunque al crocevia tra la sicurezza nazionale, la cyber-intelligence, e la geopolitica delle nuove tecnologie. È dunque importante analizzare, al di là del funzionamento di questa tecnologia di sorveglianza, i fenomeni più generali che possono definire il mercato globale degli spyware commerciali, che sono strettamente correlati al potere di Stato.

Il presente capitolo analizzerà il ruolo dei sistemi di intrusione nella sicurezza nazionale e nella lotta contro le minacce ibride attraverso cinque differenti prospettive complementari. Innanzitutto, valuterà come queste nuove tecnologie permettano alle agenzie di intelligence di accedere alle comunicazioni protette nell'era della criptografia diffusa. In secondo luogo, analizzerà l'uso di queste nuove tecnologie per le operazioni di sicurezza e antiterrorismo. Successivamente, verranno analizzate la geopolitica della **diplomazia della sorveglianza**, con particolare attenzione al modello israeliano di esportazione delle nuove tecnologie cyber. Infine, verranno discussi i rischi strategici connessi al fenomeno degli spyware commerciali, per terminare con un caso applicativo che ci consenta di comprendere concretamente come funziona questa nuova tecnologia di sorveglianza.

2.1 Oltre la crittografia: le capacità di accesso ai dispositivi mobili e alle comunicazioni protette per scopi di intelligence

Nel corso degli ultimi due decenni, il continuo evolversi delle tecnologie di comunicazione digitale ha profondamente trasformato il contesto operativo dell'intelligence e della sicurezza nazionale. La diffusione capillare delle piattaforme di messaggistica criptata, dei servizi di cloud storage e delle applicazioni mobili ha modificato radicalmente il modo in cui individui, organizzazioni e istituzioni comunicano, condividono informazioni e coordinano attività complesse.

In particolare, molte delle principali piattaforme di comunicazione contemporanee - tra cui Signal, WhatsApp e Telegram[36] - utilizzano protocolli di **crittografia end-to-end**, progettati per impedire a terze parti di accedere

[36] Marczak, Bill; Scott-Railton, John; *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*; Citizen Lab Report No. 186, University of Toronto; 2025.

al contenuto delle comunicazioni. In questi sistemi, il messaggio viene cifrato direttamente sul dispositivo del mittente e può essere decifrato esclusivamente dal dispositivo del destinatario. Nemmeno i fornitori del servizio sono tecnicamente in grado di leggere il contenuto delle conversazioni che transitano sulle proprie infrastrutture.

Questa evoluzione tecnologica ha rappresentato un importante progresso nella tutela della privacy e nella sicurezza delle comunicazioni digitali. Tuttavia, dal punto di vista delle autorità incaricate della sicurezza nazionale, essa ha introdotto nuove e significative complessità investigative. Organizzazioni terroristiche, gruppi criminali transnazionali e soggetti statali ostili hanno progressivamente iniziato a sfruttare queste tecnologie per coordinare attività clandestine con un livello di protezione molto più elevato rispetto al passato.

La diffusione sempre più ampia della crittografia è quindi diventata uno dei fattori centrali del cosiddetto **"going dark problem"**, ossia la progressiva perdita di capacità da parte delle agenzie investigative di accedere alle comunicazioni digitali utilizzate da soggetti sospettati di attività criminali o terroristiche.[2] Questo fenomeno ha spinto numerosi Stati a investire nello sviluppo di strumenti tecnologici in grado di aggirare i sistemi di cifratura senza compromettere direttamente l'architettura crittografica delle piattaforme di comunicazione.

In questo contesto si colloca l'emergere della **tecnologia di intrusione informatica mirata**, concepita per consentire alle agenzie di intelligence e alle forze di sicurezza di accedere direttamente al dispositivo utilizzato dall'individuo oggetto di sorveglianza. Piuttosto che tentare di violare la crittografia delle comunicazioni, questi strumenti agiscono a livello del dispositivo stesso, permettendo di acquisire le informazioni prima che vengano cifrate o dopo che sono state decifrate dal terminale dell'utente.

Tra gli attori che operano nello sviluppo di tali tecnologie vi sono aziende specializzate nel settore della cyber-intelligence commerciale, tra cui **Paragon Solutions**, fondata in Israele nel 2019 da ex membri dell'Unità 8200 delle Forze di Difesa Israeliane. Quest'ultima rappresenta la principale struttura di cyber intelligence militare israeliana ed è considerata una delle unità più avanzate al mondo nel campo della **signals intelligence (SIGINT)**, ossia l'intercettazione, l'analisi e la decodifica di segnali elettronici e comunicazioni digitali.

L'Unità 8200 svolge un ruolo centrale nel sistema di sicurezza nazionale israeliano. Le sue attività comprendono operazioni di **cyber warfare**, sia offensive sia difensive, la decifrazione di codici e sistemi crittografici complessi, nonché il monitoraggio continuo delle comunicazioni digitali nelle aree di interesse strategico per la sicurezza israeliana, in particolare nei paesi limitrofi e nei territori palestinesi. Nel corso degli anni, diverse fonti internazionali hanno attribuito all'unità un ruolo significativo nello sviluppo di alcune delle operazioni cyber più sofisticate mai realizzate.

Tra queste viene spesso citato il caso del malware **Stuxnet**[37], utilizzato tra il 2005 e il 2010 per sabotare le centrifughe nucleari dell'impianto iraniano di Natanz, in un'operazione generalmente ritenuta frutto della cooperazione tra Stati Uniti e Israele. Più recentemente, alcune analisi di sicurezza hanno indicato un possibile coinvolgimento dell'unità anche nella pianificazione tecnica di operazioni di sabotaggio mirate contro infrastrutture di comunicazione utilizzate da organizzazioni armate nella regione mediorientale.

Oltre al ruolo operativo nel campo dell'intelligence e della guerra cibernetica, l'Unità 8200 ha avuto un impatto significativo anche sullo sviluppo dell'ecosistema tecnologico israeliano. Numerosi ex membri dell'unità hanno infatti fondato alcune delle più importanti aziende israeliane nel settore della tecnologia e della cybersicurezza. Tra queste figurano società come **Check Point**[38], una delle principali aziende mondiali nel campo della sicurezza informatica, ma anche piattaforme digitali globali come **Waze** e **Wix**.

[37] Lo Prete, Davide; Sposini, Alessia; "Stuxnet e oltre: la guerra "invisibile" tra Iran, Israele e Stati Uniti"; *Geopolitica.info*; 2021. Link.

[38] L'azienda è stata pioniera nella commercializzazione di sistemi di sicurezza perimetrale capaci di operare un'**analisi contestuale del traffico**. A differenza dei sistemi precedenti, il *FireWall-1* di Check Point era in grado di monitorare lo **stato delle connessioni attive**, validando i dati in transito sulla base della sessione di comunicazione.

Per questo motivo l'Unità 8200 viene spesso descritta come una sorta di **"Silicon Valley militare"**, un ambiente altamente selettivo in cui giovani talenti con elevate competenze matematiche, informatiche e ingegneristiche vengono formati attraverso attività operative complesse e altamente innovative. Il modello di lavoro dell'unità, basato su piccoli team autonomi e sulla risoluzione creativa di problemi tecnologici complessi, ha contribuito a generare un ecosistema imprenditoriale dinamico che continua a influenzare in modo significativo il settore della cybersecurity globale.

Dal punto di vista organizzativo, l'unità seleziona i propri membri tra i giovani più promettenti del sistema educativo israeliano, spesso tra i 18 e i 21 anni, sulla base di avanzate capacità analitiche e informatiche. Le stime disponibili indicano che l'Unità 8200 potrebbe contare tra i **5.000 e i 10.000 effettivi**, rappresentando una quota significativa del personale complessivo dell'Aman.

In questo quadro, la nascita di aziende come Paragon Solutions rappresenta un'evoluzione quasi naturale del modello israeliano di innovazione tecnologica legata alla sicurezza nazionale. Le competenze sviluppate all'interno delle unità di intelligence militare vengono infatti trasferite nel settore privato, dando origine a un ecosistema industriale altamente specializzato nello sviluppo di strumenti avanzati di sorveglianza digitale e cyber intelligence.

L'utilizzo di tecnologie di intrusione informatica mirata implica una trasformazione profonda del paradigma dell'intelligence digitale. Lo smartphone, ad esempio, non costituisce più soltanto un mezzo di comunicazione, ma una vera e propria piattaforma di acquisizione informativa. I dispositivi mobili contengono infatti una quantità estremamente ampia di dati: informazioni di geolocalizzazione, cronologie di comunicazione, contatti personali, file multimediali e accesso a numerose applicazioni utilizzate quotidianamente dall'individuo.

Per le agenzie di sicurezza, la possibilità di accedere a queste informazioni consente non soltanto di intercettare le comunicazioni di un determinato individuo, ma anche di ricostruire la struttura delle **reti sociali, logistiche e operative** di cui esso fa parte. In questo senso, l'intelligence digitale contemporanea non si limita più alla raccolta di singole informazioni, ma mira a mappare interi ecosistemi relazionali e infrastrutture organizzative.

Dal punto di vista delle politiche di sicurezza, il ricorso a strumenti di intrusione informatica mirata rappresenta quindi una risposta tecnologica alla crescente complessità dell'ambiente digitale contemporaneo. Allo stesso tempo, queste tecnologie sollevano interrogativi significativi dal punto di vista giuridico e politico, in particolare per quanto riguarda il delicato equilibrio tra sicurezza nazionale, tutela della privacy e controllo democratico delle attività di sorveglianza.

Il dibattito su questi temi è particolarmente intenso nei paesi democratici, dove l'impiego di strumenti di intrusione digitale è generalmente soggetto a **autorizzazioni giudiziarie e meccanismi di supervisione istituzionale**. In assenza di tali strumenti di controllo, il rischio è che tecnologie sviluppate per il contrasto al terrorismo o alla criminalità organizzata possano essere utilizzate anche per finalità di sorveglianza politica o repressione del dissenso.

2.2 Il ruolo nelle operazioni speciali: l'utilizzo di software di spionaggio mirato per neutralizzare reti terroristiche o attori ostili prima dell'azione fisica

Oltre a questi aspetti investigativi, i sistemi di intrusioni informatiche rivestono sempre più rilevanza per i **compiti di sicurezza preventiva** svolti da agenzie di intelligence e da specializzati reparti delle forze armate.

In questo contesto, infatti, gran parte delle principali minacce alla sicurezza nazionale presenta una **struttura reticolare e transnazionale**. Organizzazioni terroristiche, gruppi di cybercriminalità, reti di traffico illegale, ecc., agiscono attraverso infrastrutture digitali diffuse e impiegano piattaforme di comunicazione criptate per coordinare attività transnazionali. In questo scenario, la possibilità di accedere ai dispositivi digitali dei singoli

individui sospettati consente alle autorità di **prevedere i propositi dei gruppi bersaglio**, raccogliendo informazioni fondamentali sulle intenzioni operative dei gruppi terroristici.

Le informazioni raccolte attraverso l'uso dei mezzi di intrusione digitale possono avere impieghi per diversi scopi operativi. In primo luogo, esse consentono di individuare ulteriori membri delle reti e la struttura organizzativa dei gruppi oggetto d'indagine. In secondo luogo, esse consentono di sorvegliare la preparazione delle attività ostili, fornendo alle autorità il tempo necessario per intervenire prima che queste attività si traducano in attacchi concreti.

In questo modo, i sistemi di sorveglianza digitale diventano componenti imprescindibili di un modello operativo fondato sulla **prevenzione delle minacce**, piuttosto che sulla reazione rispetto a fatti accaduti. Si tratta, infatti, di un modello che si inserisce in una trasformazione più ampia nella gestione delle minacce alla sicurezza nazionale, in cui l'obiettivo prioritario non è più individuare i responsabili, ma **impedire che l'attacco avvenga**.

L'impiego di tali operazioni di intelligence, che si fondano sull'impiego di strumenti di *intrusion digitale*[39], può essere integrato con altre modalità di raccolta di informazioni, come ad esempio la sorveglianza fisica, l'intercettazione tradizionale e l'analisi dei dati. Ciò consente alle agenzie di sicurezza di costruire una comprensione più completa dei network ostili e dei loro modelli d'operatività.

Nel quadro dell'impiego di operazioni antiterrorismo, l'accesso a dispositivi digitali dei sospetti può rivelarsi particolarmente efficace nel rilevare piani d'attacco, **cellule dormienti**, contatti esterni e fonti di finanziamento di organizzazioni clandestine. In diversi casi investigativi, la ricostruzione dell'interazione comunicativa digitale è stata in grado di far emergere i piani d'operatività in via di progettazione, consentendo alle forze dell'ordine di intervenire prima che tali piani d'operatività potessero essere portati a termine.

In sostanza, le tecnologie sviluppate dalla Paragon si collocherebbero **all'intersezione tra cyber intelligence e operazioni di sicurezza**, fornendo gli Stati strumenti in grado di accelerare i tempi di risposta, ovvero i tempi intercorrenti tra la raccolta delle informazioni e l'azione operativa. Tale accelerazione del ciclo informazione-decisione rappresenta uno degli elementi centrali delle moderne strategie di sicurezza nazionale.

2.3 Diplomazia della sorveglianza: come l'export di tecnologie cyber (modello Israele) influenza i rapporti di forza tra Paesi alleati e rivali

Al di là degli aspetti tecnologici e funzionali, i moderni sistemi di intrusione informatica sono emersi anche come strumenti di influenza geopolitica. Negli ultimi due decenni Israele è riuscito a costruire un sistema particolarmente sofisticato nello sviluppo e nell'applicazione di capacità avanzate di cybersecurity e cyber intelligence. All'interno di questo sistema, il coinvolgimento di attori privati è spesso caratterizzato da un elevato grado di continuità con l'apparato di sicurezza nazionale. Tale modello si basa sulla valorizzazione di competenze maturate nel sistema militare e di intelligence cibernetica, in particolare all'interno delle unità d'élite delle Forze di Difesa israeliane, come la **Unità 8200**, una struttura che svolge funzioni paragonabili a quelle della National Security Agency statunitense per quanto riguarda la raccolta e l'analisi delle informazioni digitali.[40]

La nascita e lo sviluppo di questo ecosistema non possono essere compresi senza considerare il contesto strategico in cui Israele opera. Lo Stato israeliano si trova infatti in una condizione geopolitica peculiare: è l'unica democrazia liberale stabile nel Medio Oriente e, sin dalla sua fondazione, ha dovuto confrontarsi con un ambiente regionale caratterizzato da conflittualità persistente, minacce militari e attività di gruppi armati

[39] Morano, Caterina Patrizia; *Cybersecurity, intrusion, detection systems e intelligenza artificiale*; Il mondo dell'Intelligence, Sistema di Informazione per la sicurezza della Repubblica; 2015. Link.
[40] Johnson, Craig; *Unit 8200: Producing Top Cybersecurity Talent*; Diary of a Cyber Headhunter, Substack; 2024. Link.

ostili. A ciò si aggiungono le tensioni con attori statali come **l'Iran**, che negli ultimi anni ha investito in modo crescente nelle capacità di guerra ibrida e cyber, e la presenza di organizzazioni armate non statali, tra cui gruppi palestinesi attivi (Hamas, su tutti) e organizzazioni come Hezbollah, che hanno dimostrato una crescente capacità di utilizzare strumenti tecnologici e digitali nelle proprie attività operative.

In questo quadro, lo sviluppo di capacità avanzate nel campo della cybersecurity e dell'intelligence digitale è diventato per Israele non solo un'opzione tecnologica, ma una **necessità strategica**. La dimensione cyber rappresenta infatti uno dei pochi domini nei quali uno Stato relativamente piccolo può compensare gli svantaggi strutturali derivanti dalla propria profondità strategica limitata e dalla pressione esercitata da attori ostili nel proprio vicinato. Investire nella superiorità tecnologica e nella capacità di penetrare reti digitali avversarie significa, in altre parole, acquisire uno strumento fondamentale per anticipare minacce, raccogliere informazioni e mantenere un vantaggio operativo rispetto ai propri rivali.

Proprio all'interno di questo contesto si è sviluppato il cosiddetto **modello israeliano della cybersecurity**[41], caratterizzato da una stretta integrazione tra apparato statale, settore militare e industria privata. Molti degli imprenditori e degli ingegneri che oggi guidano aziende leader nel campo della cyber-intelligence provengono direttamente dalle unità tecnologiche delle forze armate israeliane, dove hanno maturato esperienza nello sviluppo di strumenti avanzati di intrusione, analisi dei dati e guerra informatica. Una volta concluso il servizio militare, queste competenze vengono trasferite nel settore privato, dando vita a un ecosistema imprenditoriale altamente specializzato che continua tuttavia a mantenere rapporti stretti con le istituzioni di sicurezza nazionale.

Il caso di **Paragon** può essere interpretato come un esempio particolarmente significativo del cosiddetto *modello israeliano* nel settore della sicurezza tecnologica. La società è stata fin dall'inizio associata a figure di primo piano provenienti dall'apparato militare, dall'intelligence e dalla leadership politica del Paese, tra cui l'ex Primo ministro **Ehud Barak** e l'ex comandante dell'Unità 8200 **Ehud Schneorson**. Questa composizione riflette una caratteristica strutturale dell'ecosistema israeliano della cybersecurity: la presenza di un legame diretto e relativamente lineare tra il sistema di sicurezza nazionale, le élite politico-strategiche e il settore tecnologico privato.

In Israele, infatti, le competenze sviluppate all'interno delle unità di intelligence militare non rimangono confinate alla dimensione operativa dello Stato, ma tendono a trasformarsi rapidamente in capitale tecnologico e imprenditoriale. Ex ufficiali e specialisti delle unità cyber delle Forze di Difesa israeliane - in particolare della **Unità 8200** - entrano frequentemente nel settore privato dopo il servizio militare, portando con sé conoscenze tecniche, reti professionali e una visione strategica maturata all'interno dell'apparato di sicurezza nazionale. Questo processo genera una continuità molto forte tra **ricerca militare, innovazione tecnologica e sviluppo industriale**.

In questo senso, aziende come Paragon non rappresentano semplicemente iniziative imprenditoriali nel settore della cybersicurezza, ma si collocano all'interno di un ecosistema più ampio in cui **tecnologia, intelligence e politica** risultano profondamente interconnesse. La presenza di figure politiche e militari di alto livello nella governance o nell'ambiente strategico di queste imprese testimonia il modo in cui lo Stato israeliano ha costruito, nel corso degli anni, un sistema in cui la sicurezza nazionale e lo sviluppo tecnologico procedono spesso in modo parallelo e complementare.

La dimensione commerciale del prodotto assume quindi anche un marcato contenuto politico. Mentre aziende come **NSO Group** sono state coinvolte in scandali internazionali legati all'utilizzo dei loro strumenti da parte di regimi autoritari, Paragon ha costruito una parte significativa della propria legittimità pubblica attraverso una strategia comunicativa volta a differenziarsi esplicitamente da questo modello. La società ha più volte sostenuto di vendere i propri sistemi esclusivamente a governi democratici che rispettano le "norme

[41] Sharma, Rohit; *Cybersecurity in Israel*; 2025. DOI: 10.1007/978-981-16-2717-0_115-1.

internazionali" e i "diritti fondamentali", presentando così i propri prodotti come strumenti compatibili con l'architettura di valori del mondo occidentale.

All'interno di questa narrazione, Paragon ha introdotto anche una formula particolarmente significativa dal punto di vista comunicativo: quella della distribuzione etica dello spyware a favore delle cosiddette **"democrazie illuminate"**. Secondo la società, l'accesso ai propri strumenti sarebbe limitato a un gruppo ristretto di **39 Paesi selezionati**, individuati sulla base di criteri politici e istituzionali legati al rispetto dello stato di diritto e alla cooperazione internazionale in materia di sicurezza. Attraverso questa retorica selettiva, l'azienda non si limita a descrivere il proprio modello di business, ma costruisce una vera e propria **cornice normativa e morale** entro cui collocare l'utilizzo delle proprie tecnologie.

Questa strategia comunicativa riflette un aspetto più ampio della **diplomazia tecnologica israeliana**. Negli ultimi anni Israele ha infatti utilizzato il proprio primato nel settore cyber non solo come leva economica, ma anche come strumento di politica estera. Le tecnologie di sicurezza informatica, comprese quelle legate alla sorveglianza digitale, sono diventate un elemento sempre più rilevante nelle relazioni bilaterali con numerosi Paesi. Attraverso la vendita, il trasferimento tecnologico o la cooperazione nel campo della cyber-intelligence, Israele ha rafforzato relazioni strategiche con partner regionali e internazionali, creando nuove forme di cooperazione nel campo della sicurezza e dell'intelligence.

All'interno di questo quadro si inserisce la cosiddetta **diplomazia della sorveglianza**, che può essere interpretata come una declinazione specifica della più ampia diplomazia tecnologica. La fornitura di strumenti avanzati di intrusione informatica consente infatti di costruire relazioni di sicurezza particolarmente strette tra Stati. Chi acquisisce queste tecnologie non ottiene soltanto un software, ma entra spesso in una relazione di cooperazione tecnica che include supporto operativo, aggiornamenti, formazione e integrazione con altre infrastrutture di sicurezza digitale. Questo tipo di rapporto genera inevitabilmente **forme di dipendenza tecnologica** e contribuisce a rafforzare i legami strategici tra il Paese produttore e quello acquirente.

Dal punto di vista comunicativo, la retorica delle "democrazie illuminate" svolge quindi una funzione fondamentale: consente di presentare strumenti intrinsecamente controversi come parte di un **ecosistema di sicurezza legittimo e regolato**, trasformando una tecnologia potenzialmente invasiva in un asset coerente con la narrativa della cooperazione tra Stati democratici. È proprio attraverso questa costruzione discorsiva che la dimensione commerciale dello spyware tende a sovrapporsi alla sfera della diplomazia e della politica internazionale.

Tuttavia, proprio questa costruzione discorsiva mette in luce uno degli elementi più problematici della diplomazia della sorveglianza contemporanea. La distinzione tra utilizzo "legittimo" e utilizzo "illegittimo" degli spyware commerciali, spesso presentata come una linea di demarcazione chiara tra Stati democratici e regimi autoritari, si scontra con una realtà molto più complessa sul piano operativo e politico. La storia recente mostra infatti che anche Stati democratici possono utilizzare strumenti di sorveglianza avanzata contro giornalisti, dissidenti, attivisti o organizzazioni della società civile. La questione centrale, dunque, non riguarda tanto la natura del regime che acquista lo strumento, quanto piuttosto il livello di **accountability, controllo parlamentare e supervisione giudiziaria** che ne regola l'utilizzo.[42]

In questo contesto, l'esportazione di tecnologie cyber non può essere considerata una pratica neutrale. Come dimostrato dal caso di **NSO Group** e dello spyware **Pegasus**, la diffusione di questi strumenti rafforza relazioni bilaterali, crea nuove dipendenze tecnologiche e genera nuove dinamiche di potere tra Stati, sia alleati sia rivali. La diplomazia della sorveglianza rappresenta quindi una modalità attraverso cui capacità tecnologiche avanzate vengono trasformate in una fonte di influenza internazionale. Israele ha saputo utilizzare questo strumento non solo come asset economico, ma anche come leva di proiezione strategica, rafforzando il proprio ruolo all'interno delle reti internazionali di cooperazione in materia di sicurezza.

[42] Toy, Staff; "US lawmakers demand info from DEA, FBI on use of Israeli spyware"; *The Times of Israel*; 2022. Link.

All'interno di questo ecosistema tecnologico emergono tuttavia differenze significative tra le diverse tipologie di strumenti disponibili sul mercato. Lo spyware **Pegasus**, sviluppato da NSO Group, è noto per la sua capacità di ottenere un controllo estremamente esteso del dispositivo bersaglio, consentendo l'estrazione di una vasta gamma di dati presenti nello smartphone, tra cui contenuti delle comunicazioni, registri delle chiamate, file multimediali, dati di geolocalizzazione e informazioni archiviate nelle applicazioni installate.

Il sistema **Graphite**, sviluppato da Paragon, viene invece descritto come uno strumento progettato per operare in modo più mirato sulle infrastrutture di comunicazione digitale. Secondo le informazioni disponibili, una delle sue caratteristiche distintive consiste nella capacità di **estrarre dati non soltanto dal dispositivo fisico, ma anche direttamente dai servizi di cloud storage associati all'utente**, permettendo così di accedere a contenuti sincronizzati su piattaforme remote. Questo approccio amplia il raggio d'azione delle operazioni di intrusione informatica e può rendere più complessa la rilevazione dell'attività di sorveglianza, poiché parte delle informazioni viene acquisita attraverso l'ecosistema digitale collegato al dispositivo e non esclusivamente tramite il terminale stesso.[43]

Questa distinzione non è soltanto di natura tecnica, ma assume una rilevanza significativa anche sul piano **commerciale, politico ed etico**. Presentando Graphite come uno strumento focalizzato sull'accesso selettivo alle comunicazioni e sui dati associati ai servizi digitali dell'utente, Paragon ha cercato di costruire una narrativa di maggiore proporzionalità e specializzazione rispetto a piattaforme percepite come strumenti di controllo totale del dispositivo. In questo modo, la differenza tra le due architetture tecnologiche diventa anche un elemento di posizionamento nel mercato internazionale degli spyware, contribuendo a delineare diverse strategie di legittimazione e differenti modelli di utilizzo delle tecnologie di sorveglianza.

In questo senso, la competizione tra piattaforme di intrusione informatica non si gioca soltanto sul piano delle capacità tecniche, ma anche su quello della **legittimità politica e della percezione etica**. Le tecnologie di sorveglianza avanzata diventano così non solo strumenti operativi di intelligence, ma anche asset strategici attraverso cui Stati e aziende contribuiscono a ridefinire il rapporto tra sicurezza nazionale, innovazione tecnologica e influenza internazionale.

Allo stesso tempo, questo modello riflette una trasformazione più ampia del rapporto tra sicurezza nazionale e innovazione tecnologica. In un contesto internazionale in cui la competizione strategica si svolge sempre più spesso nel dominio digitale, le capacità di cyber intelligence e intrusione informatica diventano strumenti centrali per la raccolta di informazioni e per la gestione delle minacce emergenti. Le aziende che operano in questo settore non sono quindi semplici attori economici, ma componenti di un ecosistema strategico in cui **tecnologia, sicurezza e politica estera** risultano sempre più intrecciate.

2.4 Rischi e resilienza: le implicazioni per la sicurezza delle comunicazioni governative italiane e il rischio di escalation nella 'guerra delle ombre' (cyber-warfare)

Se da un lato strumenti di intrusione informatica avanzata come Graphite possono rappresentare una risorsa operativa per le attività di intelligence e sicurezza nazionale, dall'altro la loro crescente diffusione solleva interrogativi rilevanti per la resilienza delle comunicazioni governative e per la stabilità del sistema internazionale. La disponibilità di software capaci di compromettere dispositivi mobili e piattaforme di comunicazione cifrata riduce infatti la soglia tecnica necessaria per penetrare infrastrutture digitali utilizzate da soggetti istituzionali, diplomatici e militari.

Il problema non riguarda soltanto la possibilità che questi strumenti vengano utilizzati da attori ostili contro governi stranieri. Riguarda anche la natura stessa del mercato globale degli spyware commerciali, che tende a

[43] Studio della Commissione PEGA del Parlamento Europeo; *The use of Pegasus and equivalent surveillance spyware*; Parlamento Europeo; 2023. Link.

creare un ecosistema tecnologico caratterizzato da un elevato grado di opacità. In questo contesto, la linea di separazione tra uso legittimo, uso improprio e uso politico delle tecnologie di sorveglianza diventa progressivamente più difficile da tracciare. La disponibilità di questi strumenti a clienti governativi, anche formalmente sottoposti a procedure di autorizzazione o di vetting, non elimina il rischio di impieghi non trasparenti, uso selettivo contro oppositori interni o tentativi di penetrazione delle comunicazioni di figure chiave dello Stato.

Un elemento particolarmente significativo in questo senso emerge dal **report pubblicato dal Citizen Lab**[44], il centro di ricerca dell'Università di Toronto specializzato nello studio delle tecnologie di sorveglianza digitale. Nel corso delle proprie analisi sull'infrastruttura tecnica riconducibile a Paragon Solutions, i ricercatori hanno identificato server, certificati digitali e nodi di comunicazione associati al funzionamento del sistema Graphite. Ancora più rilevante è il fatto che le informazioni raccolte da Citizen Lab abbiano contribuito all'identificazione di un exploit **zero-click utilizzato per colpire circa novanta account WhatsApp appartenenti a giornalisti e membri della società civile**. Questo episodio dimostra come strumenti di intrusione informatica di alto livello possano essere impiegati in operazioni di sorveglianza mirata anche al di fuori di contesti strettamente militari o di sicurezza nazionale.

Il caso evidenzia inoltre una trasformazione più ampia dell'ecosistema della sicurezza digitale. Le operazioni di intrusione informatica non si svolgono più esclusivamente all'interno delle infrastrutture statali, ma coinvolgono sempre più spesso piattaforme tecnologiche globali e infrastrutture digitali private. In questo scenario, la sicurezza delle comunicazioni dipende sempre più dalla cooperazione tra una pluralità di attori: governi, piattaforme digitali, centri di ricerca indipendenti e aziende tecnologiche. Il fatto che l'exploit individuato da Citizen Lab sia stato successivamente mitigato attraverso la collaborazione con Meta dimostra come la sicurezza del cyberspazio contemporaneo sia il risultato di un equilibrio complesso tra **attori pubblici e privati**.

Accanto a questi aspetti emerge un ulteriore elemento di vulnerabilità spesso meno discusso nel dibattito pubblico: la **dipendenza tecnologica dai fornitori privati di strumenti di intrusione informatica**. Anche nei casi in cui software come Graphite vengano installati su infrastrutture controllate direttamente dalle autorità governative, la natura proprietaria di queste tecnologie implica inevitabilmente una forma di dipendenza dal vendor per quanto riguarda aggiornamenti, manutenzione del sistema e sviluppo di nuove vulnerabilità sfruttabili. Questa relazione introduce un problema strutturale di sicurezza della supply chain tecnologica. Le aziende che sviluppano questi strumenti possiedono infatti una conoscenza approfondita dell'architettura tecnica dei sistemi installati e mantengono spesso un ruolo centrale nel loro aggiornamento operativo.

Dal punto di vista della sicurezza nazionale, ciò solleva interrogativi rilevanti sul piano della **sovranità digitale**. L'utilizzo di strumenti di sorveglianza avanzata sviluppati da società esterne comporta infatti il rischio che informazioni operative sensibili, o quantomeno metadati tecnici relativi alle operazioni, transitino all'interno di una filiera tecnologica non completamente sotto il controllo dello Stato. Anche nel caso in cui i dati raccolti restino formalmente sotto il controllo dell'agenzia utilizzatrice, la dipendenza da software proprietari e da exploit sviluppati da fornitori privati introduce un livello di vulnerabilità che deve essere attentamente valutato.

Per un Paese come l'Italia, questo scenario impone una riflessione particolarmente netta. La sicurezza nazionale non dipende soltanto dalla capacità di acquisire strumenti di sorveglianza offensiva, ma anche - e soprattutto - dalla capacità di proteggere le comunicazioni delle istituzioni, del comparto intelligence, della diplomazia e degli apparati militari da intrusioni analoghe. In altri termini, la disponibilità di spyware sul

[44] Marczak, Bill; Scott-Railton, John; Robertson, Kate; Perry, Astrid; Brown, Rebekah; Abdul Razzak, Bahr; Anstis, Siena; Deibert, Ron; *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*; Citizen Lab Report No. 183, University of Toronto; 2025.

mercato internazionale produce una **simmetria strategica inquietante**: gli stessi strumenti che alcuni governi considerano essenziali per la propria sicurezza possono costituire una minaccia per la sicurezza degli altri.

Questo aspetto assume un rilievo ancora maggiore se si considera il ruolo centrale che smartphone e piattaforme di comunicazione digitale svolgono oggi nelle attività istituzionali. Diplomatici, funzionari pubblici, ufficiali militari e rappresentanti delle istituzioni utilizzano quotidianamente dispositivi mobili e applicazioni di messaggistica per scambiare informazioni e coordinare attività operative. La compromissione di uno di questi dispositivi può quindi tradursi non soltanto nella sottrazione di informazioni sensibili, ma anche nella possibilità di ricostruire reti relazionali istituzionali, flussi decisionali e dinamiche interne alle amministrazioni pubbliche.

Questa dinamica contribuisce ad alimentare quella che viene spesso definita **"guerra delle ombre" nel cyberspazio**: un conflitto a bassa visibilità caratterizzato da operazioni coperte, penetrazioni silenziose, raccolta occulta di informazioni e difficoltà di attribuzione immediata. Non si tratta di una prospettiva teorica o futura, ma di una dimensione del confronto strategico già pienamente operativa.[45] Negli ultimi anni, numerose attività di intrusione informatica attribuite - direttamente o indirettamente - ad attori statali hanno dimostrato come il dominio cyber venga ormai utilizzato come strumento di pressione geopolitica permanente. Le operazioni riconducibili a gruppi legati alla Federazione Russa[46], ad esempio, hanno colpito infrastrutture governative, reti diplomatiche e sistemi di comunicazione in diversi paesi europei e nordamericani, mostrando come il cyberspazio sia diventato uno dei principali teatri della competizione strategica contemporanea.

Di conseguenza, il rischio di escalation non deriva soltanto dalla capacità offensiva degli strumenti tecnologici, ma soprattutto dalla loro opacità operativa. Quando uno Stato scopre - o sospetta - di essere stato oggetto di un'operazione di intrusione informatica, la risposta può risultare difficile da calibrare, proprio perché il perimetro dell'attacco e l'identità dell'attore responsabile restano spesso incerti. L'ambiguità dell'attribuzione e la natura coperta di molte operazioni cyber rendono infatti più complessa la distinzione tra attività di intelligence, operazioni di influenza e vere e proprie azioni ostili, aumentando il rischio di fraintendimenti e di escalation non intenzionali.

Per queste ragioni, la questione degli spyware commerciali non può essere ridotta né a un semplice problema tecnologico né a una controversia giuridica. Si tratta di una questione pienamente strategica, che investe la **sicurezza delle comunicazioni governative, la sovranità digitale e la stabilità delle relazioni internazionali**. In un ambiente internazionale sempre più segnato da forme di conflitto coperte e asimmetriche, la capacità degli Stati di proteggere le proprie infrastrutture comunicative e di ridurre le vulnerabilità della propria supply chain tecnologica diventa un elemento centrale della sicurezza nazionale.

2.5 Applicazione pratica sul campo

Per comprendere concretamente il funzionamento e l'utilizzo operativo di strumenti di intrusione informatica come quelli sviluppati da Paragon Solutions è necessario osservare il modo in cui queste tecnologie vengono impiegate all'interno delle attività investigative e di intelligence. Gli spyware di nuova generazione non sono progettati per effettuare operazioni di sorveglianza indiscriminata su larga scala, ma per operazioni mirate finalizzate a ottenere accesso diretto ai dispositivi digitali utilizzati da specifici soggetti considerati di interesse investigativo.

In un'operazione di intelligence digitale, la fase iniziale consiste nell'**identificazione del bersaglio**. Questa attività avviene generalmente attraverso strumenti investigativi tradizionali, come l'analisi delle comunicazioni disponibili, la sorveglianza fisica, l'attività informativa svolta da fonti umane o l'analisi di dati provenienti da indagini precedenti. L'obiettivo è individuare con precisione il soggetto di interesse e,

[45] Davis, Elizabeth; *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*; 2021. DOI: 10.5771/9781538149683.
[46] Jones, Seth G.; *Russia's Shadow War Against the West*; CSIS, Center for Strategic & International Studies; 18 marzo 2025. Link.

soprattutto, il dispositivo digitale utilizzato abitualmente per comunicare o gestire le proprie attività. L'identificazione del terminale rappresenta infatti un passaggio fondamentale: nelle operazioni di intrusione informatica il dispositivo personale costituisce il punto di accesso principale all'ecosistema informativo dell'individuo monitorato.

Una volta identificato il dispositivo bersaglio, le autorità investigative possono ricorrere a strumenti di intrusione informatica mirata per ottenere accesso remoto al terminale. Nel caso di spyware avanzati come Graphite, l'infezione può avvenire sfruttando vulnerabilità informatiche presenti nei sistemi operativi o nelle applicazioni installate sul dispositivo. Queste vulnerabilità, spesso definite **zero-day**, rappresentano falle di sicurezza non ancora note ai produttori dei software e quindi non ancora corrette attraverso aggiornamenti di sicurezza. In molti casi l'accesso al dispositivo può essere ottenuto attraverso modalità cosiddette **zero-click**, che non richiedono alcuna interazione da parte dell'utente bersaglio. Il dispositivo viene compromesso semplicemente ricevendo dati attraverso applicazioni di comunicazione o servizi online, sfruttando i processi automatici di gestione dei contenuti presenti nel sistema operativo o nelle piattaforme digitali.

Una volta installato, lo spyware opera come un sistema di sorveglianza invisibile che consente agli operatori di intelligence di accedere a una vasta gamma di informazioni presenti nel dispositivo. Tra queste rientrano i contenuti delle conversazioni sulle applicazioni di messaggistica istantanea, i registri delle chiamate, le rubriche dei contatti, i file multimediali, i messaggi di posta elettronica e i dati di geolocalizzazione. In alcuni casi è inoltre possibile accedere alle informazioni archiviate nei servizi di cloud storage collegati al dispositivo, consentendo agli investigatori di recuperare dati anche se questi sono stati eliminati localmente dall'utente.

Il vantaggio strategico di questo approccio risiede nel fatto che le informazioni possono essere acquisite **prima che vengano cifrate o dopo che sono state decifrate dal dispositivo**, aggirando così i sistemi di crittografia end-to-end utilizzati dalle principali piattaforme di comunicazione digitale e le sue vulnerabilità[47]. Piuttosto che tentare di violare i protocolli crittografici durante la trasmissione dei dati, le tecnologie di intrusione informatica mirata consentono quindi di accedere direttamente alla fonte dell'informazione, ovvero il dispositivo utilizzato dal soggetto monitorato.

Per comprendere meglio la logica operativa di questi strumenti si può considerare uno scenario investigativo nel quale un'agenzia di sicurezza stia monitorando un individuo sospettato di appartenere a una rete logistica collegata a un'organizzazione terroristica internazionale. Il soggetto utilizza abitualmente piattaforme di messaggistica criptata per comunicare con altri membri della rete e coordinare attività operative. In questo contesto, le tecniche tradizionali di intercettazione delle comunicazioni risultano inefficaci a causa dei sistemi di crittografia end-to-end che proteggono il contenuto dei messaggi.

Attraverso un'operazione di intrusione informatica mirata, l'agenzia può compromettere il dispositivo mobile del sospetto e accedere direttamente alle informazioni presenti nel terminale. L'analisi dei dati raccolti può permettere agli investigatori di ricostruire le comunicazioni interne alla rete, identificare i contatti più frequenti del soggetto, individuare eventuali luoghi di incontro e comprendere le modalità con cui vengono coordinate le attività del gruppo. In questo modo, l'intrusione informatica non rappresenta soltanto uno strumento di sorveglianza individuale, ma diventa un mezzo per **mappare strutture relazionali e operative più ampie**.

Dal punto di vista dell'analisi investigativa, i dati ottenuti tramite lo spyware possono essere utilizzati per costruire modelli di **network analysis**, che permettono di individuare nodi centrali all'interno di una rete organizzativa e di comprendere le dinamiche di interazione tra i diversi soggetti coinvolti. Questo tipo di analisi

[47] Le vulnerabilità non si limitano soltanto a quelle delle applicazioni, come Whatsapp, ma anche a quelle del dispositivo stesso. Ad esempio, la Apple è dovuta correre ai ripari con i dispositivi più recenti. Si veda ad esempio: Apple Security Engineering and Architecture; "Memory Integrity Enforcement: A complete vision for memory safety in Apple devices"; *Apple Security Research Blog*; 2025. Link.

consente alle autorità di sicurezza di passare dalla semplice raccolta di informazioni a una comprensione più sistemica delle strutture operative di gruppi criminali o terroristici.

L'utilizzo di strumenti di intrusione informatica mirata riflette quindi una trasformazione più ampia dell'intelligence contemporanea. Lo smartphone o il computer personale non rappresentano più soltanto strumenti di comunicazione, ma vere e proprie **piattaforme di acquisizione informativa**, capaci di fornire una quantità estremamente ampia di dati relativi alle attività digitali e relazionali di un individuo. Attraverso l'accesso a queste informazioni, le agenzie di sicurezza possono ricostruire non solo le comunicazioni di un determinato soggetto, ma anche il contesto operativo e sociale in cui egli agisce.

Allo stesso tempo, proprio questa profondità di accesso ai dispositivi personali rappresenta uno degli aspetti più controversi di queste tecnologie. L'intrusione informatica mirata consente infatti di raccogliere una quantità estremamente ampia di dati sensibili che riguardano non soltanto le comunicazioni, ma l'intero ecosistema digitale dell'individuo monitorato. Per questo motivo, l'utilizzo di tali strumenti solleva interrogativi rilevanti sul piano giuridico e politico, soprattutto nei contesti democratici in cui le attività di sorveglianza devono essere bilanciate con la tutela dei diritti fondamentali e sottoposte a meccanismi di controllo istituzionale.

Capitolo 3 – Le leve di Pechino: CETC, BeiDou e la fusione civile-militare

A cura di Vittorio Iacopini

Palantir vende la guerra al Pentagono, mentre Paragon la affitta ai governi che possono permettersela. In ambedue i casi, il potere tecnologico risiede altrove rispetto a chi lo esercita: in una società privata, in un contratto, in una licenza revocabile. Pechino osserva questo modello e lo giudica, nella sua essenza, una forma di debolezza strutturale.

La risposta cinese non è speculare, lontana dalla creazione di un Palantir di Stato, o di un Paragon governativo. È la **fusione civile-militare** (军民融合), dottrina che affonda le radici nel concetto taoista-legista di ***shi*** (勢), ossia la disposizione del campo prima dello scontro, il potere come architettura invisibile che orienta gli eventi prima che accadano. Il potenziale strategico è di conseguenza generato dalla configurazione delle forze in un contesto, che rende certe evoluzioni degli eventi più probabili e altre meno, indipendentemente dall'azione diretta. Sun Tzu lo descrive con un'immagine concisa: **un masso rotondo sulla sommità di una montagna non ha bisogno di essere spinto con forza, basta che il terreno sia inclinato**.

Tale concezione trova una declinazione bellica già teorizzata nel 1999, quando i colonnelli del PLA Qiao Liang e Wang Xiangsui anticiparono nel loro saggio "**Unrestricted Warfare**" la dissoluzione dei confini tra tecnologia militare e civile: ogni progresso applicato a scopi civili può essere convertito per obiettivi militari, ogni infrastruttura può diventare un'arma, **ogni spazio – compresa la rete informatica o il mercato finanziario – può diventare campo di battaglia**.[48] Una visione che la dottrina Gerasimov avrebbe sistematizzato quasi quindici anni dopo nel concetto di guerra ibrida.[49]

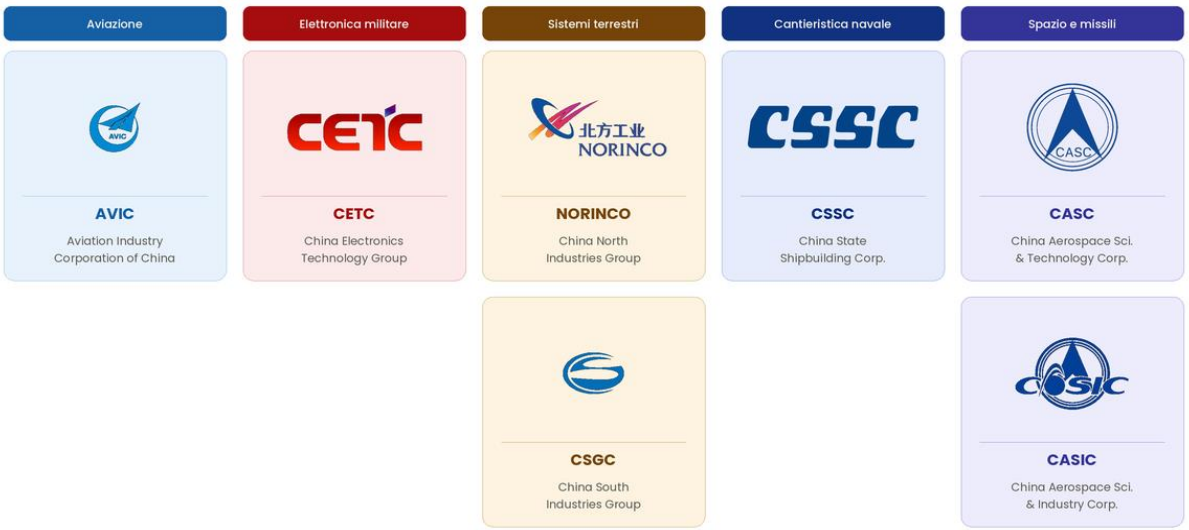

Figura 1. Le principali imprese statali cinesi nel settore della difesa e del dual-use (SOE).

Fonte: elaborazione dell'autore su dati da Béraud-Sudreau, Lucie; Nouwens, Meia; *Weighing Giants: Taking Stock of the Expansion of China's Defence Industry*; Defence and Peace Economics, vol. 32, n. 2; 2021; pp. 151–177.

[48] Qiao, Liang; Wang, Xiangsui; *Unrestricted Warfare: China's Master Plan to Destroy America*; Shadow Lawn Press; 2017 [ed. or. PLA Literature and Arts Publishing House, 1999]. Il sottotitolo *China's Master Plan to Destroy America* fu aggiunto dall'editore panamense nella prima traduzione inglese e non compare nell'edizione originale cinese, il cui sottotitolo recita: *Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization*.
[49] Gerasimov, Valery; *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*; trad. Robert Coalson; Military Review, gennaio-febbraio 2016. Link. L'articolo è la traduzione inglese del testo originale pubblicato su Voyenno-Promyshlennyy Kurier il 27 febbraio 2013.

Alla dimensione strategica si intreccia la **visione confuciana dello Stato come organismo unitario**: il confine tra interesse collettivo e volontà sovrana non è una tensione da gestire, ma una contraddizione da eliminare alla radice. È qui che la distanza con il modello occidentale si amplia – non sul piano tecnologico, bensì su quello filosofico e, ancor prima, antropologico. Da un lato l'individuo, l'azienda privata; dall'altro la collettività come soggetto indiviso, in cui **Stato, industria e forza militare parlano una sola lingua**.

Secondo dati ufficiali cinesi del 2017, **le cellule del Partito Comunista sono presenti nel 68% delle imprese private e nel 91% di quelle statali**. A partire dal 2020, il Partito ha intensificato il monitoraggio diretto delle aziende high-tech, orientandone le decisioni strategiche. Lo Stato incrementa contestualmente la propria presenza finanziaria attraverso investimenti di **SOE** e organismi governativi, condizionando l'accesso alle risorse. Anche i 300 unicorni censiti nel 2021 non operano in condizioni di libero mercato, essendo soggetti a crescente controllo politico e riorientamento strategico. La distinzione tra settore privato e Stato, in Cina, è una distinzione di facciata: utile alla narrazione, irrilevante nella pratica.[50]

Oltre il Pacifico, la fusione civile-militare è quindi un'espressione di ordine cosmologico applicato alla competizione globale. Molteplici aziende detenute dallo Stato diventano le colonne portanti della strategia cinese per i decenni a venire. Direzionate dal Partito, le compagnie producono tecnologia per lo Stato e poi, se necessario, per il mercato. Così, la direzione del flusso si inverte: con essa cambia l'intera logica del rapporto tra potere pubblico e innovazione privata, che invece struttura il modello occidentale.

Tra queste emerge la **China Electronics Technology Group Corporation (CETC)**, il conglomerato statale delegato al settore dell'elettronica per la difesa, protagonista delle pagine che seguono.

3.1 CETC dallo Xinjiang al teatro operativo

Mettendo tra parentesi il giudizio etico – necessario ma non dirimente ai fini dell'analisi strategica – un vantaggio appare inequivocabile: il Governo può implementare e sperimentare sistemi di sorveglianza e fusione dati analoghi a quelli di Palantir senza vincoli normativi, e dispone di un **laboratorio a scala reale composto da 1,4 miliardi di cittadini**.

Come conseguenza di ciò, il concetto di dual use assume la sua accezione più radicale. Il sistema viene concepito *ab origine* per essere simultaneamente civile e militare, commerciale e operativo. Ogni piattaforma testata sulla popolazione diventa potenzialmente traslabile su un teatro di guerra. Qui emerge **l'Integrated Joint Operations Platform** (**IJOP**, 体化联合作战平台), sviluppata dalla CETC. Se poi la piattaforma viene testata in un territorio considerato "ribelle" dal Partito Comunista, ancora meglio.

È il caso dello **Xinjiang**, regione nell'estremo nord-ovest del "Regno di Mezzo"[51]. Da sempre influenzata dalle culture autoctone dell'area centro-asiatica, è – insieme al Tibet – una delle poche regioni cinesi in cui gli han non costituiscono la maggioranza della popolazione.[52] Il gruppo etnico più numeroso sono gli Uiguri, che compongono il 46% della popolazione regionale: popolo turco-musulmano con lingua, tradizioni e identità culturale distinte dalla han dominante nel resto della Cina.[53] Una presenza che Pechino ha storicamente percepito come una variabile da gestire. Prima attraverso la colonizzazione demografica, poi con

[50] Evron, Yoram; Bitzinger, Richard A.; *The Fourth Industrial Revolution and Military–Civil Fusion: A New Paradigm for Military Innovation?*; Cambridge University Press; 2023.
[51] Il termine "Regno di Mezzo" è la traduzione letterale di *Zhōngguó* (中国), nome con cui la Cina si autodefinisce: *zhōng* (中) "centro", *guó* (国) "stato/regno". Riflette la tradizionale concezione sinocentrica del mondo civilizzato.
[52] State Council Information Office of the People's Republic of China; *Xinjiang Population Dynamics and Data*; State Council Information Office; 2021. Link.
[53] Pew Research Center; *Measuring Religion in China – 5. Islam*; Pew Research Center; 2023. Link.

l'assimilazione forzata, infine con quello che le autorità definiscono "mantenimento della stabilità"[54] e che la comunità internazionale documenta come repressione sistematica.

In tale quadro, attraverso il reverse engineering dell'app mobile utilizzata dalla polizia dello Xinjiang – sviluppata da HBFEC, sussidiaria CETC – è stata ricostruita con precisione l'architettura di sorveglianza sottostante. Il sistema aggrega dati eterogenei collegandoli al numero di carta d'identità nazionale: altezza al centimetro, colore dell'auto, traiettoria di telefoni e veicoli, consumo di elettricità, contatti con l'estero.[55]

A ciò si sommano comportamenti quotidiani e leciti. Non socializzare con i vicini, usare WhatsApp, donare a una moschea, allontanarsi dal proprio distretto senza permesso, anch'essi vengono codificati come "micro-indizi" di potenziale minaccia e trasmessi automaticamente alle autorità. Il risultato è un sistema di targeting preventivo in cui **l'algoritmo sostituisce il giudizio umano**: non si indaga su chi ha commesso un reato, ma su chi il sistema ha classificato come deviante. Per molti degli individui segnalati, la destinazione è stata la detenzione arbitraria nei campi di "rieducazione politica".[56]

La distinzione tra sorveglianza di massa e warfare data-driven non si riduce a una questione di contesto. Difatti, la guerra introduce variabili di complessità ben più ostiche: ambienti elettromagnetici contestati, avversari che reagiscono, sistemi progettati per resistere alla degradazione. Eppure, il trasferimento non è privo di fondamento.

Le capacità **di fusione dati multi-dominio, di targeting predittivo e di gestione automatizzata delle priorità, sviluppate e testate su scala reale nello Xinjiang**, rappresentano un patrimonio tecnico e dottrinale che nessun esercizio simulativo avrebbe potuto produrre con la stessa profondità. Il laboratorio Xinjiang ha rappresentato il battesimo di una dottrina, la stessa che alimenta i **Digital Twins** tattici del PLA, repliche digitali del teatro operativo su cui simulare, pianificare e decidere prima ancora che l'azione abbia luogo.

Nelle parole del Maggiore Generale del PLA Wang Mingxiao: «costruire un mondo digitale altamente speculare rispetto al mondo fisico reale. Come guardare in uno specchio»[57] – e attraverso quello specchio, decidere prima che il nemico si muova. Anche qui CETC è protagonista. Questo, infatti, fornisce sistemi di comando, controllo, comunicazioni, computer, intelligence, sorveglianza e ricognizione (**C4ISR**) per tutte le branche delle forze armate.[58]

Ulteriore conferma della sinergia tra PLA e CETC è il volume di appalti che quest'ultima si è aggiudicata. Sono 90 i contratti affidati all'azienda su 155 offerte a cui ha aderito tra gennaio 2023 e dicembre 2024. Prima tra le imprese controllate dallo Stato per numero di appalti in questo periodo, **CETC diventa primo braccio operativo dell'innovazione bellica cinese**.[59] La stessa infrastruttura trasla dal contesto della sorveglianza interna al dominio militare. Il terreno, ancora una volta, viene inclinato prima dello scontro.

3.2 Lo spettro come campo di battaglia

Se la superiorità dell'informazione è centrale, la sua condizione di possibilità risiede nel controllo dello spettro elettromagnetico, complementare ai Digital Twins e da essi dipendente. Senza dati in tempo reale che

[54] Chinese Communist Party Central Committee; *Document Number 7: Record of the Meeting of the Standing Committee of the Politburo Concerning the Maintenance of Stability in Xinjiang*; 1996; citato in Dillon, Michael; *Xinjiang Uyghur Autonomous Region (Eastern Turkestan)*, Supplementary Memorandum; University of Durham; UK Parliament Select Committee on Foreign Affairs, Appendix 19. Link.
[55] Wang, Maya; *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*; Human Rights Watch; 2019. Link.
[56] Ibidem.
[57] Qian, Xiaohu; Wang, Lingshuo; *Wang Mingxiao: accelerare l'applicazione militare della tecnologia del gemello digitale*; China Military Online — PLA Daily; 2021. Link.
[58] China Electronics Technology Group Corporation (CETC); "C4KISR – Products & Service: International Trade"; CETC. Link.
[59] McFaul, Cole; Bresnick, Sam; Chou, Daniel; *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage*; Center for Security and Emerging Technology (CSET); 2025. Link.

viaggiano su frequenze protette, ogni replica digitale del teatro operativo diventa uno specchio opaco. Il teatro privilegiato è il Pacifico occidentale, dove la dottrina cinese punta a rendere insostenibile la proiezione di potenza statunitense. Quella che gli analisti occidentali codificano come **Anti-Access/Area Denial** (A2/AD) è la risposta asimmetrica sviluppata da Pechino a partire dagli anni Novanta. Dopo aver osservato la prima Guerra del Golfo, la Cina ha ipotizzato un esito sfavorevole in un eventuale conflitto convenzionale con gli Stati Uniti e si è messa all'opera.[60]

In tal senso, **la guerra elettronica è diventata il dominio determinante del conflitto moderno**, cogliendo impreparata buona parte della dottrina occidentale. I quadri militari del PLA l'hanno trasformata da mera funzione di supporto operativo a spina dorsale della guerra contemporanea: prima concettualmente, poi attraverso la modernizzazione sistematica dell'Esercito Popolare di Liberazione in questa direzione.[61]

Lo spettro elettromagnetico cessa di essere un enabler dello scontro per diventarne il terreno stesso. In quest'ambito si decide chi vede, chi comunica, chi guida le proprie armi con precisione – e chi no.

La kill chain cinese si articola in tre fasi distinte ma strettamente collegate, tutte dipendenti dal controllo dello spettro (Figura 2).

La prima fase, *Find/Fix*, è quella del rilevamento e della localizzazione. La Cina impiega radar skywave over-the-horizon (OTH) che riflettono segnali nella banda ad alta frequenza sulla ionosfera, individuando navi fino a 2.000-3.000 km di distanza, ben oltre la portata dei sistemi convenzionali. Parallelamente, costellazioni satellitari captano ed elaborano le emissioni elettroniche delle unità navali ostili per triangolarne la posizione. Il nemico viene individuato ben prima di entrare nel raggio d'azione visivo cinese.

Segue la seconda fase: *Track/Target*, che trasforma il rilevamento in puntamento preciso. Satelliti radar ad apertura sintetica (SAR) e ottici aggiornano la posizione del bersaglio quasi in tempo reale. Su questo fronte Pechino ha investito in modo sistematico: la costellazione Jilin-1 conta oggi oltre 117 satelliti ed è in grado di osservare qualsiasi punto del globo circa 40 volte al giorno.[62] I dati satellitari vengono trasmessi alle piattaforme di lancio attraverso reti C4ISR.[63]

Infine, nella fase terminale, avviene l'ingaggio. Missili balistici antinave come il DF-21D, i sensori di bordo – radar attivi o cercatori a infrarossi (IR) – devono distinguere il bersaglio reale dal rumore di fondo e correggere la traiettoria negli ultimi secondi, quando il bersaglio si è già spostato dalla posizione originariamente rilevata. Lo **spettro è il *medium* attraverso cui questo aggiustamento avviene**. Tra il momento in cui un satellite scatta una foto e il momento in cui i dati vengono elaborati e trasmessi al missile, passano dai 15 minuti (scenario ottimistico) alle 2 ore.[64]

A tenere insieme le tre fasi è la dottrina cinese dell'**Integrated Network Electronic Warfare** (**INEW**). Proteggere la propria kill chain e, al contempo, distruggere quella nemica. Il jamming delle comunicazioni satellitari e dei segnali GPS avversari serve esattamente a questo.

Il Pentagono, nel suo rapporto annuale al Congresso del 2025, ha riconosciuto che la Cina dispone già di una gamma di jammer terrestri e sta sviluppando jammer spaziali, inclusi spooffers per i sistemi di navigazione satellitare globale e jammer per le comunicazioni satellitari (SATCOM) su bande di frequenza multiple, comprese quelle ad altissima frequenza utilizzate dal sistema militare statunitense. All'inizio del 2024,

[60] Heginbotham, Eric et al.; *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*; RAND Corporation; 2015; pp. 25-26, 272-275.
[61] Ibidem.
[62] Xinhua; "Chinese Remote Sensing Satellite Constellation to Offer Global Services"; *Xinhua News Agency*; 4 marzo 2025. Link.
[63] Heginbotham; *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power*, 1996–2017; pp. 157-165.
[64] Ibidem; pp. 165-170.

scienziati cinesi hanno dichiarato di aver raggiunto il monitoraggio e l'analisi in tempo reale dell'intero spettro elettromagnetico a banda larga, a supporto delle future operazioni di guerra elettronica del PLA.[65]

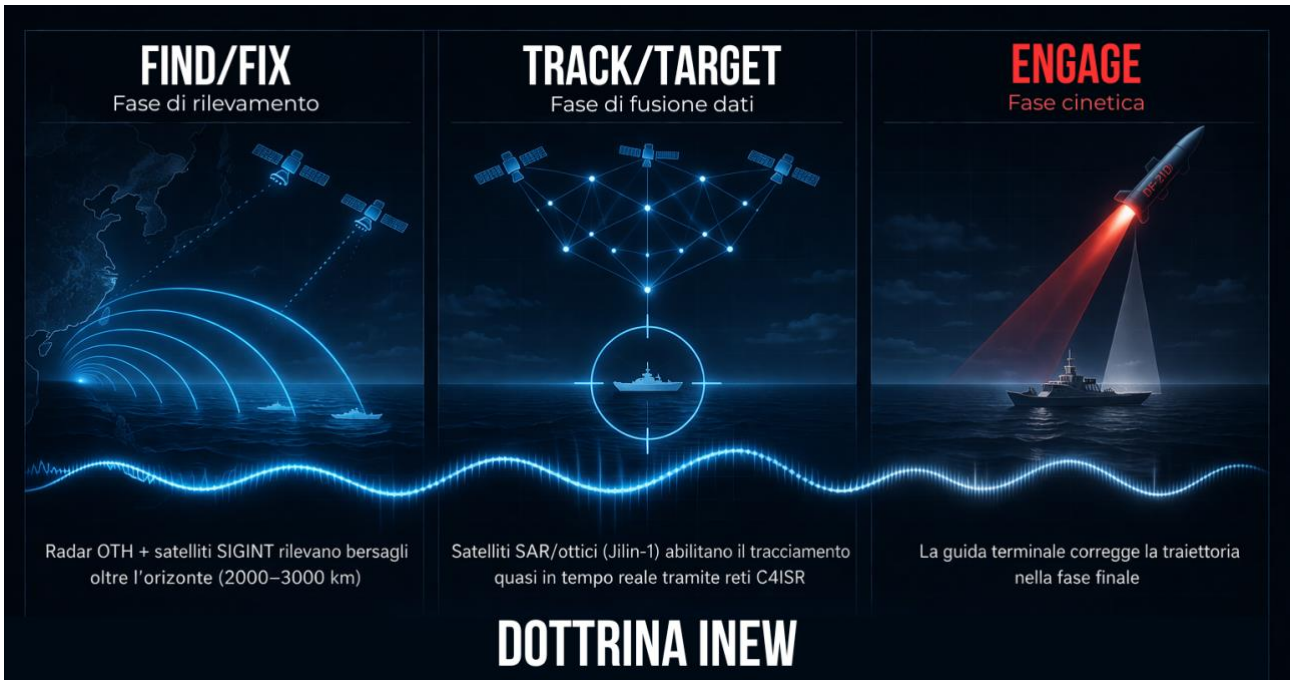

Figura 2. La catena di ingaggio cinese: rilevamento, fusione dati e attacco cinetico nella dottrina INEW.

Fonte: elaborazione dell'autore su dati da Heginbotham; *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power*, 1996–2017; pp. 157-170.

Lo spettro elettromagnetico è la colonna portante dell'attuale assetto militare cinese, trasversale a ogni potenziale azione cinetica dell'Esercito Popolare di Liberazione. Lo era già nella dottrina ufficiale: nel 2009 la National Defense University (NDU) di Pechino enunciava che «tutti i tipi di armi impiegate dai militari moderni – artiglieria, carri armati, aerei, navi da guerra e missili – sono equipaggiati in misura diversa con sistemi di informazione elettronica, e il sistema di comando che dirige le operazioni militari moderne non può prescindere dalle infrastrutture elettroniche».[66] Nel tempo che separa quelle prime enunciazioni dottrinali dal presente, la Cina ha accresciuto in modo sostanziale il proprio potenziale nel dominio della guerra elettronica, trasformando un principio teorico in un'architettura operativa concreta.

Al centro di tale framework si trova ancora una volta la China Electronics Technology Group Corporation. CETC è l'ingegnere statale dello spettro – chiarito altresì nella propria autodefinizione istituzionale, "forza principale dell'elettronica militare" (军工电子主力军)[67] e "forza tecnologica strategica dello Stato" (国家战略科技力量)[68]. Il soggetto industriale che progetta, integra e mantiene l'infrastruttura elettromagnetica senza cui la kill chain cinese non regge, dalla rilevazione oltre l'orizzonte alla guida terminale del missile.

[65] U.S. Department of Defense; *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*; Department of Defense; 2025. Link;

[66] National Defense University of the People's Republic of China; *Lectures on Joint Campaign Information Operations*; trad. e ed. China Aerospace Studies Institute (CASI), Air University; 2021. L'opera, redatta con il contributo del General Staff Operations Department e dell'Academy of Military Sciences, costituisce il materiale didattico ufficiale dei corsi NDU sull'information operations a livello di campagna congiunta. L'edizione di riferimento è del 2009. Link.

[67] China Electronics Technology Group Corporation (CETC); "集团简介 – Profilo del Gruppo"; CETC. Link.

[68] China Electronics Technology Group Corporation (CETC); "使命定位 – Missione e posizionamento strategico"; CETC. Link.

3.3 BeiDou e la sovranità satellitare

L'infrastruttura C4ISR, entro cui si è inquadrato il ruolo del software e del dominio dello spettro, è strettamente dipendente da un ulteriore elemento che, come evidenziato nella Figura 2, risulta imprescindibile in ogni fase della kill chain: una rete satellitare efficiente, capillare e sovrana. Pechino lo ha imparato sulla propria pelle trent'anni fa.

Nel 1996, durante la Terza Crisi dello Stretto di Taiwan, la Cina lanciò tre missili nell'area come segnale di deterrenza. Il primo colpì a circa 18 chilometri dalla base militare di Keelung. Gli altri due si persero. Pechino sostenne che gli Stati Uniti avevano deliberatamente interrotto il segnale GPS su cui la Cina dipendeva per la guida missilistica. Nelle parole di un colonnello del PLA questa fu «un'umiliazione indimenticabile. È così che abbiamo deciso di sviluppare il nostro sistema di navigazione globale, qualunque fosse il costo».[69]

A trent'anni di distanza, la lezione si è tramutata nella flotta di **satelliti GNSS** più numerosa al mondo: 45 satelliti operativi stimati[70] contro i 31 del GPS americano.[71] Il sistema si chiama **BeiDou** (BDS) – altro grande protagonista di questo capitolo – ed è un progetto interamente statale sviluppato principalmente da CASC e CASIC, le due aziende pubbliche del settore aerospaziale cinese. CETC ne costituisce l'infrastruttura digitale: fornisce i terminali, i chip di ricezione e l'integrazione nella catena di comando del PLA.

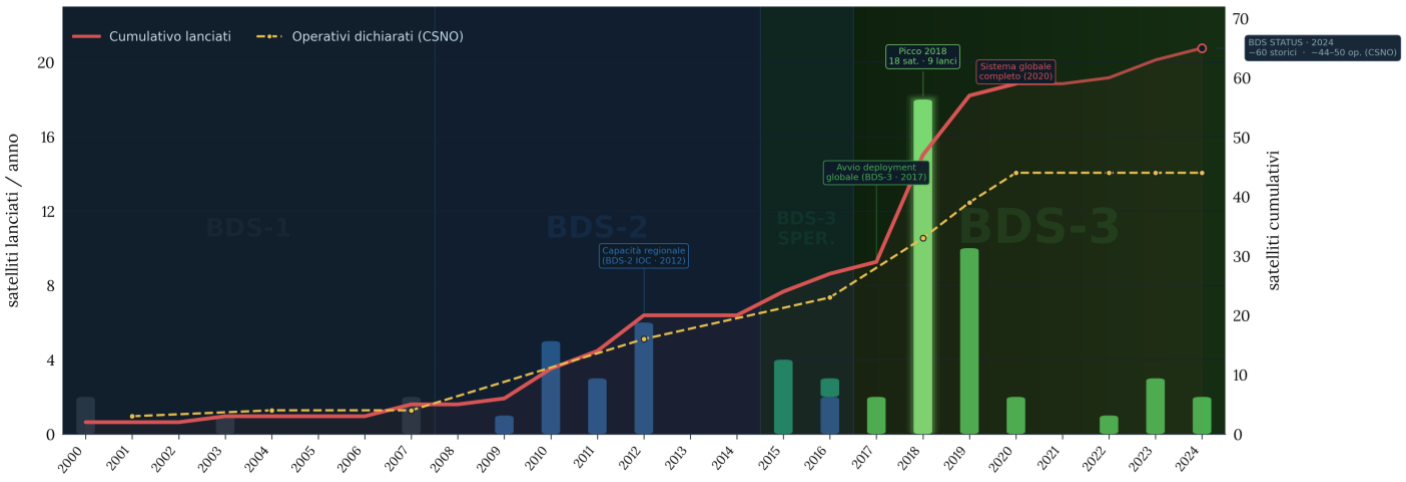

Figura 3. Evoluzione dei lanci e della costellazione BeiDou (2000–2024)

Fonte: elaborazione dell'autore su dati da molteplici fonti.[72]

Senza GNSS, un missile non sa dove si trova in volo, un drone non si orienta, due unità su teatri distanti non possono coordinarsi nello stesso istante. Come hanno testimoniato gli ultimi trent'anni di conflitti, questa è l'infrastruttura che rende possibile la guerra di precisione moderna.

---

[69] U.S.-China Economic and Security Review Commission; *Chapter 2, Section 2: China's Space and Counterspace Programs*; in *2015 Annual Report to Congress*; U.S.-China Economic and Security Review Commission; 2015; p. 302. Link; Goswami, Namrata; "The Economic and Military Impact of China's BeiDou Navigation System"; The Diplomat; 2020. Link.

[70] Sewall, Sarah; Vandenberg, Tyler; Malden, Kaj; *China's BeiDou: New Dimensions of Great Power Competition*; Belfer Center for Science and International Affairs, Harvard Kennedy School; 2023. Link. Il numero di satelliti BeiDou operativi varia a seconda delle fonti e dei criteri di classificazione (inclusione o esclusione di satelliti in fase di test o in riserva). Il dato di 45 satelliti è una stima attendibile basata su fonti multiple riferite al 2023-2024.

[71] National Coordination Office for Space-Based Positioning, Navigation, and Timing; "Space Segment"; GPS.gov. Link.

[72] European Space Agency / eoPortal; "China Navigation Satellite System (CNSS) – BeiDou Constellation"; eoPortal. Link. Sewall, *China's BeiDou: New Dimensions of Great Power Competition*. Link. Tan, Shusen; *GNSS Systems and Engineering: The Chinese BeiDou Navigation and Position Location Satellite*; John Wiley & Sons e National Defense Industry Press; 2018. Xie, Jun; "BeiDou Navigation Satellite System in 2024"; *GPS World*; 2024. Link.
La conta cumulativa è riferita ai satelliti lanciati (inclusi quelli sperimentali e di sostituzione), non ai satelliti operativi attivi.

La flotta cinese ha attraversato tre generazioni in vent'anni: regionale e sperimentale nel 2000, esteso all'Asia-Pacifico nel 2012, globale nel 2020, con capacità integrate di messaggistica, ricerca e soccorso e posizionamento ad alta precisione (Figura 3).

Il sistema di navigazione satellitare BeiDou opera **in tre diverse tipologie di orbite**, differenziandosi dagli altri sistemi GNSS come il GPS, i quali utilizzano principalmente orbite medie (Medium Earth Orbit, MEO) ad altitudini comprese tra 19.000 e 24.000 km. La costellazione di BeiDou comprende satelliti posizionati su tre orbite distinte: l'orbita terrestre geostazionaria (Geostationary Earth Orbit, GEO); l'orbita geosincrona inclinata (Inclined Geosynchronous Orbit, IGSO) e l'orbita media.

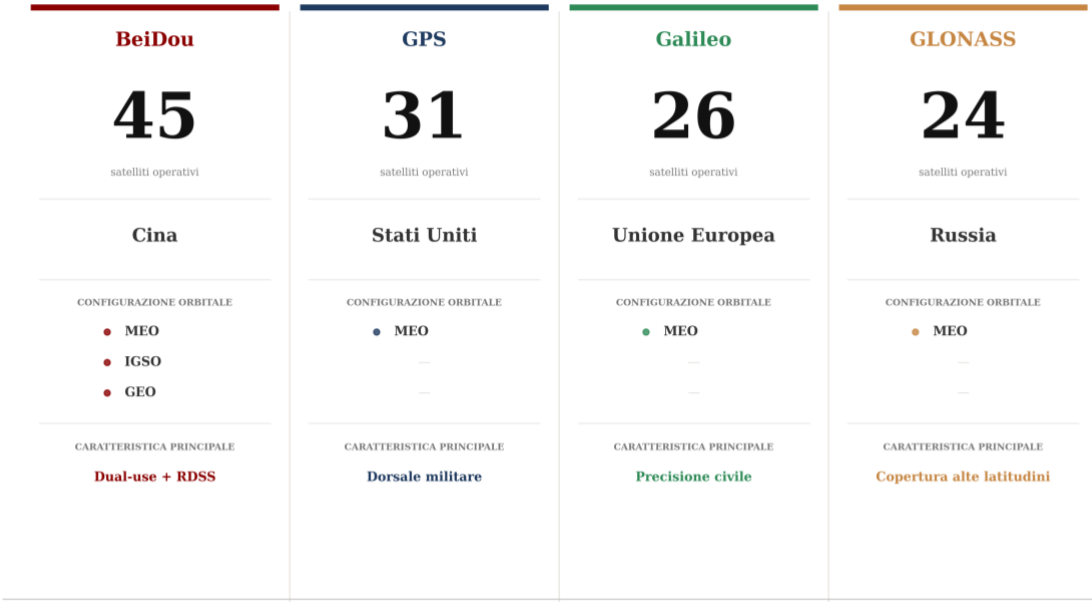

Figura 4. Flotte satellitari GNSS globali a confronto: dimensione operativa dei quattro sistemi globali (2024).

Fonte: elaborazione dell'autore su dati da molteplici fonti.[73]

Il posizionamento *sui generis* della costellazione cinese si traduce in vantaggi operativi concreti. La combinazione delle tre orbite consente a BeiDou di operare sia come sistema di navigazione passivo standard (RNSS), analogamente agli altri GNSS, sia di integrare capacità di determinazione radio attiva (RDSS) attraverso i satelliti geostazionari. Tale architettura ibrida permette, in determinate condizioni, una riduzione del tempo di acquisizione iniziale del segnale (TTFF) e una maggiore disponibilità di satelliti visibili, soprattutto nella regione Asia-Pacifico. In aggiunta, la distribuzione multi-orbita contribuisce ad aumentare la resilienza del sistema rispetto a interferenze e jamming, pur senza eliminarne la vulnerabilità, e supporta servizi di sincronizzazione temporale altamente precisi. Oggi, Pechino dispone dell'unico sistema GNSS con copertura globale a integrare in modo sistemico queste diverse componenti orbitali e funzionali.[74]

Dunque, BeiDou è la rappresentazione fattuale dello sviluppo tecnologico cinese e delle sue prerogative d'autonomia strategica, *condicio sine qua non* per svincolarsi da dipendenze esterne e sostenere una proiezione di potenza credibile.

[73] National Coordination Office for Space-Based Positioning, Navigation, and Timing; "Space Segment". Link. Sewall, *China's BeiDou: New Dimensions of Great Power Competition*. Link. European GNSS Service Centre (GSC); "Constellation Information – Galileo System Status"; GSC. Link. Information and Analysis Center for Positioning, Navigation and Timing (IAC); "GLONASS Constellation Status"; IAC; marzo 2026. Link.

[74] Jiang, Yi; Zhang, Shufang; Zhao, Huakai; *BeiDou Navigation Satellite System: Maritime Applications*; Springer Nature; 2025; pp 14-19, 99-109.

BeiDou non è solo questo. È anche – e forse soprattutto – uno strumento di influenza geopolitica. Ogni paese che adotta BeiDou come infrastruttura critica adotta contestualmente chip cinesi, standard tecnici cinesi, reti di aggiornamento gestite dalla Repubblica Popolare Cinese. La dipendenza che ne deriva è sistemica. È ciò che la letteratura strategica chiama **Standard Power**, e che costituisce il nucleo del paragrafo che segue.

3.4 Standard Power

Con lo Standard Power usciamo dallo schema descritto finora – conflitto, dottrine militari, dati nel contesto bellico. Questo rappresenta per antonomasia il soft power, categoria teorizzata dal politologo Joseph Nye Jr.: «la capacità di ottenere ciò che si desidera attraverso l'attrazione piuttosto che tramite coercizione o pagamenti».[75]

Lo Standard Power si costruisce attraverso **infrastrutture**, **standard tecnici** e **dipendenze** che si sedimentano nel tempo fino a diventare irreversibili. Una logica perfettamente conciliabile con la pazienza strategica cinese. Dove l'Occidente ragiona per mandati elettorali, **Pechino programma per decenni**. Il consenso è una variabile irrilevante, mentre il tempo un alleato strutturale.

Il meccanismo è strutturalmente semplice. Un paese in via di sviluppo riceve offerte di infrastruttura cinese: stazioni di riferimento CORS, terminali BeiDou, sistemi di monitoraggio agricolo o idroelettrico. Le condizioni sono economicamente vantaggiose, spesso nel quadro della ***Belt and Road Initiative*** o della ***Digital Silk Road***. L'adozione appare una scelta tecnica neutrale.

Nondimeno, ogni stazione installata richiede aggiornamenti software gestiti da Pechino. Ogni terminale integra chip cinesi con standard proprietari. Ogni rete di monitoraggio genera dati che transitano attraverso infrastrutture sotto controllo cinese. Per i leader dei paesi in via di sviluppo è quindi difficile rifiutare infrastrutture scontate e opportunità di sviluppo economico, anche con la consapevolezza di legare quell'infrastruttura ai segnali cinesi comportando una riduzione di sovranità.

BeiDou è uno dei casi più emblematici di questa strategia applicata al dominio satellitare. La sua diffusione non segue una logica puramente geografica, bensì si articola **lungo direttrici funzionali integrate** (vedi Figura5). **Una prima direttrice coincide con lo spazio della *Belt and Road Initiative***, all'interno del quale BeiDou opera come livello abilitante per infrastrutture fisiche già realizzate, garantendo servizi di **navigazione**, **sincronizzazione** e **supporto logistico**.

Una seconda direttrice interessa il Sud-est asiatico, dove l'influenza cinese si traduce in una progressiva integrazione dei sistemi di navigazione nei **settori civile**, **commerciale** e, in alcuni casi, **dual-use**.

La terza direttrice è rappresentata dall'Africa, dove l'ecosistema infrastrutturale è già fortemente permeato dalla presenza cinese. In questo contesto, il sistema satellitare si aggiunge a **porti**, **ferrovie** ed **energia**, costituendone un'estensione funzionale, contribuendo a consolidare una dipendenza tecnologica e operativa.

L'espansione avviene tipicamente in modo graduale, spesso preceduta da programmi di cooperazione scientifica, formazione tecnica e installazione di stazioni a terra , che fungono da meccanismi di ingresso nel sistema.

L'espansione internazionale di BeiDou segue una traiettoria progressiva e strutturata. In primo luogo, la Cina inserisce il sistema in cornici diplomatiche multilaterali, come dimostrano il *China-Africa BeiDou Cooperation Forum* (2021) o l'accordo bilaterale con l'Argentina nel 2020,[76] presentandolo come bene pubblico per lo sviluppo. Su questa base politica si innesta una fase di formazione e trasferimento di

[75] Nye, Joseph S. Jr.; *Soft Power: The Means to Success in World Politics*; "Preface"; PublicAffairs; 2004.
[76] Baar, Jemima; "BeiDou and Strategic Advancements in PRC Space Navigation"; *China Brief*, vol. 24, n. 5; Jamestown Foundation; 2024. Link.

conoscenza, attraverso centri dedicati: ne è un esempio il *China–Arab States BeiDou/GNSS Center in Tunisia* (2018) e i programmi di borse di studio rivolti a tecnici e decisori locali.[77]

L'integrazione prosegue poi tramite progetti pilota settoriali, come il monitoraggio dei disastri in Cambogia, **Laos** e **Myanmar** o le applicazioni agricole sviluppate con la Russia, che rendono tangibili i benefici del sistema e ne favoriscono la diffusione. Il passaggio critico avviene con l'installazione di **infrastrutture fisiche**, in particolare le stazioni CORS (Continuously Operating Reference Stations): esempi emblematici sono le 30 stazioni realizzate in **Uganda** o il piano per 220 stazioni in **Thailandia**, che abilitano un posizionamento ad alta precisione e generano una dipendenza tecnica difficilmente reversibile.[78]

Su questa base, BeiDou viene progressivamente integrato nei settori critici, sostenuto anche dal riconoscimento internazionale da parte di organismi come IMO e ICAO, che ne legittimano l'uso nei trasporti globali. Infine, nei casi di cooperazione più avanzata, l'integrazione si estende al dominio militare: l'accordo con il **Pakistan** per l'accesso al segnale criptato e l'impiego nei sistemi d'arma (Raad II, Babur, JF-17) rappresenta il livello più elevato, in cui **la dipendenza tecnologica si trasforma in dipendenza strategica**.[79]

Nella Figura 5 si è tentato di rappresentare graficamente questa traiettoria, classificando i paesi non in base a una semplice adesione al sistema, ma secondo il grado prevalente di integrazione lungo le diverse fasi del processo. La mappa tenta di fornire lettura dinamica della diffusione di BeiDou, evidenziando quattro livelli d'adozione: da forme di cooperazione tecnica fino a livelli di integrazione infrastrutturale e, nei casi più avanzati, strategico-militare. In tal senso, la distribuzione geografica riflette non solo la presenza del sistema, ma soprattutto la profondità della dipendenza generata.

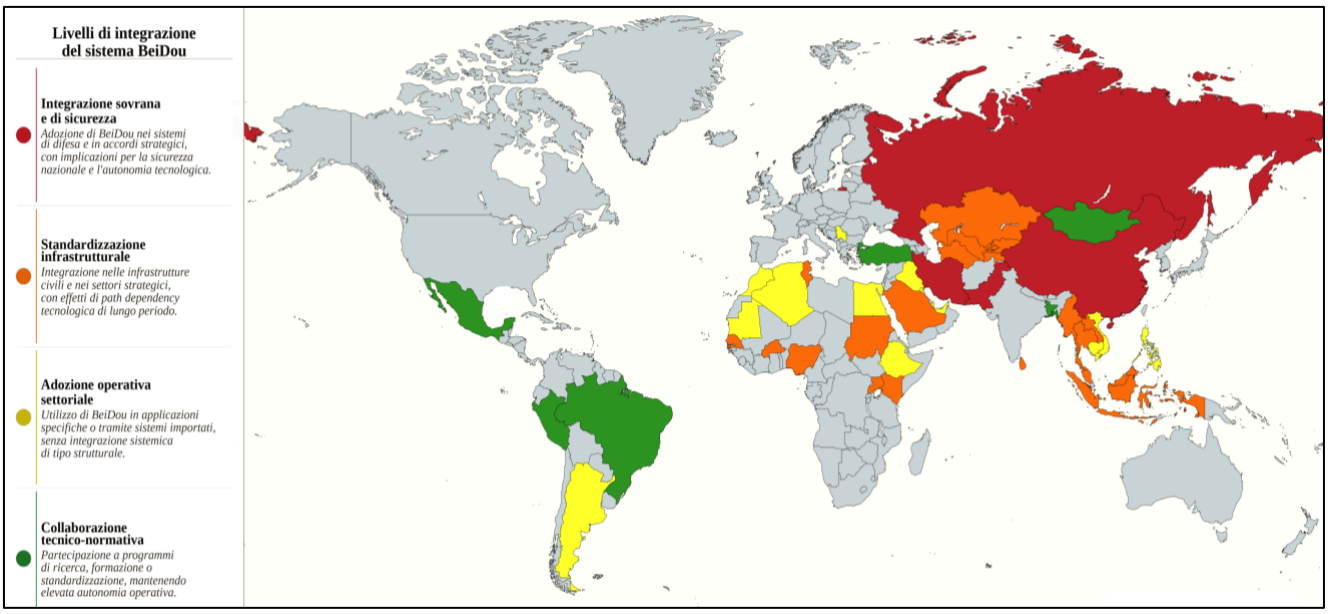

Figura 5. La geografia della dipendenza da BeiDou: distribuzione globale per livello di integrazione.

Fonte: elaborazione dell'autore su dati da molteplici fonti.[80]

[77] Lin, Luzhou; "China and Arab States Promote BeiDou via Space Silk Road"; *China Daily*; 2025. Link.
[78] Pollpeter, Kevin; Tsai, Tsun-Kai; *To Be More Precise: BeiDou, GPS, and the Emerging Competition in Satellite-Based PNT*; CNA; China Aerospace Studies Institute, Air University; 2024. Link.
[79] Lalwani, Sameer P.; *A Threshold Alliance: The China-Pakistan Military Relationship*; Special Report n. 517; United States Institute of Peace (USIP); 2023. Link.
[80] Pollpeter, Kevin; "To Be More Precise: The Beidou Satellite Navigation and Positioning System"; *China Brief*, vol. 7, n. 10; Jamestown Foundation; 2007. Link. Pollpeter; *To Be More Precise: BeiDou, GPS, and the Emerging Competition in Satellite-Based PNT*. Link. L'Argentina è classificata come "adozione operativa settoriale" (giallo) sulla base dell'accordo con la Cina del 2020. Tuttavia, con il governo di Javier Milei, è in atto un cambiamento di postura. L'intero quadro va quindi considerato dinamico e in evoluzione.

Segue poi la cooperazione con la **Russia**, che si distingue nettamente dalle altre direttrici per ratio e finalità. Questa, come nessuna tra le precedenti, mira a costruire un'integrazione tra pari in chiave esplicitamente revisionista. Aumentare precisione, copertura e resilienza, sono gli obiettivi dell'interoperabilità tra GLONASS e BeiDou. L'installazione di stazioni di monitoraggio reciproche consolida questa architettura condivisa, mentre in ambito militare l'integrazione rafforza navigazione, targeting e coordinamento di droni e missili. Nel complesso, non si tratta di un rapporto asimmetrico, ma della costruzione di un'infrastruttura alternativa che riflette lo sfaldamento dell'ordine internazionale e si configura come espressione concreta di un revisionismo tecnologico anti-occidentale.[81]

Infine, vi è **l'Iran**. Il regime islamico offre il banco di prova più eloquente delle capacità analizzate in questo capitolo, per quanto parziale e non sistematizzabile. Da poco più di un mese, CETC e BeiDou sono usciti dal dominio della teoria ed entrati in quello della realtà operativa. La verifica sotto fuoco contro l'egemone statunitense. Disputato e messo in discussione, quest'ultimo è ancora il termine di paragone reale di qualsiasi ambizione tecnologico-militare di Pechino.

3.5 L'Iran come laboratorio bellico

Prima di entrare nel dettaglio delle dinamiche belliche è necessario soffermarsi sulla relazione tra la Cina e la Repubblica Islamica dell'Iran. Si tratta di un rapporto di lunga data, rafforzato dall'instaurazione del regime degli Ayatollah: Pechino abbandonò il sostegno ai partiti comunisti iraniani per posizionarsi come attore favorevole al nuovo status quo regionale. Seguirono gli embarghi occidentali, che la Cina capitalizzò rapidamente. Il nuovo regime fu spinto a fare affidamento su fornitori di armi non occidentali, tra cui Pechino stessa, che fornì all'Iran i missili Silkworm contribuendo all'addestramento dei membri del Corpo delle Guardie della Rivoluzione Islamica (IRGC) al loro utilizzo.[82]

Con l'isolamento internazionale e una Cina economicamente sempre più emancipata, si è sviluppata una dipendenza asimmetrica. **L'Iran è molto più dipendente da Pechino, suo principale partner commerciale, di quanto questo non lo sia da Teheran**. La dimensione energetica ne è la misura più emblematica: le esportazioni iraniane di greggio sono indirizzate per l'80-90% verso la Cina, che ne riceve il 14% del proprio fabbisogno importato.[83]

In tal senso, la **partnership strategica** venticinquennale avviata nel 2021 fornisce il quadro formale entro cui leggere questa relazione. L'accordo prevede – tra i tanti punti – una stretta collaborazione militare che verte su addestramento congiunto, ricerca e sviluppo, cooperazione nell'intelligence e costruzione di infrastrutture. Pechino naviga tuttavia una tensione strutturale: da un lato i benefici della cooperazione economica nel quadro della *Belt and Road Initiative*, dall'altro la pressione a tradurre quella cooperazione in impegno militare esplicito. Una scelta non priva di costi, sotto gli occhi di attori regionali diffidenti e di Washington.[84]

È un'ambiguità strategica deliberata. La Cina vuole il dividendo iraniano senza portarne il rischio geopolitico. È anche per questa ragione che il presente paragrafo avrà necessariamente carattere esplorativo. Le fonti disponibili sono prevalentemente occidentali – intelligence americana, centri studi israeliani, reportistica specializzata – poiché Pechino mantiene un profilo volutamente basso su questa cooperazione e non produce documentazione pubblica verificabile. A ciò si aggiungono due ulteriori limiti: l'opacità strutturale dei sistemi CETC e BeiDou in contesto militare, e la vicinanza temporale alle operazioni, che rende qualsiasi analisi necessariamente parziale. Tra qualche tempo sapremo di più. Per ora, cerchiamo di ricapitolare quanto

[81] Kolodii, Roman; Pili, Giangiuseppe; Crawford, Jack; *Hi-Tech, High Risk? Russo-Chinese Cooperation on Emerging Technologies*; Royal United Services Institute (RUSI); 2024. Link.
[82] Mackenzie, Peter; *A Closer Look at China-Iran Relations: Roundtable Report*; CNA; 2010. Link.
[83] García-Herrero, Alicia; "What the War in Iran Means for China"; Analysis 06/2026; *Bruegel*; 2026. Link.
[84] International Institute for Iranian Studies (Rasanah); *The Iran-China 25-Year Comprehensive Strategic Partnership: Challenges and Prospects*; Rasanah – International Institute for Iranian Studies; 2021. Link.

disponibile in relazione al ruolo dei due strumenti cinesi analizzati nel presente capitolo nel primo mese di combattimento.

In questa finestra, la tecnologia cinese ha probabilmente avuto un ruolo significativo, sebbene difficilmente quantificabile. Più che singoli trasferimenti di sistemi, le evidenze disponibili avvicinano l'ipotesi di **moduli riconducibili a un'architettura integrata di sorveglianza e targeting sviluppata da CETC**. I **radar** delle famiglie YLC e JY rappresenterebbero il livello di rilevamento, potenzialmente integrato – almeno sul piano funzionale – con sistemi di navigazione satellitare (BeiDou), capacità di guerra elettronica e processi di data fusion.

In un livello più avanzato, alcune fonti suggeriscono la presenza – o quantomeno la valutazione operativa – di radar a bassa frequenza di derivazione cinese, come il **JY-27A o il YLC-8B**.[85] Tali indicazioni, pur convergenti, non risultano confermate da evidenze indipendenti e devono essere interpretate con cautela, in un contesto caratterizzato da scarsa trasparenza e frequente ricorso a canali informativi indiretti.

Questi sistemi, operanti rispettivamente in **banda VHF e UHF**, sono progettati per degradare il vantaggio stealth attraverso una maggiore probabilità di rilevamento iniziale.[86] La plausibilità della presenza di tali sistemi è rafforzata da evidenze open-source che documentano l'esportazione e l'impiego operativo di radar cinesi in contesti mediorientali altamente contestati.[87]

L'episodio del 19 marzo 2026, relativo al danneggiamento di un velivolo **F-35** statunitense, offre un indizio operativo di particolare interesse. Mentre fonti iraniane hanno rivendicato l'ingaggio, il CENTCOM ha confermato unicamente l'atterraggio di emergenza del velivolo, senza attribuirne pubblicamente le cause.[88]

Alcune ricostruzioni riconducono il danneggiamento all'impiego di un sistema a corto raggio di tipo Majid, basato su guida infrarossa.[89] Più che contraddire l'ipotesi di un'architettura multilivello, tale ricostruzione appare coerente con una dinamica operativa in cui il rilevamento iniziale e il cueing – potenzialmente supportati da sensori radar o passivi – confluiscono in un ingaggio terminale affidato a sistemi IR, meno vulnerabili alle contromisure elettroniche e particolarmente adatti a operare contro piattaforme a bassa osservabilità.

Il ricorso a sensori passivi elettro-ottici e infrarossi è del resto coerente con un approccio volto a ridurre la vulnerabilità alle operazioni di soppressione delle difese aeree (SEAD): sistemi che non emettono segnali elettromagnetici propri risultano strutturalmente più difficili da localizzare e neutralizzare.[90] In questo senso, l'integrazione di tecnologie o logiche operative riconducibili al modello cinese appare plausibile. La dottrina INEW attribuisce infatti valore centrale alla **combinazione di capacità passive e attive all'interno di architetture distribuite di rilevamento, guerra elettronica e comando**.

Al di là della verifica fattuale dell'evento, il caso evidenzia una dinamica più ampia: la crescente efficacia di architetture multilivello di rilevamento e tracciamento, in grado di degradare, pur senza annullare, il vantaggio stealth. In tale configurazione, anche radar a bassa frequenza, inclusi quelli di produzione CETC, possono contribuire alla fase iniziale di **detection**, alimentando una catena informativa che si integra con sensori passivi e sistemi di targeting in una logica operativa distribuita.

---

[85] Helmy, Nadia; "How China Aims to Block Mossad Operations in Iran"; *Modern Diplomacy*; 2026. Link. Kasapoğlu, Can; *Assessing Defense Cooperation Between Iran and China in the Wake of the 12-Day War – MENA Defense Intelligence Digest*; Hudson Institute; 2025. Link. Litnarovych, Vlad; "China Reportedly Armed Iran With Secret Radar Capable of Tracking Stealth Jets"; *United24 Media*; 2026. Link.
[86] Hundman, Eric; *China's Air Defense Radar Industrial Base*; BluePath Labs / China Aerospace Studies Institute, Air University; 2025; p.9. Link.
[87] ImageSatIntl; post su X (già Twitter); gennaio 2019. Link.
[88] Britzky, Haley; Liebermann, Oren; "US F-35 Damaged by Suspected Iranian Fire Makes Emergency Landing, Sources Say"; *CNN*; 2026. Link.
[89] al-Zein, Abbas; "Iran Strikes at the Myth of US Air Supremacy"; The Cradle; 2026. Link.
[90] Liang, Rui; Liu, Xuanzun; "Iran Says It Hit an F-35; Chinese Expert Analyzes How Iran Could Have Struck It Using Infrared Detection, Breaking US Stealth Myth"; *Global Times*; 2026. Link.

DOMINIO	CONTRIBUTO CINESE	VALUTAZIONE	CONFIDENZA
Rilevamento (Radar)	Export sistemi radar (famiglie YLC/JY) *Diffusione know-how dual-use (CETC)*	*Presente / strutturale*	HIGH
Sensori passivi (EO/IR, EW)	Tecnologie EO/IR e logica INEW *Integrazione passive-active sensing*	*Operativamente consistente*	MEDIUM–HIGH
C2 & Data Fusion	Architetture distribuite multi-sensore *Compatibili con design CETC*	*Strutturalmente plausibile ma opaco*	MEDIUM
PNT (BeiDou)	Accesso a GNSS alternativo *Ridondanza rispetto al GPS*	*Abilitante strategico per resilienza e targeting*	MEDIUM–HIGH
Targeting	Integrazione PNT + sensori *Maggiore stabilità della kill chain*	*Effetto operativo osservabile*	MEDIUM–HIGH
Delivery (missili/droni)	Influenza indiretta (componenti, logiche progettuali) *Non core*	*Limitata ma plausibile*	MEDIUM

Figura 6. Contributo cinese alla kill chain iraniana: valutazione per domini operativi (MCF–BeiDou–CETC).

Fonte: elaborazione dell'autore sulla base di OSINT e letteratura specialistica (cfr. §3.5 fonti ivi richiamate).

Se i radar e i sensori passivi costituiscono i livelli di rilevamento e tracciamento, il passaggio successivo riguarda la **trasformazione di tali informazioni in capacità di targeting preciso**. Qui, il sistema di navigazione satellitare BeiDou assume un ruolo potenzialmente abilitante.

In quest'ottica, è più agevole comprendere l'evoluzione dottrinaria e tecnologica delle capacità missilistiche iraniane. Il primo impiego transfrontaliero del 2017 evidenziò limiti significativi, con missili che mancarono i bersagli di diverse centinaia di metri. Già nel 2019, tuttavia, l'attacco contro le installazioni saudite di Abqaiq e Khurais mostrò una capacità di strike integrato, mentre nel 2020 i missili balistici impiegati contro la base di Ayn al-Asad colpirono con elevata precisione bersagli puntuali.[91]

Il confronto tra la guerra dei dodici giorni del giugno 2025 e il conflitto in corso non consente di misurare con precisione un **salto netto del CEP**[92] **dei vettori iraniani**, ma evidenzia una loro **trasformazione qualitativa**. Nel 2025, l'Iran ha fatto ricorso a salve massicce – più di 500[93] – per compensare limiti di accuratezza e alti tassi di intercettazione; nel 2026, pur sotto intensa pressione, continua a generare effetti operativi migliori con volumi ridotti, suggerendo un miglioramento della catena di targeting più che della sola precisione intrinseca del vettore.

Alcuni episodi operativi risultano coerenti con tale dinamica. In particolare, sono stati riportati impatti con elevata precisione su target puntuali, tra cui assetti aerei non protetti – come droni Reaper parcheggiati[94] – e infrastrutture radar in contesti operativi del Golfo.[95] Tali eventi, pur non consentendo inferenze conclusive sul

[91] Ruhe, Jonathan; Cicurel, Ari; *Iran's Evolving Missile and Drone Threat*; JINSA Gemunder Center for Defense and Strategy; 2026; pp. 11-12. Link.
[92] Circular Error Probable, ossia il raggio entro cui cade il 50% degli impatti.
[93] Marzbanmehr, Arash; "Twelve Days of Inferno: The Cost of Opening Pandora's Box"; Al Jazeera Centre for Studies; 2025. Link.
[94] Martinez, Luis; "More Than a Dozen $16M Reaper Drones Have Been Destroyed in Iran Operations, US Officials Say"; *ABC News*; 2026. Link.
[95] Beaule, Victoria; Charalambous, Peter; Inal, Kerem; "US and Allied Radar Sites in the Middle East Struck at Least 10 Times: Visual Analysis"; *ABC News*; 2026. Link.

CEP dei vettori impiegati, suggeriscono una crescente efficacia nella fase terminale della kill chain, verosimilmente legata a una migliore integrazione tra rilevamento, tracciamento e targeting.

In questo quadro, il contributo di infrastrutture **PNT** (**Positioning, Navigation and Timing**) avanzate assume una rilevanza sistemica. Più che incrementare in modo lineare la precisione del singolo vettore, l'accesso a sistemi GNSS alternativi e più resilienti consente di stabilizzare l'intero processo di targeting, riducendo la vulnerabilità alle interferenze elettroniche e migliorando la coerenza dell'ingaggio.

Il salto iraniano non risiede dunque nel singolo missile, ma nella **crescente integrazione della catena operativa**. Le tecnologie come BeiDou costituiscono un fattore abilitante in linea con l'evoluzione osservata.

A prescindere dalle modalità e dall'intensità con cui il Corpo delle Guardie della Rivoluzione Islamica abbia impiegato i sistemi analizzati, il punto rilevante è un altro: **la Cina osserva, apprende e adatta**. Il teatro mediorientale rappresenta un ulteriore contesto in cui gli Stati Uniti espongono dottrine, architetture e sistemi in condizioni operative reali, offrendo a Pechino un **flusso continuo di evidenze empiriche**.

Al contrario, la Cina resta un attore opaco, il cui ultimo conflitto su larga scala risale al 1979, ma che nel frattempo ha sviluppato un approccio sistemico fondato sull'integrazione tra domini. In un eventuale confronto su Taiwan – ipotesi che impone cautela ma non può essere esclusa – lo scontro con Washington avverrebbe su un piano strutturalmente diverso rispetto ai conflitti del passato.

Più che la superiorità del singolo sistema d'arma, **saranno determinanti il controllo dello spettro elettromagnetico, la coerenza dell'integrazione software e la resilienza delle infrastrutture satellitari**. In questo senso, il caso iraniano ci dà conferma che la guerra contemporanea premia la coerenza dell'architettura più della perfezione del vettore.

3.6 Limiti e vulnerabilità

Il capitolo ha fin qui descritto un'architettura coerente e ambiziosa. Resta da verificare se sia anche solida. Diverse vulnerabilità strutturali, tecnologiche e operative, ne condizionano la credibilità sul lungo termine.

Un primo limite è proprio legato a Taiwan che ospita l'unica fonderia al mondo in grado di produrre i chip di cui Pechino ha bisogno. CETC progetta e integra semiconduttori per terminali BeiDou, sistemi radar e piattaforme C4ISR, ma non produce in proprio i nodi litografici più avanzati. Nove su dieci provengono dall'isola "ribelle".[96] La Cina dipende ancora da TSMC per i chip sotto i 7 nanometri. SMIC, il principale produttore cinese, ha dimostrato nel 2023 la capacità di fabbricare chip a 7nm utilizzando litografia DUV con tecniche di multi-patterning, ma i rendimenti (yield)[97] restano bassi e la **produzione su scala industriale non è comparabile**.[98]

Il collo di bottiglia è a monte: le macchine per la litografia a ultravioletto estremo (EUV), indispensabili per i nodi sotto i 5nm, sono monopolio della olandese **ASML** e soggette a restrizioni all'export imposte dagli Stati Uniti, dai Paesi Bassi e dal Giappone a partire dal 2023.[99] Il paradosso strategico è evidente: in uno scenario di conflitto su Taiwan, Pechino rischierebbe di distruggere o rendere inaccessibile la fonderia da cui dipende. L'autosufficienza dichiarata nel settore dei semiconduttori resta, ad oggi, un obiettivo politico e meno una

[96] U.S. International Trade Administration; "Taiwan – Semiconductors Including Chip Design for AI"; *Taiwan Country Commercial Guide*; U.S. Department of Commerce; 2025. Link.
[97] Lo yield indica la percentuale di chip funzionanti sul totale dei chip fabbricati su un singolo wafer di silicio. Nei processi litografici avanzati, dove i circuiti misurano pochi nanometri, anche minime impurità o imprecisioni rendono inutilizzabile il chip. Uno yield basso significa costi unitari elevati e impossibilità di produrre su scala industriale. TSMC raggiunge yield superiori all'80% nei nodi a 7nm; le stime disponibili per SMIC sullo stesso nodo sono significativamente inferiori.
[98] Shivakumar, Sujai; Wessner, Charles; Howell, Thomas*; Balancing the Ledger: Export Controls on U.S. Chip Technology to China; Center for Strategic and International Studies* (CSIS); 2024. Link.
[99] Ibidem.

realtà industriale. Il tema della filiera dei semiconduttori meriterebbe un approfondimento a sé, che esula dall'oggetto di questo capitolo. Il limite, tuttavia, resta strutturale e va tenuto in conto.

La seconda vulnerabilità è intrinseca nella centralità di BeiDou stesso, e vale per qualsiasi costellazione GNSS. Il capitolo ha evidenziato come la configurazione multi-orbita ne aumenti la resilienza rispetto ad altri sistemi GNSS, ma resilienza non significa invulnerabilità. **I satelliti in orbita sono esposti a minacce cinetiche (ASAT) e non cinetiche (jamming, spoofing, laser ad alta energia**). Gli Stati Uniti e la Russia dispongono di capacità ASAT dimostrate; lo stesso vale per la Cina, che nel 2007 ha distrutto un proprio satellite con un missile, provando indirettamente che la propria costellazione è vulnerabile allo stesso tipo di attacco.[100] Sul piano elettronico, le capacità statunitensi di jamming GNSS – testate in esercitazioni e documentate da fonti aperte – rappresentano una minaccia diretta alla catena di targeting cinese descritta nella sezione 3.2.[101] **Se BeiDou degrada, la kill chain si spezza**.

Vi è poi un limite meno quantificabile ma non meno rilevante: l'assenza di verifica operativa**. L'ultimo conflitto su larga scala combattuto dalla Cina risale al 1979**. Nessun ufficiale del PLA in servizio attivo ha esperienza diretta di combattimento. Le dottrine INEW, i Digital Twins, l'integrazione C4ISR sono stati **concepiti, sviluppati e testati in esercitazioni e simulazioni** – mai sotto il fuoco di un avversario in grado di degradare lo spettro, accecare i satelliti e colpire i nodi di comando. Il confronto con l'ecosistema occidentale è, su questo piano, sbilanciato: Palantir è stata validata sul campo in Ucraina, Paragon in operazioni di intelligence documentate. La tecnologia cinese, per quanto sofisticata, non ha ancora superato questo tipo di stress-test. L'Iran ne offre un'indicazione parziale, indiretta e non generalizzabile.

A questo si lega il problema dell'interoperabilità reale. La fusione civile-militare presuppone che sistemi prodotti da aziende diverse – CETC, CASC, CASIC, Norinco – funzionino come un organismo unico in condizioni operative degradate: comunicazioni contestate, catena di comando sotto attacco, dati parziali o corrotti. Gli standard NATO sono stati collaudati in decenni di esercitazioni congiunte tra forze armate di paesi diversi. **La Cina ha testato la propria integrazione solo in esercitazioni nazionali e in simulazioni**. La distanza tra la coerenza dell'architettura sulla carta e la sua tenuta sotto pressione reale è un'incognita che nessuna esercitazione può colmare del tutto.

Infine, il modello stesso che ne costituisce la forza porta con sé un limite strutturale. La **direzione centralizzata garantisce coerenza e pazienza strategica, ma sopprime la "distruzione creativa"**[102] che in Occidente genera innovazioni di rottura. L'iniziativa individuale, il dissenso tecnico, la competizione tra attori indipendenti sono variabili che il sistema cinese tende a comprimere per principio. Il risultato è un modello efficace nell'ingegneria incrementale e nell'integrazione di sistemi esistenti, ma la cui **capacità di produrre salti di paradigma resta da dimostrare.**

[100] United States Space Force; "Space Threat Fact Sheet"; U.S. Space Force; 2025. Link.
[101] Capaccio, Anthony; "US Space Force to Use Three Weapons to Jam Chinese Satellites via Remote Control"; *Bloomberg*; 2025. Link.
[102] Il concetto di distruzione creativa (o *distruzione creatrice*) è formulato da Schumpeter, Joseph A.; *Capitalismo, Socialismo, Democrazia*; ETAS LIBRI; 1977; cap. VII. Schumpeter identifica nell'iniziativa individuale e nella competizione tra attori indipendenti il motore dell'innovazione di rottura. Il modello cinese dispone delle grandi strutture necessarie a sostenerla, ma ne comprime la dinamica competitiva interna.

Bibliografia

Libri

Davis, Elizabeth; *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*; 2021. DOI: 10.5771/9781538149683.

Evron, Yoram; Bitzinger, Richard A.; *The Fourth Industrial Revolution and Military–Civil Fusion: A New Paradigm for Military Innovation?*; Cambridge University Press; 2023.

Jiang, Yi; Zhang, Shufang; Zhao, Huakai; *BeiDou Navigation Satellite System: Maritime Applications*; Springer Nature; 2025.

Nye, Joseph S. Jr.; *Soft Power: The Means to Success in World Politics*; PublicAffairs; 2004.

Qiao, Liang; Wang, Xiangsui; *Unrestricted Warfare: China's Master Plan to Destroy America*; Shadow Lawn Press; 2017 [ed. or. PLA Literature and Arts Publishing House, 1999].

Schumpeter, Joseph A.; *Capitalismo, Socialismo, Democrazia*; ETAS LIBRI; 1977.

Sharma, Rohit; *Cybersecurity in Israel*; 2025.

Tan, Shusen; *GNSS Systems and Engineering: The Chinese BeiDou Navigation and Position Location Satellite*; John Wiley & Sons / National Defense Industry Press; 2018.

Report istituzionali e think tank

Bienvenue, E.; Kelton, M.; Rogers, Z.; Sullivan, M.; Ford, M.; Private Tech Companies, the State, and the New Character of War; Carnegie Endowment; 2025. https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies

Béraud-Sudreau, Lucie; Nouwens, Meia; *Weighing Giants: Taking Stock of the Expansion of China's Defence Industry*; Defence and Peace Economics, vol. 32, n. 2; 2021; pp. 151–177.

García-Herrero, Alicia; "What the War in Iran Means for China"; Analysis 06/2026; Bruegel; 2026. https://www.bruegel.org/analysis/what-war-iran-means-china.

Heginbotham, Eric; Nixon, Michael; Morgan, Forrest E.; Heim, Jacob L.; Hagen, Jeff; Li, Sheng; Engstrom, Jeffrey; Libicki, Martin C.; DeLuca, Paul; Shlapak, David A.; Frelinger, David R.; *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*; RAND Corporation; 2015.

Hundman, Eric; *China's Air Defense Radar Industrial Base*; BluePath Labs / China Aerospace Studies Institute, Air University; 2025. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Infrastructure/2025-03-10%20Air%20Defense%20Radars.pdf?ver=n23Kh46_R--EG2y9MEQAPg%3D%3D.

International Institute for Iranian Studies (Rasanah); *The Iran-China 25-Year Comprehensive Strategic Partnership: Challenges and Prospects*; Rasanah – International Institute for Iranian Studies; 2021. https://rasanah-iiis.org/english/wp-content/uploads/sites/2/2021/04/The-Iran-China-25-Year-Comprehensive-Strategic-Partnership-Challenges-and-Prospects.pdf.

Jones, Seth G.; *Russia's Shadow War Against the West*; CSIS, Center for Strategic & International Studies; 18 marzo 2025. https://www.csis.org/analysis/russias-shadow-war-against-west.

Kasapoğlu, Can; *Assessing Defense Cooperation Between Iran and China in the Wake of the 12-Day War – MENA Defense Intelligence Digest*; Hudson Institute; 2025. https://www.hudson.org/missile-defense/mena-defense-intelligence-digest-september-2025-can-kasapoglu.

Kolodii, Roman; Pili, Giangiuseppe; Crawford, Jack; *Hi-Tech, High Risk? Russo-Chinese Cooperation on Emerging Technologies*; Royal United Services Institute (RUSI); 2024. https://www.rusi.org/explore-our-research/publications/commentary/hi-tech-high-risk-russo-chinese-cooperation-emerging-technologies.

Lalwani, Sameer P.; *A Threshold Alliance: The China-Pakistan Military Relationship*; Special Report n. 517; United States Institute of Peace (USIP); 2023. https://www.usip.org/sites/default/files/2023-03/sr-517_threshold-alliance-china-pakistan-military-relationship.pdf.

Mackenzie, Peter; *A Closer Look at China-Iran Relations: Roundtable Report*; CNA; 2010. https://www.cna.org/reports/2010/D0023622.A3.pdf.

Marczak, Bill; Scott-Railton, John; Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted; Citizen Lab Report No. 186, University of Toronto; 2025.

Marczak, Bill; Scott-Railton, John; Robertson, Kate; Perry, Astrid; Brown, Rebekah; Abdul Razzak, Bahr; Anstis, Siena; Deibert, Ron; Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations; Citizen Lab Report No. 183, University of Toronto; 2025.

Marzbanmehr, Arash; "Twelve Days of Inferno: The Cost of Opening Pandora's Box"; Al Jazeera Centre for Studies; 2025. https://studies.aljazeera.net/en/analyses/twelve-days-inferno-cost-opening-pandora%E2%80%99s-box.

McFaul, Cole; Bresnick, Sam; Chou, Daniel; *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage*; Center for Security and Emerging Technology (CSET); 2025. https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion/.

Pollpeter, Kevin; Tsai, Tsun-Kai; *To Be More Precise: BeiDou, GPS, and the Emerging Competition in Satellite-Based PNT*; CNA; China Aerospace Studies Institute, Air University; 2024. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Space/2024-05-20%20To%20Be%20More%20Precise%20-%20Beidou.pdf.

Ruhe, Jonathan; Cicurel, Ari; *Iran's Evolving Missile and Drone Threat*; JINSA Gemunder Center for Defense and Strategy; 2026. https://jinsa.org/wp-content/uploads/2026/02/Irans-Evolving-Missile-and-Drone-Threat.pdf.

Sewall, Sarah; Vandenberg, Tyler; Malden, Kaj; *China's BeiDou: New Dimensions of Great Power Competition*; Belfer Center for Science and International Affairs, Harvard Kennedy School; 2023. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/Chinas-BeiDou_V10.pdf.

Shivakumar, Sujai; Wessner, Charles; Howell, Thomas*; Balancing the Ledger: Export Controls on U.S. Chip Technology to China; Center for Strategic and International Studies* (CSIS); 2024. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

Studio della Commissione PEGA del Parlamento Europeo; *The use of Pegasus and equivalent surveillance spyware*; Parlamento Europeo; 2023. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.

Wang, Maya; *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*; Human Rights Watch; 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

Articoli e analisi giornalistiche

al-Zein, Abbas; "Iran Strikes at the Myth of US Air Supremacy"; The Cradle; 2026. https://thecradle.co/articles/iran-strikes-at-the-myth-of-us-air-supremacy.

Baar, Jemima; "BeiDou and Strategic Advancements in PRC Space Navigation"; *China Brief*, vol. 24, n. 5; Jamestown Foundation; 2024. https://jamestown.org/beidou-and-strategic-advancements-in-prc-space-navigation/.

Beaule, Victoria; Charalambous, Peter; Inal, Kerem; "US and Allied Radar Sites in the Middle East Struck at Least 10 Times: Visual Analysis"; *ABC News*; 2026. https://abcnews.com/International/us-allied-radar-sites-middle-east-struck-10/story?id=131164670.

Bergengruen, V.; "How Tech Giants Turned Ukraine Into an AI War Lab"; Time Magazine; 2024. https://time.com/6691662/ai-ukraine-war-palantir/

Booth, R.; "MPs urge UK government to halt contract giving Palantir FCA data access"; The Guardian; 2026. https://www.theguardian.com/technology/2026/mar/23/mps-urge-uk-government-halt-palantir-contract-fca

Booth, R.; "NHS deal with AI firm Palantir called into question after officials' concerns revealed"; The Guardian; 2026. https://www.theguardian.com/society/2026/feb/12/nhs-deal-with-ai-firm-palantir-called-into-question-after-officials-concerns-revealed

Britzky, Haley; Liebermann, Oren; "US F-35 Damaged by Suspected Iranian Fire Makes Emergency Landing, Sources Say"; *CNN*; 2026. https://edition.cnn.com/2026/03/19/politics/f-35-damage-iran-war.

Capaccio, Anthony; "US Space Force to Use Three Weapons to Jam Chinese Satellites via Remote Control"; *Bloomberg*; 2025. https://www.bloomberg.com/news/articles/2025-11-04/us-space-force-to-use-three-weapons-to-jam-chinese-satellites-via-remote-control.

Glosselin-Malo, E.; "Ukraine feeds sensitive military data to Palantir AI for training"; Defense News; 2026. https://www.defensenews.com/global/europe/2026/01/21/ukraine-feeds-sensitive-military-data-to-palantir-ai-for-training/

Gordon, L.; "Palantir and Airbus Extend Strategic Collaboration"; Business Wire; 2026. https://www.businesswire.com/news/home/20260210301221/en/Palantir-and-Airbus-Extend-Strategic-Collaboration

Goswami, Namrata; "The Economic and Military Impact of China's BeiDou Navigation System"; *The Diplomat*; 2020. https://thediplomat.com/2020/07/the-economic-and-military-impact-of-chinas-beidou-navigation-system/.

Helmy, Nadia; "How China Aims to Block Mossad Operations in Iran"; *Modern Diplomacy*; 2026. https://moderndiplomacy.eu/2026/01/28/how-china-aims-to-block-mossad-operations-in-iran/.

Hitchens, Theresa; "Pentagon's flagship AI effort, Project Maven, moves to NGA"; Breaking Defense; 2022. https://breakingdefense.com/2022/04/pentagons-flagship-ai-effort-project-maven-moves-to-nga/

Horowitz, Michael C.; "Artificial Intelligence and the Future of Strategic Stability"; Texas National Security Review; 2026. https://tnsr.org/roundtable/artificial-intelligence-and-the-future-of-strategic-stability/

Ignatius, David; "How the algorithm tipped the balance in Ukraine"; The Washington Post; 2022. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

Jaura, R.; "Come Palantir sta aiutando l'Ucraina nella sua guerra con la Russia"; L'Indro; 2025. https://www.lindro.eu/2025/08/27/come-palantir-sta-aiutando-l-ucraina-nella-sua-guerra-con-la-russia/

Jaura, R.; "Software on the Front Line: How Palantir Is Aiding Ukraine in Its War with Russia"; InDeptNews; 2025. https://indepthnews.net/software-on-the-front-line-how-palantir-is-aiding-ukraine-in-its-war-with-russia/.

Johnson, Craig; "Unit 8200: Producing Top Cybersecurity Talent"; Diary of a Cyber Headhunter, Substack; 2024. https://craigjohnsonr5.substack.com/p/unit-8200-producing-top-cybersecurity.

Kosoy, D.; "Palantir, the Secretive Tech Giant Shaping Ukraine's War Effort"; United 24 Media; 2025. https://united24media.com/war-in-ukraine/palantir-the-secretive-tech-giant-shaping-ukraines-war-effort-5519

Liang, Rui; Liu, Xuanzun; "Iran Says It Hit an F-35; Chinese Expert Analyzes How Iran Could Have Struck It Using Infrared Detection, Breaking US Stealth Myth"; *Global Times*; 2026. https://www.globaltimes.cn/page/202603/1357330.shtml.

Lin, Luzhou; "China and Arab States Promote BeiDou via Space Silk Road"; *China Daily*; 2025. https://www.chinadaily.com.cn/a/202511/07/WS690db158a310fc20369a3d5f.html.

Litnarovych, Vlad; "China Reportedly Armed Iran With Secret Radar Capable of Tracking Stealth Jets"; *United24 Media*; 2026. https://united24media.com/latest-news/china-reportedly-armed-iran-with-secret-radar-capable-of-tracking-stealth-jets-16960.

Lo Prete, Davide; Sposini, Alessia; "Stuxnet e oltre: la guerra "invisibile" tra Iran, Israele e Stati Uniti"; *Geopolitica.info*; 7 maggio 2021. https://geopolitica.info/stuxnet-e-oltre-la-guerra-invisibile-tra-iran-israele-e-stati-uniti/.

Martinez, Luis; "More Than a Dozen $16M Reaper Drones Have Been Destroyed in Iran Operations, US Officials Say"; *ABC News*; 2026. https://abcnews.com/Politics/dozen-16m-reaper-drones-destroyed-iran-operations-us/story?id=131163787.

Morano, Caterina Patrizia; *Cybersecurity, intrusion, detection systems e intelligenza artificiale*; Il mondo dell'Intelligence, Sistema di Informazione per la sicurezza della Repubblica; 2015. https://www.sicurezzanazionale.gov.it/data/cms/posts/513/attachments/f952b540-e8aa-4ba4-a97a-0ec51cf52ace/download/.

Moschetti, Matteo; "La macchina che sa tutto di tutti: cos'è davvero Palantir?"; Centro Analisi e Studi Italus – C.A.S.I.; 2025. https://centrostudicasi.com/la-macchina-che-sa-tutto-di-tutti-cose-davvero-palantir/

Mosley, L.; "Ukraine at 'bleeding edge' of military tech, says Palantir executive"; Bloomberg Technology; 2025. https://www.youtube.com/shorts/xYaAeQvxy10

Pollpeter, Kevin; "To Be More Precise: The Beidou Satellite Navigation and Positioning System"; *China Brief*, vol. 7, n. 10; Jamestown Foundation; 2007. https://jamestown.org/to-be-more-precise-the-beidou-satellite-navigation-and-positioning-system/.

Shone, E.; "The great Ministry of Defence-to-Palantir pipeline"; Progressive International; 2026. https://progressive.international/wire/2026-02-24-the-great-ministry-of-defence-to-palantir-pipeline/en/

Strout, N.; "Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up"; C4isrnet; 2021. https://www.c4isrnet.com/industry/2021/08/12/palantir-with-joint-all-domain-command-and-control-the-pentagon-is-finally-catching-up/

Toy, Staff; "US lawmakers demand info from DEA, FBI on use of Israeli spyware"; The Times of Israel; 31 dicembre 2022. https://www.timesofisrael.com/us-lawmakers-demand-info-from-dea-fbi-on-use-of-israeli-spyware/

Xie, Jun; "BeiDou Navigation Satellite System in 2024"; GPS World; 2024. https://www.gpsworld.com/beidou-navigation-satellite-system-in-2024/.

Xinhua; "Chinese Remote Sensing Satellite Constellation to Offer Global Services"; *Xinhua News Agency*; 4 marzo 2025. http://en.sasac.gov.cn/2025/03/04/c_18928.htm.

Fonti primarie

Chinese Communist Party Central Committee; *Document Number 7: Record of the Meeting of the Standing Committee of the Politburo Concerning the Maintenance of Stability in Xinjiang*; 1996; citato in Dillon, Michael; *Xinjiang Uyghur Autonomous Region (Eastern Turkestan)*, Supplementary Memorandum; University of Durham; UK Parliament Select Committee on Foreign Affairs, Appendix 19. https://publications.parliament.uk/pa/cm199900/cmselect/cmfaff/574/574ap20.htm.

Gerasimov, Valery; *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*; trad. Robert Coalson; Military Review, gennaio-febbraio 2016. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

Documentazione istituzionale e corporate

Apple Security Engineering and Architecture; "Memory Integrity Enforcement: A complete vision for memory safety in Apple devices"; *Apple Security Research Blog*; 2025. https://security.apple.com/blog/memory-integrity-enforcement.

China Electronics Technology Group Corporation (CETC); "C4KISR – Products & Service: International Trade"; CETC. http://en.cetc.com.cn/enzgdzkj/products/ternational_trade38/c4kisr46/index.html#:~:text=CETC%2C%20a%20state%2Downed%20company,including%20land%2C%20sea%20and%20air.

China Electronics Technology Group Corporation (CETC); "使命定位 – Missione e posizionamento strategico"; CETC. https://www.cetc.com.cn/zgdk/1593037/qywh61/smdw53/index.html.

China Electronics Technology Group Corporation (CETC); “集团简介 – Profilo del Gruppo”; CETC. https://www.cetc.com.cn/zgdk/1593037/jtjj/index.html.

European GNSS Service Centre (GSC); "Constellation Information – Galileo System Status"; GSC. https://www.gsc-europa.eu/system-service-status/constellation-information.

European Space Agency / eoPortal; "China Navigation Satellite System (CNSS) – BeiDou Constellation"; eoPortal. https://www.eoportal.org/satellite-missions/cnss#beidou-3s.

ImageSatIntl; post su X (già Twitter); 2019. https://x.com/ImageSatIntl/status/1087795248762441728.

Information and Analysis Center for Positioning, Navigation and Timing (IAC); "GLONASS Constellation Status"; IAC; marzo 2026. https://glonass-iac.ru/en/cus/.

National Coordination Office for Space-Based Positioning, Navigation, and Timing; "Space Segment"; GPS.gov. https://www.gps.gov/space-segment.

National Defense University of the People's Republic of China; *Lectures on Joint Campaign Information Operations*; trad. e ed. China Aerospace Studies Institute (CASI), Air University; 2021. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-10-12%20Lectures%20on%20Joint%20Campaign%20Information%20Operations.pdf.

Palantir Platforms; Gotham; Palantir Platforms; 2026. https://www.palantir.com/platforms/gotham/

Palantir Technologies ltd.; AIP for Defense; Palantir Solutions; 2026. https://www.palantir.com/platforms/aip/defense/

Palantir Technologies ltd.; Palantir Supply Chain Solutions; Palantir Solutions; 2026. https://www.palantir.com/offerings/supply-chain

Palantir Technologies ltd.; The Ontology system; Palantir Foundry Documentation; 2026. https://www.palantir.com/docs/foundry/architecture-center/ontology-system

Palantir Technologies UK, ltd.; Palantir Platform: Gotham; Digital Marketplace; 2024. https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/801146272055049

Pew Research Center; *Measuring Religion in China – 5. Islam*; Pew Research Center; 2023. https://www.pewresearch.org/religion/2023/08/30/islam/.

Qian, Xiaohu; Wang, Lingshuo; *Wang Mingxiao: accelerare l'applicazione militare della tecnologia del gemello digitale*; China Military Online — PLA Daily; 2021. http://www.81.cn/zt/2021nzt/2021qglh/lhjs/9993836.html.

State Council Information Office of the People's Republic of China; *Xinjiang Population Dynamics and Data*; State Council Information Office; 2021. http://english.scio.gov.cn/whitepapers/2021-09/26/content_77775276_4.htm.

U.S. Department of Defense; *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*; Department of Defense; 2025. https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

U.S. International Trade Administration; “Taiwan – Semiconductors Including Chip Design for AI”; *Taiwan Country Commercial Guide*; U.S. Department of Commerce; 2025. https://www.trade.gov/country-commercial-guides/taiwan-semiconductors-including-chip-design-ai.

U.S.-China Economic and Security Review Commission; *Chapter 2, Section 2: China's Space and Counterspace Programs*; in *2015 Annual Report to Congress*; U.S.-China Economic and Security Review Commission; 2015. https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%202%20-%20China%27s%20Space%20and%20Counterspace%20Programs.pdf.

United States Space Force; “Space Threat Fact Sheet”; U.S. Space Force; 2025. https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet/.