DOPPIOZERO

Guerra: bombardate i Cloud!

Mauro Zanchi

7 Aprile 2026

L’illusione ottica della nuvola si è infranta contro la solidità brutale del cemento e la ferocia cinetica delle esplosioni belliche, rivelando che il cloud è la maschera di un’astrazione metafisica e una vulnerabile infrastruttura geolocalizzata. La retorica della dematerializzazione, che per decenni ha descritto i dati come entità fluttuanti in un etere incorporeo, è crollata nel momento in cui i data center di Amazon negli Emirati Arabi Uniti e in Bahrain sono diventati bersagli militari delle Guardie Rivoluzionarie Iraniane (IRGC). La metamorfosi del data center da asilo tecnologico a obiettivo militare di primo piano segna una discontinuità profonda nella dottrina della sicurezza globale. Il silicio è divenuto un nuovo fronte di guerra cinetica. I nodi del cloud sono oggi percepiti come estensioni fisiche delle capacità di intelligence e proiezione militare avversaria. La giustificazione addotta da Teheran – l’individuazione di questi centri come pilastri del supporto logistico e informativo degli eserciti nemici – svela come l'integrazione di modelli di intelligenza artificiale (per esempio Claude di Anthropic) nelle operazioni belliche statunitensi abbia rimosso lo scudo di neutralità civile che storicamente proteggeva tali asset.

L’impatto di questa offensiva scardina anche le certezze dei colossi tecnologici Microsoft, Google Cloud e Amazon Web Services, che alimentano l’IA fornendo la potenza di calcolo, lo spazio di archiviazione e la connessione Internet ad alta velocità necessari per addestrare i modelli più avanzati. Il termine *hyperscaler* definisce una categoria di fornitori di servizi cloud (Cloud Service Provider) dotati di un'infrastruttura di dimensioni monumentali, capace di scalare le proprie risorse in modo continuativo per rispondere a una domanda globale massiccia. Mentre un normale data center può servire centinaia o migliaia di clienti locali, un *hyperscaler* gestisce milioni di utenti simultanei e carichi di lavoro che spaziano dall'intelligenza artificiale generativa allo streaming video globale. Quando strutture che, secondo i dati IBM, ospitano almeno 5.000 server e possono estendersi su migliaia di metri quadrati (una scala che per i grandi distretti raggiunge circa i 92.900 chilometri quadrati) diventano bersagli di droni e missili,

la magnitudo del danno trascende il disservizio digitale per colpire la capacità di calcolo nazionale. Vincent Boulanin del SIPRI (Stockholm International Peace Research Institute) sottolinea che i data center sono le centrali elettriche dell'era dell'IA; senza di essi, l'addestramento dei modelli e l'elaborazione dei dati si arrestano, paralizzando sia le app bancarie, sia l'intero apparato decisionale di uno Stato. Questa vulnerabilità è accentuata dal fatto che, mentre la sicurezza perimetrale terrestre è tradizionalmente robusta, la protezione dello spazio aereo sopra queste fabbriche di dati è rimasta colpevolmente trascurata. Fino a oggi, la priorità delle difese terra-aria era riservata a raffinerie o impianti di desalinizzazione, ma l'evento dell'1 marzo impone una revisione delle gerarchie delle infrastrutture critiche. La risposta tecnica di Amazon, basata sulla suddivisione in zone di disponibilità, ha mostrato una resilienza parziale, ma l'interruzione prolungata dei servizi documentata fino all'11 marzo evidenzia i limiti della migrazione dei dati in contesti di guerra aperta. L'impossibilità legale di spostare determinate informazioni fuori dai confini nazionali di Bahrein o Emirati rende il collasso fisico di un centro un punto di non ritorno per la sovranità informativa locale. Il futuro di questi asset sembra ora oscillare tra la diplomazia internazionale e l'irrigidimento militare. Più voci, dopo il bombardamento dei data center di Amazon, propongono di classificare i data center come infrastrutture critiche da proteggere tramite scudi missilistici nazionali, simili all'Iron Dome israeliano, spostando la difesa dal piano del codice a quello dei vettori d'intercettazione. Ora, però, l'instabilità dell'area del Golfo rischia di produrre un effetto di fuga degli investimenti, mettendo in discussione la crescita del mercato dei data center negli Emirati, che era destinata a raddoppiare i ricavi dai 3,29 miliardi di dollari del 2026 fino ai 7,7 miliardi previsti per il 2031. La fine dell'innocenza dei data center sancisce che, nel diritto internazionale, la distinzione tra infrastruttura civile e militare è ormai sbiadita dalla potenza di calcolo che esse sprigionano, rendendo ogni server un potenziale bersaglio legittimo in un conflitto post-digitale.

L'informazione è materia, occupa spazio, consuma energia e, soprattutto, è soggetta alle leggi della fisica e della geopolitica. Quando parliamo di cloud, stiamo in realtà parlando di un capannone con dei server dentro, situato su un pezzo di terra preciso, sotto la sovranità di uno Stato specifico. I sistemi di Amazon sono progettati per resistere alla perdita di una *Availability Zone*, ma l'attacco simultaneo a due zone ha provocato un collasso sistemico, che ha paralizzato banche, flussi logistici e infrastrutture vitali. Questo blackout è stata la dimostrazione che la centralizzazione dei dati nelle mani di pochi provider iperscalabili ha creato dei "single point of failure" di proporzioni continentali. Milioni di persone si sono ritrovate improvvisamente prive di accesso alla propria

vita digitale, scoprendo che i loro strumenti di lavoro, i loro risparmi e le loro identità erano confinati in un edificio in fiamme nel deserto. Nei data center ci sono infrastrutture necessarie per far funzionare app bancarie, servizi cloud e piattaforme di intelligenza artificiale. Questa fragilità strutturale solleva interrogativi profondi sulla sovranità digitale e sulla natura stessa della proprietà nel XXI secolo. Abbiamo delegato la conservazione della nostra memoria e della nostra operatività a entità terze, convinti che la "nuvola" fosse un luogo sicuro, perché invisibile e sospeso in un luogo immateriale, non facilmente individuabile. Ma l'invisibilità non è invulnerabilità; al contrario, è una forma di occultamento, che impedisce di percepire il rischio. Il problema riguarda sia la minaccia cinetica delle bombe, sia la silenziosa e costante pressione del potere legale. Un provider cloud, per quanto garantisca la riservatezza attraverso contratti complessi, è prima di tutto un soggetto giuridico registrato in un Paese. La *Cloud Act* statunitense o le normative di sicurezza interna di altri Stati meno democratici stabiliscono un principio gerarchico inequivocabile, ovvero che l’autorità statale prevale sull’accordo privato. Se i nostri dati risiedono in un capannone situato in un territorio straniero, essi sono soggetti alle leggi di quel territorio, a prescindere dalla nazionalità dell’utente o della sede legale dell’azienda madre. Lo Stato può bussare alla porta e pretendere l'accesso ai dati senza che l'interessato ne venga mai a conoscenza, trasformando il provider in un involontario agente di sorveglianza. Ci troviamo di fronte a un paradosso geografico. I nostri dati sono globali nella fruizione ma locali nella conservazione. Questa discrepanza crea una zona grigia in cui la privacy dei cittadini e la sicurezza delle imprese sono appese alla stabilità diplomatica tra nazioni. L'attacco ai data center di Amazon segna l'inizio di un periodo storico in cui la geopolitica del server diventa la variabile dominante dell'economia mondiale. Non possiamo più permetterci di ignorare dove si trovino fisicamente i nostri bit. La dipendenza totale da flussi di lavoro che esistono solo online ci ha resi ostaggi di una topografia invisibile. La transizione verso il cloud è stata venduta come una liberazione dai vincoli dell'hardware, ma si è rivelata una forma di feudalesimo digitale, in cui gli utenti sono coloni su terre altrui. La resilienza di una nazione o di un'azienda si misura sia dalla capacità di difesa dei propri confini fisici, sia dalla distribuzione strategica dei propri dati e dalla capacità di rimpatriare le funzioni vitali in caso di crisi. Inoltre, il mito della nuvola è servito negli anni scorsi a nascondere l'estrattivismo di risorse e la centralizzazione del potere. Oggi, quel mito è bruciato insieme ai server di Manama e Dubai. Dobbiamo iniziare a pensare ai dati come a risorse critiche, simili all'acqua o all'energia, la cui gestione richiede una consapevolezza spaziale e legislativa assoluta. Chiedersi dove siano i propri dati non è più una curiosità tecnica, è un atto di autodifesa. La trasparenza del cloud si è rivelata molto

opaca. Dietro l'interfaccia pulita delle nostre app si nasconde una giungla di cavi, sistemi di raffreddamento e giurisdizioni ostili. Se la realtà è tornata a reclamare il suo spazio attraverso la violenza, la nostra risposta deve essere una nuova alfabetizzazione infrastrutturale che rifiuti la narrazione dell'immateriale per abbracciare la durezza fisica del reale.

L'implementazione di una strategia di cloud ibrido ora rappresenta per le multinazionali, per il sistema economico attuale e per gli Stati una necessità di sicurezza nazionale e continuità operativa a fronte di una vulnerabilità infrastrutturale ormai palese. Per evitare il collasso sistemico osservato negli attacchi ai data center mediorientali, le organizzazioni abbandoneranno in tempi rapidi la dipendenza esclusiva dai provider iperscalabili pubblici in favore di un'architettura che integri server locali proprietari, o *on-premise*, con segmenti di nuvola pubblica distribuiti su diverse giurisdizioni politiche. Il cuore di questa strategia risiede nella distribuzione granulare dei carichi di lavoro. I dati critici e le funzioni vitali devono risiedere in infrastrutture fisiche sotto il controllo diretto dell'ente, protette da firewall analogici e sistemi di ridondanza che non dipendano dalla medesima rete elettrica o connettività sottomarina dei grandi provider. In questo scenario, il cloud pubblico viene utilizzato solo per la scalabilità di servizi non essenziali, mentre un sistema di "failover" automatico garantisce che, in caso di distruzione cinetica di un data center remoto, l'operatività possa essere riassunta istantaneamente dai nodi locali. Oltre al rischio di attacco militare, il cloud presenta effetti collaterali profondi legati alla sovranità del dato e all'estrattivismo digitale. La permanenza dei file su server esteri espone le informazioni al "Cloud Act" o a normative locali che permettono il sequestro dei dati senza notifica, trasformando la nuvola in un panopticon geopolitico dove la riservatezza è subordinata alla ragion di Stato. Altri effetti includono il cosiddetto "vendor lock-in", che rende tecnicamente ed economicamente impossibile migrare i dati da un provider all'altro, e l'impatto termodinamico di infrastrutture che consumano enormi quantità di energia e acqua, rendendo la conservazione digitale un costo ecologico occulto. Per ovviare a queste criticità, i servizi segreti e gli organi militari delle potenze mondiali hanno da tempo abbandonato il cloud commerciale in favore di alternative radicalmente diverse: le "Sovereign Clouds" e le reti "Air-Gapped". Si tratta di infrastrutture fisicamente isolate dalla rete internet pubblica, costruite su hardware certificato e situato in bunker sotterranei o siti protetti da schermature elettromagnetiche. Potenze come gli Stati Uniti utilizzano il programma JWCC (Joint Warfighting Cloud Capability), un'architettura multi-cloud customizzata che garantisce segretezza a livello di intelligence, mentre la Russia e la Cina hanno sviluppato reti nazionali sovrane che possono funzionare in totale autonomia dal resto del mondo. Queste élites militari

adottano inoltre il "de-clouding" o il "fog computing", dove l'elaborazione dei dati avviene ai margini della rete, vicino ai sensori o alle truppe sul campo, riducendo la necessità di trasmettere informazioni verso capannoni vulnerabili. L'alternativa per le entità civili ad alto rischio è dunque il ritorno a un'informatica decentralizzata e sovrana, basata su protocolli di crittografia end-to-end dove le chiavi di accesso non sono mai in possesso del provider, garantendo che anche in caso di sequestro fisico dei server, il dato rimanga un ammasso di bit incomprensibili e inutilizzabili per l'aggressore o lo Stato ospitante.