Palantir, Anduril e Kyndryl: tre archetipi del nuovo ecosistema defence-tech tra guerra software-defined e “hardware turn”

di Gordon Mensah e Giovanni Trotta

Abstract

Questo paper analizza la trasformazione del settore defence-tech a partire da una tesi centrale: la guerra contemporanea è sempre più software-defined, ma questa evoluzione accresce, anziché ridurre, la rilevanza strategica delle infrastrutture materiali e computazionali che sostengono il potere digitale. In questa prospettiva, software, dati e modelli non operano in modo autonomo, ma dipendono da uno stack più ampio composto da cloud, reti, semiconduttori, standard tecnici, capacità di integrazione e supply chain. Attraverso la comparazione di tre archetipi aziendali – Palantir, Anduril e Kyndryl – il contributo ricostruisce tre nodi fondamentali del nuovo ecosistema della difesa: dati-decisione, autonomia-commando e controllo e infrastruttura-continuità. Ne emerge che la superiorità operativa non dipende soltanto da modelli o piattaforme, ma dal controllo coordinato di dati, sistemi, infrastrutture e capacità industriali che rendono possibile la continuità, la resilienza e la scalabilità delle operazioni. In questa chiave, il paper evidenzia la particolare vulnerabilità europea, esposta al rischio di una crescente dipendenza da stack digitali e infrastrutture in larga misura statunitensi, e si interroga sulla possibilità che iniziative come EuroStack e un approccio “Buy European” costituiscano una risposta credibile non solo sul piano industriale e strategico, ma anche in termini di sovranità operativa e controllo democratico.

This paper examines the transformation of the defence-tech sector through a central claim: contemporary warfare is increasingly software-defined, yet this evolution enhances rather than diminishes the strategic relevance of the material and computational infrastructures underpinning digital power. From this perspective, software, data, and models do not operate autonomously, but rely on a broader stack made up of cloud systems, networks, semiconductors, technical standards, integration capabilities, and supply chains. By comparing three corporate archetypes – Palantir, Anduril, and Kyndryl – the paper identifies three key nodes within the emerging defence ecosystem: data-to-decision, autonomy-command and control, and infrastructure-continuity. It argues that operational superiority no longer depends solely on models or platforms, but on the coordinated control of data, systems, infrastructures, and industrial capabilities that enable continuity, resilience, and scalability in operations. Against this backdrop, the paper highlights Europe’s particular vulnerability, as it faces growing dependence on largely US-based digital stacks and infrastructures, and asks whether initiatives such as EuroStack and a “Buy European” approach can offer a credible response not only in industrial and strategic terms, but also in relation to operational sovereignty and democratic accountability.

ISSN 2038-1662

Introduzione

Negli ultimi anni, il lessico della trasformazione digitale sta attraversando ciò che Luciano Floridi ha definito un *hardware turn*: dopo una lunga fase in cui il digitale è stato rappresentato come quasi immateriale, l'attenzione si è progressivamente spostata verso le infrastrutture, le risorse fisiche e le catene di controllo che rendono possibile – e governabile – il funzionamento dell'infosfera. In questa prospettiva, il punto non è contrapporre *software* e *hardware*, ma comprendere come il potere digitale si distribuisca lungo uno *stack* più ampio, nel quale modelli, dati e applicazioni dipendono da *data center*, *cloud*, semiconduttori, reti, cavi, satelliti, standard tecnici e *supply chain*. Chi controlla questa base materiale controlla anche le condizioni operative entro cui il *software* può funzionare, scalare e tradursi in leva geopolitica.

Questo passaggio non contraddice la crescente centralità del *software* nella guerra contemporanea; al contrario, ne chiarisce i presupposti. Il fatto che il conflitto sia sempre più *software-defined* non implica che l'*hardware* diventi marginale. Significa, piuttosto, che lo strato *software* tende a dominare la funzione – integrazione, decisione, interoperabilità – mentre l'infrastruttura materiale ne definisce i limiti reali di scalabilità, latenza, sicurezza e continuità operativa. In termini tecnologici, la velocità del ciclo decisionale dipende oggi dalla capacità di collegare dati, modelli e *workflow* in ambienti operativi complessi; ma tale capacità resta vincolata alla disponibilità di risorse computazionali, alla qualità delle architetture *cloud-edge*, alla resilienza delle reti e alla tenuta delle catene di fornitura. L'intelligenza artificiale e, più in generale, lo *stack software*, in altri termini, non operano nel vuoto: sono incorporati in una *supply chain* computazionale che comprende *chip* avanzati, capacità di calcolo, infrastrutture ibride, connettività e servizi di orchestrazione.

È in questo senso che il riferimento di Floridi all'*hardware turn* acquista una valenza particolarmente forte nel comparto della difesa. Se il *software* è lo strato che consente di integrare piattaforme, fondere segnali, coordinare sensori e produrre decisioni operative, la sua efficacia dipende comunque da una base materiale che può trasformarsi in vincolo strategico. *Data center*, *cloud*, reti sicure, semiconduttori, standard di interoperabilità e *supply chain* non sono dunque uno sfondo neutrale, ma parte integrante della potenza militare contemporanea. La lettura di Draghi sulle dipendenze industriali assume qui un significato pienamente strategico: la capacità di agire "a velocità *software*" resta condizionata da chi controlla l'infrastruttura che la rende possibile e da chi presidia i nodi abilitanti dello *stack* digitale.

ISSN 2038-1662

Questa dinamica emerge con particolare evidenza nella difesa, dove il valore non risiede più soltanto nelle singole piattaforme, ma nella capacità di costruire architetture digitali integrate. La superiorità operativa dipende sempre più dall'interoperabilità tra sistemi eterogenei, dalla possibilità di collegare sensori, dati logistici, piattaforme *legacy*, modelli di IA e catene di comando in un ambiente coerente, governabile e sicuro. In questo quadro, il ruolo del *system integrator* – inteso come attore capace di governare il "sistema di sistemi" – diventa decisivo. Non si tratta soltanto di integrare componenti tecniche, ma di rendere computabile e operativa la relazione tra dati, decisione e infrastruttura, assicurando al tempo stesso auditabilità, controllo degli accessi, resilienza *cyber* e continuità del servizio.

In parallelo, anche le *Big Tech* sono entrate stabilmente nella filiera. Dario Guarascio descrive l'emergere di un *military-digital complex*, in cui piattaforme e *cloud* statunitensi diventano attori centrali sia come *contractor* sia come infrastrutture abilitanti della potenza militare. In questo quadro, iniziative come *GenAI.mil*, che porta Google Gemini in una piattaforma *enterprise* per l'adozione di IA generativa nel perimetro della difesa statunitense, mostrano come la superiorità operativa passi anche dall'accesso privilegiato a modelli, *cloud* e strumenti di frontiera. La rilevanza di questi attori, dunque, non dipende soltanto dalla loro capacità di fornire applicazioni o servizi, ma dal fatto che presidiano alcuni dei nodi fondamentali dello *stack* digitale contemporaneo.

L'effetto internazionale di questa trasformazione è ancora più profondo se letto come un sistema di infrastrutture e reti. *Pipelines*, *ports*, *financial transaction arrangements* e altri grandi sistemi tecnici diventano architetture di proiezione estera e di influenza strutturale, come discusso nella letteratura sulle infrastrutture in politica globale e, soprattutto, nel paradigma della *weaponized interdependence*, dove il controllo di nodi-chiave consente effetti di *chokepoint* e *panopticon* su dati, scambi e transazioni. In altre parole, la dipendenza tecnologica non è solo un tema industriale, ma una condizione che può tradursi in vincoli strategici e asimmetrie nelle relazioni internazionali.

È qui che si colloca la vulnerabilità europea. Così come nella *digital sovereignty* l'Europa ha sperimentato una dipendenza sistemica dalle *Big Tech*, oggi rischia di riprodurre lo stesso schema nel dominio *defence-tech*, affidando parti cruciali della propria sicurezza a *stack* e piattaforme in gran parte americane. Il *framework* "*Buy European*" legato a *EuroStack* sintetizza questa preoccupazione: l'attuale paradigma di *procurement* "*buy from wherever*" alimenta dipendenza, estrazione di valore e

ISSN 2038-1662

vulnerabilità giurisdizionali e tecnologiche, proponendo criteri di sovranità – giurisdizione, reversibilità, interoperabilità, controllo operativo – per evitare "*sovereign prisons*". In parallelo, la riflessione sul crescente attrito regolatorio e strategico tra UE e USA – una *transatlantic tech war* in formazione – segnala che la dipendenza da *cloud*, piattaforme e satelliti è sempre più percepita in Europa come una vulnerabilità sulla quale poter fare *leverage*.

Da qui la domanda conclusiva che orienta anche il testo che segue: *EuroStack* e un approccio "*Buy European*" possono costituire una risposta credibile – industriale, regolatoria e strategica – alla crescente americanizzazione dello *stack* digitale della difesa europea?

Questa trasformazione si rende empiricamente visibile osservando tre tipologie aziendali che, pur collocandosi su segmenti diversi, presidiano nodi strategici del nuovo ecosistema *defence-tech*. Palantir rappresenta la piattaforma *software* di *operational AI*, orientata a trasformare dati eterogenei in decisioni operative all'interno di ambienti *mission-critical*. Anduril incarna invece il modello *software-first* che combina autonomia distribuita, sistemi *uncrewed* e piattaforme di comando e controllo, chiudendo il *loop* tra percezione, prioritizzazione e risposta. Kyndryl, infine, occupa il livello meno visibile ma altrettanto cruciale dell'infrastruttura: la modernizzazione di ambienti IT complessi, l'orchestrazione di architetture ibride, la gestione del *legacy* e la costruzione delle condizioni di continuità e resilienza senza le quali nessuna piattaforma può realmente scalare. La loro comparazione consente di leggere con maggiore precisione come si costruisca oggi la potenza militare: non solo attraverso armamenti o *software* specialistici, ma attraverso il controllo coordinato di dati, modelli, infrastrutture e capacità operative.

Palantir: piattaforma, governance e operational AI

Palantir rappresenta uno degli archetipi più chiari della *defence-tech* come strato *software* di integrazione in contesti *mission-critical*. Il suo *core business* consiste nello sviluppo di piattaforme che, storicamente, hanno assunto forme distinte a seconda dei contesti d'uso: Gotham per gli ambiti governativi e della sicurezza, Foundry per il mondo *enterprise*, e più recentemente AIP (*Artificial Intelligence Platform*), concepita per collegare modelli di IA ai dati e ai *workflow* reali. Il nucleo della proposta di Palantir non risiede dunque soltanto nella capacità di analizzare informazioni, ma nella costruzione di una piattaforma in grado di trasformare dati eterogenei in decisioni

ISSN 2038-1662

operative, organizzando il rapporto tra fonti informative diverse, modelli e processi dentro ambienti ad alta criticità.

La traiettoria tecnologica dell'azienda è quella della *operational AI*. In questo caso, l'IA non viene trattata come *analytics* di supporto marginale, né come componente separata rispetto ai processi organizzativi, ma come parte di una vera e propria "infrastruttura decisionale" che si innesta sopra sistemi preesistenti – *ERP*, *data lake*, sensori, sistemi militari – e rende computabile e governabile il passaggio dati→modelli→processi→decisioni. La piattaforma non si limita quindi a ospitare modelli, ma costruisce uno strato intermedio capace di collegare ambienti eterogenei, armonizzare dati, integrare sistemi *legacy* e inserire i modelli di IA in *workflow* effettivi, preservando al tempo stesso tracciabilità, regole di accesso e coerenza operativa.

Letta in questa prospettiva, Palantir presidia un nodo cruciale dello *stack* digitale contemporaneo: quello in cui la governance del dato si traduce in capacità operativa. In ambienti complessi e ad alta criticità, infatti, il problema non è soltanto disporre di modelli performanti, ma riuscire a inserirli in architetture informative frammentate, composte da fonti eterogenee, sistemi classificati, piattaforme pregresse e vincoli stringenti di sicurezza. La rilevanza della piattaforma deriva quindi dalla sua capacità di costruire interoperabilità tra sistemi diversi, collegare dati e decisione, e trasformare il patrimonio informativo in *output* operativo. In questo senso, Palantir incarna bene la logica della guerra sempre più *software-defined*: la superiorità non dipende solo dall'algoritmo, ma dalla possibilità di integrare modelli, dati e processi in un'infrastruttura governabile.

Dal punto di vista economico, Palantir combina una forte esposizione al settore pubblico con una strategia di espansione verso contesti regolati e industriali. La dinamica dei contratti pluriennali e dei rinnovi – si pensi alle piattaforme dati in ambito difesa o a casi discussi in ambito sanitario – è coerente con un modello di "infrastruttura *software*" che, una volta adottata, tende a diventare parte stabile della catena operativa e della governance informativa. Questo aspetto è importante perché chiarisce che il valore dell'azienda non deriva solo dalla vendita di una soluzione tecnologica, ma dalla sua capacità di radicarsi nel tempo dentro processi organizzativi complessi, diventando uno snodo persistente dell'architettura decisionale dell'ente o dell'organizzazione che la adotta.

ISSN 2038-1662

In termini di potere strutturale, ciò significa che Palantir presidia un punto nevralgico: la governance del dato e la sua trasformazione in *output* operativo. È una posizione che incide direttamente sulla capacità di coordinare sistemi eterogenei, di ridurre attriti informativi e di accelerare il ciclo decisionale in ambienti in cui il tempo, la sicurezza e la qualità dell'integrazione contano quanto, se non più, della sola performance del modello. Per questo Palantir non va letta semplicemente come fornitore di *software*, ma come attore che occupa il livello in cui il controllo dell'informazione si converte in potere organizzativo e operativo. È qui che la piattaforma diventa, più propriamente, infrastruttura della decisione.

Anduril: autonomia distribuita, comando-controllo e industrializzazione in stile Silicon Valley

Anduril incarna un secondo archetipo del comparto *defence-tech*: quello dell'impresa *software-first* che integra sistemi autonomi nei domini aereo, terrestre e marittimo con una piattaforma di comando e controllo – Lattice – capace di connettere sensori e *asset* eterogenei e di automatizzare parti della risposta. La rilevanza dell'azienda non risiede però esclusivamente nel prodotto *uncrewed* in quanto tale, ma nella capacità di chiudere il *loop* informativo-decisionale: filtrare segnali, attribuire priorità, assegnare compiti a sensori o *asset* e accelerare l'intero ciclo. In questo senso, la logica *software-defined* risulta particolarmente evidente: l'*hardware* autonomo resta decisivo, ma la capacità operativa si manifesta soprattutto nella piattaforma che orchestra sensori, dati e *asset*.

Lattice costituisce, da questo punto di vista, il vero baricentro tecnologico del modello Anduril. Non si limita a svolgere una funzione di interfaccia di comando e controllo, ma opera come uno strato di integrazione eterogenea in cui confluiscono segnali, dati e sistemi diversi. È in questo ambiente che l'impiego di tecniche di *AI/ML* per *triage*, *tasking* e accelerazione del ciclo decisionale acquista significato operativo: non come automazione generica, ma come capacità di selezionare l'informazione rilevante, ridurre il rumore, ordinare le priorità e trasformare una pluralità di input in una risposta coordinata.

La traiettoria dell'azienda mostra così un aspetto essenziale dell'IA applicata alla difesa: il vantaggio non deriva soltanto dalla qualità del singolo modello o del singolo sistema, ma dalla capacità di incorporare classificazione, prioritizzazione e assegnazione dei compiti dentro una *decision architecture* che collega percezione, elaborazione e azione. In questo passaggio, il *software* non sostituisce la componente

ISSN 2038-1662

materiale, ma la rende coordinabile su scala più ampia, riducendo la distanza tra raccolta del segnale e risposta operativa. È qui che l'integrazione tra sensori, piattaforme autonome e strato di comando-controllo diventa il vero moltiplicatore di efficacia.

L'elemento distintivo di Anduril è però anche industriale. L'impresa persegue cicli rapidi di iterazione in stile *Silicon Valley* e, simultaneamente, un progetto di scalabilità produttiva, esemplificato da Arsenal-1 come impianto *hyperscale*. Questo mix ridisegna la tradizionale separazione tra innovazione e produzione: l'autonomia diventa credibile solo se supportata da capacità industriale di serie e *supply chain*, cioè se torna pienamente in gioco la dimensione materiale richiamata dall'*hardware turn*. Le architetture modulari e l'iterazione rapida sui requisiti operativi vanno lette in questa stessa chiave: la velocità del *software* acquista rilevanza strategica solo quando può tradursi in sistemi effettivamente producibili, dispiegabili e sostenibili nel tempo.

Anduril mostra dunque come l'autonomia militare contemporanea sia un prodotto congiunto di *software*, sensoristica, produzione e infrastruttura logistica. Se Palantir rende visibile il livello della governance del dato e della trasformazione dell'informazione in *output* operativo, Anduril evidenzia il punto in cui integrazione multi-dominio, autonomia distribuita e capacità industriale convergono in una stessa architettura tecnologica. La guerra sempre più *software-defined* non riduce il peso della base materiale, ma ne ridefinisce la funzione: la superiorità operativa dipende dalla possibilità di collegare piattaforme autonome, sistemi di comando e controllo, capacità produttiva e *supply chain* dentro un ecosistema coerente e scalabile.

Kyndryl: infrastruttura, resilienza e orchestrazione dell'IT critico

Kyndryl rappresenta un terzo tipo di attore, spesso sottovalutato nel dibattito *defence-tech*: quello dell'infrastruttura e della modernizzazione di grandi ambienti IT. Nata dallo *spin-off* di IBM nel 2021, l'azienda è specializzata in *managed services* per *data center*, *mainframe*, reti e *cloud ibrido*. In una prospettiva a *stack*, Kyndryl presidia lo strato che rende possibile la continuità operativa delle amministrazioni e delle organizzazioni complesse, inclusi segmenti della pubblica amministrazione. Il suo ruolo non consiste nel produrre piattaforme di autonomia o sistemi di supporto decisionale, ma nel garantire che l'infrastruttura su cui tali capacità si appoggiano resti disponibile, governabile, sicura e interoperabile.

ISSN 2038-1662

In questo quadro, Kyndryl Bridge occupa una posizione centrale. La piattaforma si configura come un *layer* di osservabilità e orchestrazione *AI-powered*, progettato per integrare e governare *estate* tecnologici complessi in modalità *end-to-end*, soprattutto nei contesti in cui il peso del *legacy* rende difficile una trasformazione rapida. Il punto non riguarda soltanto il monitoraggio dell'infrastruttura, ma la possibilità di renderla leggibile e coordinabile come sistema unitario: raccogliere segnali da ambienti eterogenei, correlarli, automatizzare parti delle *operations* e sostenere processi di gestione distribuiti tra ambienti *on-premise*, *cloud ibrido*, reti e *mainframe*. L'IA, in questa prospettiva, non compare come funzione autonoma o verticale, ma come componente incorporata nell'orchestrazione tecnica dell'infrastruttura.

È qui che emerge con maggiore chiarezza la specificità del contributo di Kyndryl. La trasformazione digitale in contesti critici non dipende soltanto dall'introduzione di nuovi modelli o di nuove piattaforme, ma dalla capacità di standardizzare, automatizzare e stabilizzare le operazioni che sostengono l'intero ambiente tecnologico. L'industrializzazione dell'IT passa attraverso processi di osservabilità continua, automazione e uso dell'IA con l'obiettivo di ridurre rischi, migliorare la qualità del servizio e contenere la fragilità sistemica. In questo senso, il valore dell'azienda si colloca meno nella retorica dell'innovazione visibile e più nella costruzione delle condizioni operative che consentono all'innovazione di funzionare senza compromettere affidabilità e continuità.

La rilevanza di Kyndryl diventa particolarmente evidente nei contesti in cui la complessità infrastrutturale rappresenta il vero collo di bottiglia. Molte organizzazioni critiche operano infatti su architetture stratificate, nelle quali convivono sistemi storici, vincoli regolatori, requisiti di sicurezza elevati e necessità di migrazione progressiva. In questi ambienti, modernizzare non significa sostituire integralmente il passato, ma costruire forme di coordinamento tra componenti diverse, mantenendo continuità operativa durante la transizione. È in questo spazio che Kyndryl assume un rilievo strategico: la capacità di migrare, integrare e modernizzare senza interrompere il servizio diventa una funzione essenziale tanto quanto la disponibilità di *software* avanzato.

In termini sistemici, Kyndryl rende visibile una tesi spesso trascurata: la superiorità "a velocità *software*" dipende da operazioni infrastrutturali robuste, gestione del rischio, *cyber-resilienza* e capacità di trasformazione senza perdita di continuità. La potenza del digitale, in altre parole, non coincide soltanto con il modello, con il sensore o con

ISSN 2038-1662

la piattaforma applicativa, ma anche con l'insieme delle condizioni materiali e organizzative che ne rendono possibile il funzionamento su scala. L'azienda porta al centro la dimensione meno appariscente ma più strutturale dell'ecosistema tecnologico contemporaneo: quella in cui l'efficacia dell'IA dipende dalla qualità dell'infrastruttura, dalla governabilità dei processi e dalla tenuta operativa degli ambienti critici.

Per questa ragione, Kyndryl occupa un nodo distinto ma complementare rispetto agli altri attori del comparto. Se una parte della trasformazione *defence-tech* si concentra sulla governance del dato e un'altra sull'autonomia distribuita e sul comando-controllo, Kyndryl presidia il livello dell'infrastruttura-continuità: l'orchestrazione dell'IT critico, la modernizzazione del *legacy*, la standardizzazione operativa e la costruzione di ambienti tecnologici resilienti. Ciò che rende l'IA realmente operativa, in questa prospettiva, non è soltanto la disponibilità di modelli avanzati, ma la possibilità di inserirli in un'infrastruttura che regga il carico della complessità computazionale.

Comparazione e implicazione geopolitica: dove si colloca il potere

La comparazione consente di distinguere tre nodi del potere nel nuovo ecosistema *defence-tech*. Palantir occupa il nodo dati-decisione, cioè il livello della governance del dato e della sua trasformazione in azione operativa; Anduril presidia il nodo autonomia-*C2*, nel quale convergono orchestrazione multi-dominio e accelerazione del ciclo decisionale; Kyndryl si colloca invece nel nodo infrastruttura-continuità, legato all'orchestrazione dell'IT critico e ai processi di modernizzazione. Questa tripartizione riflette in modo coerente la cornice analitica proposta in apertura: la guerra è sempre più *software-defined*, ma il *software* non è mai autonomo, poiché dipende da infrastrutture, capacità materiali e *supply chain*; di conseguenza, chi controlla tali infrastrutture controlla anche una parte decisiva dei margini di sovranità operativa.

Inoltre, l'ingresso delle *Big Tech* nella filiera e l'emergere di un *military-digital complex* non costituiscono un elemento accessorio, ma un fenomeno strutturale. *Cloud*, modelli, *data center* e piattaforme digitali diventano al tempo stesso componenti della potenza militare e possibili fattori di vincolo per gli attori che non controllano lo *stack*. È precisamente su questo terreno che la vulnerabilità europea assume un significato specifico: la dipendenza non riguarda soltanto l'acquisto di sistemi o applicazioni, ma investe l'accesso e il controllo degli strati abilitanti del digitale difensivo, cioè della base materiale e infrastrutturale su cui il *software* opera.

ISSN 2038-1662

Conclusione: dalla “doppia dipendenza” alla “doppia scatola nera”

La trasformazione del settore *defence-tech* rende ancora più stringente una tensione tipica delle democrazie: le decisioni di sicurezza nazionale sono tra le più rilevanti e, allo stesso tempo, tra le meno trasparenti. È il paradosso che Ashley S. Deeks definisce *double black box*: l’opacità propria dell’ecosistema della sicurezza – classificazione, difficoltà di *oversight*, espansione del potere esecutivo – si somma all’opacità degli algoritmi e dei sistemi di IA, spesso descritti essi stessi come “scatole nere”. Quando l’IA entra stabilmente nei processi decisionali della sicurezza nazionale, o addirittura contribuisce ad automatizzarli, diventa più difficile garantire razionalità, legalità e *accountability* non solo nei confronti del pubblico, ma anche verso gli alleati e persino verso gli stessi decisori. La posta in gioco, quindi, non è soltanto industriale: riguarda la governance democratica della potenza digitale.

In questo quadro, la lettura di Dario Guarascio sull’“imperialismo digitale” offre un’ulteriore chiave interpretativa. La mutua dipendenza tra Stato e *Big Tech*, fondata sull’evoluzione del complesso militar-digitale, contribuisce a produrre un sistema in cui l’accesso ai dati e la tutela dell’espansione delle piattaforme diventano elementi strutturali dell’egemonia, insieme a dinamiche di “porte girevoli” tra vertici industriali e militari. Per l’Europa, il nodo non consiste quindi soltanto nello stabilire se adottare soluzioni *defence-tech* avanzate, ma nel definire a quali condizioni infrastrutturali, giurisdizionali e di controllo tali soluzioni vengano integrate, così da evitare che l’aumento di capacità si traduca in una riduzione della sovranità operativa e dell’*accountability*. In ultima analisi, la traiettoria di Palantir, Anduril e Kyndryl – e, più in generale, l’intreccio tra piattaforme, autonomia e infrastrutture – anticipa la domanda più ampia che oggi attraversa il continente: come beneficiare della potenza del *software* senza trasferire, insieme ad essa, la governance della sicurezza a un ecosistema opaco e potenzialmente esterno ai circuiti democratici.

Bibliografia

Deeks AS, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* (OUP 2025) https://academic.oup.com/book/59551

Drezner DW, Farrell H and Newman AL (eds), *The Uses and Abuses of Weaponized Interdependence* (Brookings Institution Press 2021) https://www.brookings.edu/books/the-uses-and-abuses-of-weaponized-interdependence/

ISSN 2038-1662

Guarascio D, *Imperialismo digitale: Economia e guerra ai tempi delle piattaforme e dell'IA* (Laterza 2026) https://www.laterza.it/scheda-libro/?isbn=9788858157718

Kellerbauer M, Klamert M and Tomkin J (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (2nd edn, OUP 2023) https://global.oup.com/academic/product/the-eu-treaties-and-charter-of-fundamental-rights-a-commentary-9780198913689

Arrowsmith S, 'The Purpose of the EU Procurement Directives: Ends, Means and the Implications for National Regulatory Space for Commercial and Horizontal Procurement Policies' (2011) 14 *Cambridge Yearbook of European Legal Studies* 1 https://www.cambridge.org/core/journals/cambridge-yearbook-of-european-legal-studies/article/abs/purpose-of-the-eu-procurement-directives-ends-means-and-the-implications-for-national-regulatory-space-for-commercial-and-horizontal-procurement-policies/121F2BAA1AD9168B22F8EA62992DC0F5

Coveri A, Cozza C, Guarascio D and Pianta M, 'Big Tech and the US Digital-Military-Industrial Complex' (2025) 60(2) *Intereconomics* https://www.intereconomics.eu/contents/year/2025/number/2/article/big-tech-and-the-us-digital-military-industrial-complex.html

Farrell H and Newman AL, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42 https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic accessed 29 March 2026.

Floridi L, 'The Hardware Turn in the Digital Discourse: An Analysis, Explanation, and Potential Risk' (2024) *Philosophy & Technology* https://link.springer.com/content/pdf/10.1007/s13347-024-00723-1.pdf

Larkin B, 'The Politics and Poetics of Infrastructure' (2013) 42 *Annual Review of Anthropology* 327 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344213

'European ambitions captured by American clouds: digital sovereignty and infrastructuring through Gaia-X' (2025) *Information, Communication & Society* https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2025.2516545

Bellanova R and others, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study* (2021) https://www.jstor.org/stable/resrep30940

European Commission, *The Draghi report: A competitiveness strategy for Europe* (9 September 2024)

ISSN 2038-1662

EuroStack, *A Proposed Framework for a Buy European Regulation of Strategic Digital Procurement* (29 September 2025) https://eurostack.eu/wp-content/uploads/2025/09/buy-european-a-framework-for-strategic-procurement-29-september-25.pdf

González R, *Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry* (Transnational Institute 2023) https://www.tni.org/files/2023-04/Militarising%20%20Big%20Tech.pdf

Guarascio D, 'Beyond the hype: AI and the military-digital complex' (Nexa Center for Internet & Society, Politecnico di Torino, Working Paper 2024) https://nexa.polito.it/wp-content/uploads/2024/11/NEXA_2024_Guarascio.pdf

Vine D and others, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex* (Costs of War, Watson Institute, Brown University 2024) https://costsofwar.watson.brown.edu/sites/default/files/papers/Silicon-Valley-MIC.pdf

Bertelsmann Stiftung, *EuroStack – A European Alternative for Digital Sovereignty* (2025) https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty

European Commission (Digital Building Blocks), 'How the DIGITAL Building Blocks can help bring EuroStack's vision of European digital sovereignty to life' https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/900014236/How%2Bthe%2BDIGITAL%2BBuilding%2BBlocks%2Bcan%2Bhelp%2Bbring%2BEuroStacks%2Bvision%2Bof%2BEuropean%2Bdigital%2Bsovereignty%2Bto%2Blife

Google Cloud (Public Sector), 'Gemini for Government: Build custom AI agents for unclassified work on GenAI.mil' (10 March 2026) https://cloud.google.com/blog/topics/public-sector/gemini-for-government-build-custom-ai-agents-for-unclassified-work-on-genaimil

US "War Department" (official site), 'The War Department Unleashes AI on New GenAI.mil Platform' https://www.war.gov/News/Releases/Release/Article/4354916/the-war-department-unleashes-ai-on-new-genaimil-platform/

ISSN 2038-1662