GOVTECH

Ridefinire il potere tecnologico: Stati Uniti e Cina nella competizione per l'ordine digitale globale

A cura di *Gregorio Staglianò*

21 MAGGIO 2026

Il Geopolitical Brief analizza la competizione tecnologica tra Stati Uniti e Cina come una dinamica ormai sistemica, che investe l'intero ecosistema digitale. Lo studio esamina le strategie delle due potenze, evidenziando come il confronto non riguardi solo l'innovazione tecnologica, ma il controllo delle condizioni che la rendono possibile e la capacità di strutturare l'ambiente tecnologico globale.

GovTech – Geopolitical Brief n. 60/maggio 2026

Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info

Il volume costituisce un prodotto di ricerca del progetto "GovTech – Governare l'era tecnologica: l'Italia tra cybersecurity, intelligenza artificiale e nuove sfide internazionali" realizzato dal Centro Studi Geopolitica.info in collaborazione con il Centro di Ricerca Cooperazione con l'Eurasia, il Mediterraneo e l'Africa Sub-Sahariana (CEMAS) e finanziato dall'Unità di Analisi, Programmazione, Statistica e Documentazione Storica del Ministero degli Affari Esteri e della Cooperazione Internazionale. Le opinioni contenute nella presente pubblicazione sono espressione degli autori, e non rappresentano necessariamente le posizioni del Ministero degli Affari Esteri e della Cooperazione Internazionale, né quelle delle altre Istituzioni partner.

ISSN : 3103-3407

INDICE

Ridefinire il potere tecnologico: Stati Uniti e Cina nella competizione per l'ordine digitale globale.....1

Ridefinire il potere tecnologico: dalla rivalità settoriale alla competizione sistemica .1

Dai principi alla pratica: la competizione per i *choke points* tecnologici 4

Il dominio cyber come spazio di competizione permanente..... 12

IA e potere sistemico: dalla competizione tecnologica al controllo dell'infrastruttura..... 14

Le ricadute della competizione sull'Europa e sull'Italia 19

Riferimenti bibliografici 23

Ridefinire il potere tecnologico: Stati Uniti e Cina nella competizione per l'ordine digitale globale

Gregorio Staglianò

Ridefinire il potere tecnologico: dalla rivalità settoriale alla competizione sistemica

A partire dal 2020, le società globali hanno attraversato una fase di accelerazione tecnologica senza precedenti, determinata dalla convergenza tra digitalizzazione forzata dei processi economici e sociali, maturazione di tecnologie abilitanti e crescente integrazione tra dimensione fisica e digitale. Questo passaggio ha reso il dominio tecnologico un fattore strutturale di potere economico e geopolitico. In tale contesto, la competizione tra Stati Uniti e Cina si è progressivamente trasformata da rivalità settoriale a competizione sistemica che non si gioca più su singole tecnologie, ma sul controllo delle infrastrutture abilitanti e delle condizioni di funzionamento dell'ecosistema digitale nel suo complesso.[1] In questo quadro, IA e cybersicurezza emergono come domini centrali e interdipendenti: la prima abilita capacità di analisi, automazione e superiorità decisionale; la seconda garantisce protezione e resilienza, ma soprattutto consente la proiezione offensiva del potere nello spazio digitale e contribuisce alla definizione delle regole e dei framework di sviluppo dell'ecosistema tecnologico. Insieme, esse non esauriscono la competizione, ma ne rappresentano i livelli più visibili e strategicamente rilevanti.[2]

La competizione si articola dunque lungo l'intero ecosistema tecnologico che sostiene l'economia digitale contemporanea: dalle materie prime critiche e dalla capacità energetica, alla produzione di semiconduttori, fino alle infrastrutture

[1] "Promethean Rivalry: The World-Altering Stakes of Sino-American AI Competition," Center for a New American Security, 2024, https://www.cnas.org/publications/reports/promethean-rivalry.
[2] "China, the United States, and the AI Race," Council on Foreign Relations, 10 ottobre, 2025, https://www.cfr.org/articles/china-united-states-and-ai-race.

cloud e ai data center, per arrivare ai dati, ai modelli di IA e ai sistemi di cybersicurezza. Si tratta di una *value chain* profondamente interdipendente, in cui ciascun livello condiziona e abilita quello successivo, trasformando l'insieme delle tecnologie digitali in un'infrastruttura strategica di potere. In questo quadro, il controllo dei diversi segmenti dell'ecosistema diventa la vera posta in gioco della competizione sistemica, poiché determina non solo la capacità di innovare, ma anche quella di diffondere standard, creare dipendenze tecnologiche e limitare l'accesso degli attori rivali ai nodi critici della filiera.[3]

Ne deriva che la competizione tra Washington e Pechino non può essere interpretata unicamente in termini di primato tecnologico, ma come capacità di plasmare l'ambiente tecnologico globale. Ciò si traduce in tre dimensioni operative della competizione: a) la diffusione, ossia la capacità di rendere le proprie tecnologie e i propri standard dominanti nei mercati internazionali; b) la dipendenza, attraverso la creazione di *lock-in* tecnologici e regolatori; e c) la possibilità di limitare o negare all'avversario l'accesso ai nodi critici della filiera. In questo quadro, il controllo dei cosiddetti *choke points* - segmenti della catena del valore difficilmente sostituibili - assume una valenza strategica analoga a quella dei colli di bottiglia industriali nelle competizioni del passato.[4]

Difatti, anche se il parallelo con la corsa agli armamenti del XX secolo appare immediato, risulta parziale. Come durante la Guerra fredda, la competizione non si esaurisce nello sviluppo della tecnologia più avanzata, ma riguarda la capacità di sostenere nel tempo un complesso industriale, scientifico e strategico in grado di produrre, integrare e diffondere innovazione su larga scala. Tuttavia, a differenza del confronto bipolare novecentesco, la competizione attuale si

[3] Chris Miller, Chip War: The Fight for the World's Most Critical Technology (New York: Scribner, 2022).
[4] "U.S.-China Technology Competition: A Brookings Global China Interview," Brookings Institution, 2021, https://www.brookings.edu/articles/u-s-china-technology-competition/.

sviluppa all'interno di un contesto di interdipendenza economica e tecnologica significativamente più profondo, in cui le filiere sono globali e le tecnologie prevalentemente *dual-use*.[5] Ne consegue che la competizione non produce un esito binario, ma si distribuisce su una pluralità di domini tecnologici e livelli dell'ecosistema, rafforzando la natura sistemica del confronto tra Stati Uniti e Cina.

Questa configurazione si riflette anche nell'evoluzione della postura politica adottata dalle due potenze: si è progressivamente affermata una logica di segmentazione selettiva delle interdipendenze, fondata sul controllo dei nodi critici della filiera e sulla costruzione di ecosistemi tecnologici differenziati. Gli Stati Uniti hanno sviluppato un approccio incentrato su controlli mirati lungo i *choke points* dell'ecosistema, dai semiconduttori avanzati alle tecnologie di produzione, affiancati a stringenti *screening* degli investimenti e al rafforzamento di alleanze tecnologiche con partner considerati affidabili. In questo quadro si inseriscono anche iniziative volte a strutturare catene del valore *trusted* lungo le filiere, attraverso accordi selettivi di cooperazione, accesso preferenziale e interoperabilità, come nel caso della cosiddetta "*Pax Silica*" (2025)[6], che segnala il passaggio da una logica puramente restrittiva a una più ampia strategia di costruzione di ecosistemi tecnologici integrati tra Stati e imprese alleate.

Parallelamente, la Cina ha adottato un approccio volto a ridurre le proprie vulnerabilità e a rafforzare la propria autonomia tecnologica senza rinunciare all'integrazione nei mercati globali. Più che un semplice tentativo di sostituzione, la strategia cinese combina sviluppo domestico nei settori più critici - come semiconduttori, software e infrastrutture digitali - con una progressiva

[5] Heino Klinck, "The Cold War Paradigm Is Inadequate for U.S.-China Strategic Competition," Ronald Reagan Institute, 1 luglio 2025, https://www.reaganfoundation.org/reagan-institute/publications/the-cold-war-paradigm-is-inadequate-for-u-s-china-strategic-competition-vol6.
[6] "Pax Silica," U.S. Department of State, dicembre 2025, https://www.state.gov/pax-silica.

diversificazione delle relazioni economiche e tecnologiche. Attraverso investimenti pubblici, una massiccia pianificazione industriale e di adozione delle tecnologie emergenti nella società cinese, Pechino mira a costruire spazi tecnologici alternativi, in cui le proprie imprese e tecnologie possano diffondersi e consolidarsi, riducendo al contempo l'esposizione ai vincoli imposti dai controlli americani.[7]

Il risultato è un modello di competizione che non elimina l'interdipendenza, ma la riconfigura in senso strategico, trasformandola da fattore di integrazione a leva di potere e di pressione geopolitica. Quella in corso, non è una semplice corsa all'innovazione, ma un processo di riorganizzazione dell'ordine tecnologico globale.

Dai principi alla pratica: la competizione per i *choke points* tecnologici

Come già evidenziato, questa configurazione sistemica della competizione trova una prima e concreta manifestazione nel controllo dei segmenti più critici delle filiere tecnologiche.

Sul versante statunitense ciò si è tradotto in una strategia il cui perno è ancora oggi rappresentato dai controlli alle esportazioni, introdotti dall'amministrazione Biden nel 2022 e implementati dal *"Bureau of Industry and Security (BIS)"* del Dipartimento del Commercio, che mirano a intervenire non solo sui prodotti finali, ma sull'intera filiera tecnologica che abilita la produzione e l'utilizzo di capacità computazionale avanzata. Con il pacchetto di controlli

[7] Jeroen Groenewegen-Lau, "Whole-of-Nation Innovation: Does China's Socialist System Give It an Edge in Science and Technology?," MERICS, 5 marzo, 2024, https://merics.org/en/report/whole-nation-innovation-does-chinas-socialist-system-give-it-edge-science-and-technology.

introdotto il 7 ottobre 2022[8], successivamente rafforzato nell'ottobre 2023[9], e nuovamente nel 2024[10], per la prima volta, gli Stati Uniti hanno esteso controlli e limiti non solo ai chip avanzati, ma anche alle tecnologie necessarie per produrli, introducendo al contempo meccanismi extraterritoriali, quali la "*Foreign Direct Product Rule (FDP)*"[11], che consentono di applicare restrizioni anche a prodotti realizzati all'estero ma basati su tecnologia statunitense.

Alla fine del 2024, con il nuovo pacchetto sanzionatorio, gli Stati Uniti hanno ampliato le restrizioni ai chip di memoria ad alta larghezza di banda (*High Bandwidth Memory, HBM*) – utilizzati su asset militari e spaziali avanzati e per il training di modelli di IA - software e macchinari, segnando il passaggio a una logica più sistemica, volta a ostacolare le traiettorie cinesi di sviluppo future in ambito militare ed economico.[12] Tuttavia, l'efficacia di queste misure resta incerta. Da un lato, i controlli stanno accelerando in Cina dinamiche di *substitution* tecnologica e integrazione verticale della filiera, con attori come Huawei e SMIC impegnati a ridurre la dipendenza da fornitori esteri. Dall'altro, il regime restrittivo genera effetti di frizione anche per gli alleati e per le imprese occidentali, esposte al mercato cinese sia in termini di ricavi sia di

[8] "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," U.S. Department of Commerce, Bureau of Industry and Security, 7 ottobre, 2022, https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples.

[9] "Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Entity List Modification," Federal Register, 25 ottobre, 2023, https://www.federalregister.gov/documents/2023/10/25/2023-23055/implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and.

[10] "Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications," U.S. Department of Commerce, Bureau of Industry and Security, 2 dicembre 2024, https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military.

[11] 15 CFR § 734.9 – Foreign-Direct Product (FDP) Rules," Electronic Code of Federal Regulations (eCFR), https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.9.

[12] Gregory C. Allen, "Understanding the Biden Administration's Updated Export Controls," Center for Strategic and International Studies (CSIS), 11 dicembre, 2024, https://www.csis.org/analysis/understanding-biden-administrations-updated-export-controls.

posizionamento nelle catene globali del valore, rischiando così di erodere nel medio periodo parte del vantaggio competitivo che intende proteggere.

In questo contesto, Washington ha iniziato a ricalibrare la propria strategia, integrando in modo più esplicito la dimensione alleata e geo-economica. La revoca, nel maggio 2025, del "*Framework for Artificial Intelligence Diffusion*"[13] segnala il passaggio da un approccio prevalentemente generalizzato a uno più selettivo e relazionale: contenere gli avversari senza compromettere la cooperazione con i partner tecnologicamente affidabili. Ne deriva una trasformazione dei controlli all'export, sempre meno strumenti puramente restrittivi e sempre più leve di gestione delle interdipendenze, funzionali alla costruzione di ecosistemi affidabili e a una gerarchia differenziata nell'accesso alle capacità computazionali critiche.

Questa architettura di sicurezza economica si intreccia strettamente con la politica industriale americana. Il "*CHIPS and Science Act*" del 2022[14] ne costituisce il pilastro domestico: uno strumento volto a ridurre vulnerabilità strutturali della *supply chain* e a rafforzare una capacità produttiva avanzata e resiliente, negli Stati Uniti e nei paesi partner. In questo contesto si inseriscono gli ingenti investimenti governativi - 6.6 miliardi di dollari - a sostegno dell'espansione di attori chiave come la taiwanese TSMC in Arizona.[15] La competizione per i semiconduttori, dunque, non riguarda soltanto la capacità di produrre chip, ma la possibilità di organizzare alleanze industriali, redistribuire le *value chain* e

[13] "Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls," U.S. Department of Commerce, Bureau of Industry and Security, 13 maggio, 2025, https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens.
[14] Michelle Kurilla, "What Is the CHIPS Act?," Council on Foreign Relations, 29 aprile, 2024, https://www.cfr.org/articles/what-chips-act.
[15] Asa Fitch, "Taiwanese Chip-Making Giant TSMC Gets $6.6 Billion for Arizona Project," Wall Street Journal, 8 aprile 2024, https://www.wsj.com/tech/taiwanese-chip-making-giant-tsmc-gets-6-6-billion-for-arizona-project-f75e9de4.

costruire nuove forme di dipendenza reciproca tra Stati e grandi attori tecnologici.

La risposta cinese alla strategia statunitense si inserisce in una visione di lungo periodo volta a ridurre vulnerabilità strutturali e a costruire un'autonomia tecnologica selettiva, combinando sostituzione domestica nei segmenti più esposti ai controlli occidentali e attivazione di leve geoeconomiche nelle fasi *upstream* delle catene del valore. In questo ambito, la posizione dominante della Cina nelle terre rare - con circa il 70% dell'estrazione globale e oltre il 90% della capacità di raffinazione - costituisce una leva strategica di primo piano.[16] Le restrizioni introdotte a partire dal 2023[17] su elementi chiave, come terbio, gallio, germanio e disprosio, e su tecnologie critiche di lavorazione, inclusa la produzione di magneti e macchinari specializzati, evidenziano come Pechino stia progressivamente utilizzando il controllo delle fasi *upstream* non solo per garantire la sicurezza delle proprie filiere, ma anche come strumento di risposta e pressione nei confronti delle restrizioni occidentali, estendendo in alcuni casi tali misure anche a soggetti esteri che utilizzano tecnologie cinesi.[18]

Programmi già avviati - come "*Made in China 2025*" e le successive strategie per l'autosufficienza tecnologica [19] - sono stati progressivamente rafforzati attraverso investimenti pubblici, incentivi fiscali e mobilitazione di capitali

[16] International Energy Agency (IEA), "Rare Earth Elements – Executive Summary," 2026, https://www.iea.org/reports/rare-earth-elements/executive-summary.
[17] MOFCOM Regular Press Conference (6 luglio 2023)," Ministry of Commerce of the People's Republic of China, 6 luglio 2023, https://english.mofcom.gov.cn/News/PressConference/art/2023/art_36fb2d80e4b4453891bb8fc83e2b3c4e.html.
[18] Tae-Yoon Kim, Shobhan Dhir, Amrita Dasgupta, and Alessio Scanziani, "With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality," International Energy Agency (IEA), 23 ottobre 2025, https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality.
[19] Kaiser Kuo, "How China Is Reinventing the Future of Global Manufacturing," World Economic Forum, 26 giugno, 2025, https://www.weforum.org/stories/2025/06/how-china-is-reinventing-the-future-of-global-manufacturing/.

statali e para-statali, con l'obiettivo di sviluppare capacità nazionali nei semiconduttori, nel *software* e nelle infrastrutture digitali. In questo quadro, il settore dei chip rappresenta il principale punto di frizione: pur rimanendo indietro nei nodi più avanzati, la Cina ha intensificato gli sforzi per consolidare la produzione su nodi maturi e per sviluppare alternative domestiche lungo l'intera filiera, dal *design* all'*equipment,* riducendo la dipendenza da fornitori esteri.[20]

Iniziative come "*Eastern Data, Western Computing*" (2022)[21], invece, rappresentano un tentativo di riorganizzare su scala geografica la produzione e l'impiego della capacità di calcolo, trasferendo i data center e le attività computazionali verso regioni occidentali caratterizzate da maggiore disponibilità energetica e costi inferiori. L'iniziativa mira a sostenere la scalabilità dell'IA e delle infrastrutture digitali attraverso una più stretta integrazione tra dati, calcolo ed energia. In questa prospettiva, il *compute* diventa anche una funzione della geografia e della capacità di organizzare le condizioni materiali dell'innovazione.

Un ulteriore livello della competizione tecnologica riguarda la trasformazione delle infrastrutture finanziarie. *Blockchain*, tokenizzazione degli asset, *stablecoin* e valute digitali non rappresentano più soltanto innovazioni di nicchia legate all'ecosistema cripto, ma stanno progressivamente diventando strumenti attraverso cui si ridefiniscono pagamenti, mercati dei capitali e sovranità monetaria. [22] La posta in gioco non è semplicemente l'adozione di nuove

[20] Gregory C. Allen, "China's New Strategy for Waging the Microchip Tech War," Center for Strategic and International Studies (CSIS), 3 maggio, 2023, https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war.
[21] Toomas Hanso, "More Than Meets the AI: China's Data Centre Strategy," International Centre for Defence and Security (ICDS), 6 novembre 2025, https://icds.ee/en/more-than-meets-the-ai-chinas-data-centre-strategy.
[22] Vladimir Lounegov, "How Tokenization of Assets Will Transform the Future of Finance," World Economic Forum, agosto 2025, https://www.weforum.org/stories/2025/08/tokenization-assets-transform-

piattaforme digitali, ma il controllo degli standard tecnici, regolatori e monetari attraverso cui circolano valore, liquidità e fiducia nell'economia globale.

In questo quadro, gli Stati Uniti partono da una posizione di forza strutturale: il ruolo internazionale del dollaro. La crescita delle *stablecoin* denominate in dollari tende infatti a proiettare l'egemonia monetaria americana dentro l'ecosistema digitale, trasformando asset privati emessi su *blockchain* in infrastrutture di pagamento globali ancorate alla liquidità statunitense. [23] La regolazione americana del settore, culminata nel 2025 con il "*GENIUS Act*" [24], segnala il tentativo di ricondurre l'espansione delle *stablecoin* entro un quadro normativo capace di rafforzare, più che indebolire, la centralità del dollaro. In altri termini, Washington non interpreta più il cripto-spazio soltanto come rischio finanziario o area speculativa, ma anche come possibile estensione della propria potenza monetaria.

La Cina, al contrario, ha seguito una traiettoria più selettiva e statocentrica. Dopo avere imposto forti restrizioni al *trading* e al *mining* di criptovalute, Pechino ha concentrato la propria attenzione sullo sviluppo dello yuan digitale e su infrastrutture di pagamento controllate, coerenti con una visione della finanza digitale come leva di sovranità e sorveglianza regolatoria.[25] Tuttavia, la difficoltà di trasformare l'*e-CNY* in uno strumento realmente internazionale mostra i limiti di un modello in cui l'innovazione monetaria resta strettamente subordinata al

future-of-finance; Hyun Song Shin "Tokenisation and the Future of the Monetary System," Bank for International Settlements (BIS), 24 giugno, 2025, https://www.bis.org/publ/arpdf/ar2025e3.htm

[23] Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law," The White House, 18 luglio 2025, https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/

[24] The GENIUS Act of 2025 Stablecoin Legislation Adopted in the US," Latham & Watkins, 24 luglio 2025, https://www.lw.com/en/insights/the-genius-act-of-2025-stablecoin-legislation-adopted-in-the-us

[25] Josh Lipsky and Ananya Kumar, "What to Watch as China Prepares Its Digital Yuan for Prime Time," Atlantic Council, 16 gennaio 2026, https://www.atlanticcouncil.org/blogs/econographics/what-to-watch-as-china-prepares-its-digital-yuan-for-prime-time/

controllo politico.[26] La competizione non oppone quindi semplicemente "cripto-libertà" americana e "controllo statale" cinese, ma due modalità diverse di costruire potere finanziario digitale: una fondata sulla proiezione internazionale del dollaro attraverso attori privati regolati; l'altra sulla costruzione di infrastrutture monetarie sovrane e politicamente governabili.

Questa dinamica incide anche sui mercati finanziari tradizionali. L'IA, i semiconduttori e il *compute* sono ormai diventati oggetto di aspettative di mercato, allocazione di capitale e strumenti finanziari dedicati. La prospettiva di mercati *futures* sulla capacità computazionale, basati sui costi di accesso alle *GPU*, segnala un passaggio significativo: il *compute* tende a essere trattato come una *commodity* strategica, analoga per certi versi all'energia nelle precedenti fasi dell'industrializzazione.[27] La competizione tecnologica produce quindi effetti diretti sui mercati, mentre i mercati, a loro volta, condizionano la capacità degli attori pubblici e privati di finanziare infrastrutture, *data center*, chip e modelli di IA.

La *blockchain*, in questa prospettiva, non va letta soltanto come tecnologia decentralizzata, ma come possibile infrastruttura di registrazione, scambio e regolazione del valore. La "*Bank for International Settlements (BIS)"* ha indicato nel 2025 la tokenizzazione come una delle direttrici della prossima architettura monetaria e finanziaria, soprattutto nei pagamenti transfrontalieri, nei titoli pubblici e nei mercati mobiliari. Al tempo stesso, ha avvertito che le *stablecoin*, se non adeguatamente regolate, possono generare rischi per la stabilità finanziaria

[26] Bank for International Settlements (BIS), "Shifting Forces Behind RMB Internationalization," BIS Working Papers, 2026, https://www.bis.org/publ/work1345.htm

[27] George Hammond and Antoine Gara, "Wall Street Wants a Market for AI Compute," Financial Times, 2025, https://www.ft.com/content/3e6b81e3-954d-4ac1-936b-00ea865bc98d

e per la sovranità monetaria, in particolare nelle economie più esposte alla dollarizzazione digitale.[28]

Ne deriva che la competizione tecnologica tra Stati Uniti e Cina non riguarda soltanto chip, cloud, IA e cybersicurezza, ma anche l'architettura finanziaria che sostiene l'economia digitale. Il controllo delle infrastrutture monetarie digitali può diventare un nuovo choke point: chi definisce gli standard della tokenizzazione, i requisiti di riserva delle stablecoin, l'interoperabilità tra piattaforme e l'accesso ai circuiti di pagamento digitali può influenzare non solo l'innovazione finanziaria, ma anche la distribuzione del potere monetario globale.[29]

In questa prospettiva, emerge una dinamica di reciproca strumentalizzazione delle interdipendenze, in cui tanto Washington quanto Pechino tendono a valorizzare i rispettivi punti di forza lungo le catene del valore. La competizione si configura così come un confronto tra *choke points* differenti ma interconnessi, in cui ciascun attore cerca di valorizzare le proprie leve per compensare vulnerabilità strutturali. Questo processo contribuisce alla formazione di ecosistemi tecnologici parzialmente distinti ma ancora interconnessi, nei quali l'accesso a componenti critiche, capacità produttive e infrastrutture computazionali viene sempre più mediato da considerazioni di natura politica e di sicurezza. In tale contesto, le *value chain* cessano di essere semplici architetture economiche e assumono una valenza eminentemente strategica, configurandosi come spazi di competizione e, al contempo, di gestione negoziata delle dipendenze reciproche.

[28] Bank for International Settlements (BIS), "III. The Next-Generation Monetary and Financial System," BIS Annual Economic Report 2025, 24 giugno 2025, https://www.bis.org/publ/arpdf/ar2025e3.htm
[29] R. Ahmed et al., "Stablecoins and Safe Asset Prices," BIS Working Papers No. 1270, Bank for International Settlements, 2025, https://www.bis.org/publ/work1270.pdf

Tuttavia, il controllo di queste infrastrutture non esaurisce la competizione: esso si estende anche al modo in cui tali capacità vengono utilizzate, difese e contestate nello spazio digitale.

Il dominio cyber come spazio di competizione permanente

La cybersicurezza, per esempio, si è progressivamente configurata come una forma di competizione permanente tra le due superpotenze, collocata al di sotto della soglia del conflitto aperto, ma capace di produrre effetti strategici rilevanti. Più che episodi isolati, le attività nel dominio *cyber* riflettono una dinamica continua di pressione, raccolta informativa e posizionamento, in cui spionaggio, compromissione delle *supply chain* e accesso alle infrastrutture critiche diventano strumenti ordinari della competizione tecnologica. Questa evoluzione trova un preciso riscontro anche sul piano dottrinale: negli Stati Uniti, concetti come *persistent engagement* e *defend forward*, sviluppati dallo "*U.S. Cyber Command"* [30] , riflettono l'idea di un cyberspazio caratterizzato da contatto costante tra attori, in cui la sicurezza si costruisce operando in modo continuativo anche nelle reti avversarie, prevenendo minacce prima che si manifestino.

Le operazioni attribuite a gruppi di spionaggio informatico avanzato (APT) come *Volt Typhoon*, sponsorizzato dallo stato cinese e attivo almeno dal 2021, illustrano in modo emblematico questa trasformazione. Secondo le analisi delle principali agenzie statunitensi [31] si tratta di campagne mirate a settori critici quali telecomunicazioni, energia, trasporti e gestione delle risorse idriche, condotte

[30] "Cyber 101 – Defend Forward and Persistent Engagement," U.S. Cyber Command, 25 ottobre 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

[31] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency (CISA), 7 febbraio 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

con l'obiettivo non di distruggere immediatamente, ma di pre-posizionarsi, acquisire accesso stabile a infrastrutture chiave, mantenendo la capacità potenziale di interferire o interrompere servizi in caso di escalation. In questo senso, la cybersicurezza diventa una forma di "deterrenza latente", basata sulla possibilità di attivare vulnerabilità già sfruttate, coerentemente con una logica di *campaigning* continuo piuttosto che di operazioni episodiche.

La postura americana riflette un'evoluzione parallela. Operazioni come lo smantellamento della *KV-Botnet* nel gennaio 2024 [32] indicano il definitivo passaggio da una logica puramente difensiva a una postura più attiva e offensiva, che include interventi diretti su infrastrutture malevole e reti utilizzate per mascherare attività sponsorizzate da stati. La distinzione tra difesa e offesa tende così a sfumare, mentre la cybersicurezza assume caratteristiche sempre più operative e integrate con le strategie di sicurezza nazionale, in linea con una visione del dominio cyber come spazio di confronto continuo.

Tra il 2024 e il 2025 è emerso con particolare chiarezza un ulteriore livello della competizione: quello delle infrastrutture di connettività. Le compromissioni su scala globale di *provider* di telecomunicazioni e dispositivi di rete, documentate da numerosi report congiunti delle principali agenzie occidentali,[33] mostrano come la competizione tecnologica si estenda alle "arterie" attraverso cui transitano dati e comunicazioni. L'accesso a queste infrastrutture consente non solo attività di raccolta informativa su larga scala, ma anche il posizionamento persistente all'interno di nodi critici dell'ecosistema digitale. Questo tipo di

[32] "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers," U.S. Department of Justice, Office of Public Affairs, 18 settembre, 2024, https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state.

[33] Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," Cybersecurity and Infrastructure Security Agency (CISA), 27 agosto 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

presenza abilita, in prospettiva, capacità di interferenza, rallentamento o interruzione selettiva dei flussi informativi, senza necessariamente oltrepassare la soglia del conflitto aperto.

Oltretutto, l'integrazione tra cyberspazio, IA e guerra dell'informazione all'interno della dottrina cinese dell'*intelligentized warfare*[34] segnala come il dominio digitale venga concepito non come ambito separato, ma come parte integrante della competizione militare e strategica contemporanea.

Nel complesso, quindi, il dominio *cyber* si configura come uno spazio di competizione continua, in cui la distinzione tra tempo di pace e tempo di guerra tende a dissolversi, e che non rappresenta più un livello separato della competizione tecnologica, ma una sua componente strutturale.

IA e potere sistemico: dalla competizione tecnologica al controllo dell'infrastruttura

Negli ultimi anni, la competizione sull'IA ha smesso di essere una corsa tecnologica in senso stretto per diventare una competizione sul controllo delle condizioni che rendono possibile l'innovazione. Non è più decisivo soltanto chi sviluppa il modello più avanzato, ma chi è in grado di sostenere nel tempo l'insieme di infrastrutture, dati e regole che ne permettono l'addestramento, la diffusione e l'integrazione nei sistemi economici e di sicurezza.[35]

La strategia statunitense riflette chiaramente questo cambio di paradigma. L'"*America's AI Action Plan*" del luglio 2025[36] collega esplicitamente sviluppo

[34] Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," The Cyber Defense Review, 19 dicembre 2024, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012231/the-path-to-chinas-intelligentized-warfare-converging-on-the-metaverse-battlefi/.
[35] Colin H. Kahl, "The Myth of the AI Race," Foreign Affairs, 12 gennaio 2026, https://www.foreignaffairs.com/united-states/myth-ai-race.
[36] "America's AI Action Plan", The White House, 23 luglio 2025, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

tecnologico, capacità industriale e sicurezza nazionale, trattando l'IA come un asset critico da integrare in una più ampia architettura di proiezione di potenza, rivolta verso avversari e competitors esterni. È in questa logica che si inseriscono strumenti come il già citato "*CHIPS and Science Act*", o iniziative di cooperazione strategica come "*AUKUS Pillar II*"[37] (2024) che estende la collaborazione tra Stati Uniti, Regno Unito e Australia alle tecnologie emergenti. Questa architettura si fonda su un ecosistema di grandi imprese che ne costituiscono la spina dorsale operativa. NVIDIA rappresenta il nodo centrale della capacità computazionale globale, fornendo *GPU* e *stack software* che costituiscono lo standard de facto per l'addestramento dei modelli avanzati di IA. Attorno a questo livello *hardware* si articola il dominio dei *cloud provider* - Google, Amazon e Microsoft - che controllano l'accesso alla capacità computazionale e ai dati su scala globale, investendo centinaia di miliardi di dollari per espandere *data center* e infrastrutture IA. A valle, attori come Palantir traducono queste capacità in applicazioni di sicurezza e *decision-making*, integrando l'IA nei processi operativi di governi e apparati di difesa. È in questo senso che la leadership sull'IA coincide sempre più con la capacità di orchestrare una rete integrata di attori pubblici e privati, piuttosto che con il semplice primato nella ricerca.

Sul versante cinese, la competizione viene interpretata secondo una logica sistemica, sostenuta da una combinazione di pianificazione industriale, indirizzo politico e leve materiali. Basta un rapido sguardo al "*Global AI governance Plan*" [38] del luglio 2025 per capire quale sia l'obiettivo di Pechino: integrare massicciamente l'IA nei settori produttivi strategici. In questo quadro, le grandi

[37] Adam Broinowski, "AUKUS Pillar 2," Parliamentary Library, Parliament of Australia, 15 agosto 2024, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2024/August/AUKUS_Pillar_2.

[38] Global AI Governance Action Plan," Ministry of Foreign Affairs of the People's Republic of China, 29 luglio 2025, https://www.fmprc.gov.cn/mfa_eng/xw/zyxw/202507/t20250729_11679232.html.

imprese tecnologiche svolgono un ruolo centrale nell'esecuzione di questa strategia. Huawei rappresenta il tentativo più avanzato di costruire un'alternativa nazionale allo *stack* tecnologico estero, sviluppando chip, infrastrutture *cloud* e soluzioni integrate. Colossi come Alibaba e Tencent, invece, guidano la diffusione industriale dell'IA attraverso piattaforme *cloud*, sviluppo di modelli e integrazione nei servizi digitali e nei sistemi produttivi, contribuendo a creare ecosistemi applicativi su larga scala.

A differenza dell'approccio statunitense, fortemente centrato sul controllo dei nodi tecnologici e sulla costruzione di alleanze, la strategia cinese privilegia la diffusione e l'integrazione sistemica. Pechino punta a radicare l'IA nei processi produttivi, sfruttando la scala del mercato interno e la densità industriale per accelerare l'adozione e generare vantaggi cumulativi. Questo modello è ulteriormente rafforzato da un vantaggio strutturale in ambiti quali l'accesso all'energia e il controllo delle filiere dei minerali critici, che costituiscono la base materiale dello sviluppo tecnologico cinese. In questa logica, il potere non deriva solo dalla capacità di sviluppare modelli avanzati, ma dalla possibilità di incorporarli stabilmente nell'economia reale.

In prospettiva, un ulteriore dominio destinato a intensificare la competizione è quello delle tecnologie quantistiche. A differenza dell'IA, il *quantum* non produce ancora effetti di massa sull'economia digitale, ma agisce già come tecnologia abilitante ad alto valore strategico nei campi del calcolo, delle comunicazioni sicure, della crittografia e del *sensing* avanzato.[39] La sua rilevanza deriva proprio dal carattere anticipatorio: chi riuscirà a costruire capacità industriali e

[39] Henning Soller, Martina Gschwendtner, Sara Shabani, and Waldemar Svejstrup, "The Year of Quantum: From Concept to Reality in 2025," McKinsey & Company, 23 giugno, 2025, https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

scientifiche mature nel *quantum* potrà incidere sulle future condizioni di sicurezza delle comunicazioni, sulla simulazione di materiali e farmaci, sull'ottimizzazione industriale e, potenzialmente, sulla vulnerabilità degli attuali sistemi crittografici.[40]

Gli Stati Uniti mantengono un vantaggio rilevante nella combinazione tra università, laboratori federali, difesa e capitale privato. Il "*National Quantum Initiative Act*" del 2018[41] ha fornito il quadro di coordinamento della leadership americana, mentre nel novembre 2025 il "*Department of Energy*" ha annunciato 625 milioni di dollari per rinnovare i cinque "*National Quantum Information Science Research Centers*" con l'obiettivo di consolidare *hardware*, applicazioni e partenariati industriali.[42] Anche in questo caso, la logica americana non è solo scientifica: si tratta di costruire un ecosistema in grado di collegare ricerca di base, trasferimento tecnologico, sicurezza nazionale e capacità produttive.

La Cina, dal canto suo, considera il *quantum* una componente essenziale della propria strategia di autonomia tecnologica. Pechino ha investito per anni in comunicazioni quantistiche, crittografia, satelliti sperimentali e calcolo quantistico, sostenendo un ecosistema fortemente concentrato attorno a università, laboratori nazionali e grandi programmi pubblici.[43] Nel 2026, i progressi cinesi nel calcolo quantistico, inclusi processori sperimentali e prime

[40] Dustin Moody, "Transition to Post-Quantum Cryptography Standards," National Institute of Standards and Technology (NIST), 12 novembre, 2024, https://csrc.nist.gov/pubs/ir/8547/ipd

[41] National Quantum Initiative Act," U.S. Congress, 21 dicembre, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6227

[42] Energy Department Announces $625 Million to Advance Next Phase of National Quantum Information Science Research Centers," U.S. Department of Energy, 6 novembre, 2025, https://www.energy.gov/articles/energy-department-announces-625-million-advance-next-phase-national-quantum-information.

43 William Alan Reinsch, "Understanding China's Quest for Quantum Advancement," Center for Strategic and International Studies (CSIS), 2025, https://www.csis.org/analysis/understanding-chinas-quest-quantum-advancement

forme di *deployment* commerciale, hanno confermato la volontà di trasformare il quantum da ambito di ricerca avanzata a settore strategico-industriale.[44]

La competizione quantistica presenta però una differenza rispetto a quella sull'IA. Nel caso dell'intelligenza artificiale, la leva principale è la scala: dati, *compute*, modelli, *cloud* e capacità di integrazione industriale. Nel *quantum*, invece, la competizione è ancora più concentrata sulla profondità scientifica, sulla qualità del capitale umano, sulla capacità di produrre *hardware* estremamente complesso e sulla costruzione di *supply chain* specializzate. Non è quindi una corsa immediatamente misurabile in termini di adozione commerciale, ma una competizione di lungo periodo per il controllo delle infrastrutture future della sicurezza digitale.

Il punto più sensibile riguarda la crittografia. Un *quantum computing* maturo potrebbe compromettere alcuni degli algoritmi oggi alla base della sicurezza delle comunicazioni, delle transazioni finanziarie e delle infrastrutture digitali. Per questo, la transizione verso la crittografia post-quantistica non è soltanto un tema tecnico, ma un problema di sicurezza nazionale e resilienza sistemica. Gli Stati che arriveranno prima a standardizzare, implementare e diffondere soluzioni crittografiche *quantum-resistant* potranno ridurre la propria esposizione e, al tempo stesso, riscrivere gli standard globali della sicurezza digitale.[45]

In questo senso, il *quantum* completa il quadro della competizione tecnologica tra Stati Uniti e Cina. Se i semiconduttori rappresentano il collo di bottiglia materiale

[44] China's Quantum Computing Development Enters New Stage," Xinhua News Agency, 13 maggio, 2026, https://english.news.cn/20260513/01e78cf35c684afda7b7451d063970e6/c.html

[45] Next Steps in Preparing for Post-Quantum Cryptography," National Cyber Security Centre (NCSC), 4 novembre, 2025, https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography

dell'IA, e se il cyberspazio costituisce il terreno permanente della competizione, le tecnologie quantistiche rappresentano la frontiera successiva: meno visibile nell'immediato, ma potenzialmente decisiva nel ridefinire i rapporti di forza futuri. Anche qui, dunque, la competizione non riguarda solo l'invenzione tecnologica, ma la capacità di trasformarla in infrastruttura, standard, filiera e potere strategico.

Ne deriva una competizione tra modelli di potere tecnologico più che tra singole tecnologie. Da un lato, un approccio che mira a controllare i nodi critici dello sviluppo e a strutturare alleanze attorno a standard e infrastrutture, facendo leva su un ecosistema di imprese globali altamente integrate; dall'altro, un modello che privilegia la diffusione e l'integrazione industriale, sostenuto da una stretta interazione tra Stato e grandi attori tecnologici. In questo quadro, la "corsa all'IA" non ha un unico punto di arrivo né un vincitore definito: si articola piuttosto nella capacità di tradurre tecnologia in organizzazione economica, capacità industriale e influenza strategica.[46]

Le ricadute della competizione sull'Europa e sull'Italia

Per l'UE, la competizione tecnologica tra Stati Uniti e Cina si traduce in una ridefinizione strutturale delle condizioni di accesso al potere tecnologico. Tre sono le ricadute principali. In primo luogo, il rischio di un progressivo *tiering* tecnologico: regimi di *export control*, accordi industriali e architetture di alleanza tendono a organizzare l'accesso a chip, *cloud* e modelli di IA secondo una gerarchia di fiducia, con implicazioni dirette per l'autonomia industriale, la capacità militare e la libertà decisionale degli Stati europei. In secondo luogo,

[46] Alvin Wang Graylin, Paul Triolo, "There Can Be No Winners in a U.S.-China AI Arms Race," MIT Technology Review, 21 gennaio 2025, https://www.technologyreview.com/2025/01/21/1110269/there-can-be-no-winners-in-a-us-china-ai-arms-race/.

aumenta la pressione a scegliere standard, infrastrutture e *stack* tecnologici che non sono più neutrali, ma incorporano visioni politiche, modelli di governance e vincoli di sicurezza. In terzo luogo, cresce il costo della resilienza: l'integrazione di requisiti di sicurezza *by design* lungo le filiere e di obblighi di compliance avanzata richiede investimenti, competenze e massa critica che, in assenza di adeguata scala europea, rischiano di tradursi in nuove forme di dipendenza da fornitori esterni considerati *trusted*.

La posizione di Bruxelles si colloca in un equilibrio instabile tra ambizione regolatoria ed esigenze di competitività, in un contesto di crescente accelerazione tecnologica globale. Il rischio è che un'impostazione eccessivamente centrata sulla dimensione normativa finisca per tradursi in una dipendenza strutturale da tecnologie sviluppate altrove, riducendo la capacità dell'Unione di incidere in modo autonomo sugli equilibri del sistema tecnologico internazionale.

Ne emerge una scelta strategica di fondo: restare prevalentemente una *regulatory power*, capace di orientare le regole ma inserita in architetture tecnologiche definite da altri, oppure evolvere verso una forma più integrata di potere tecnologico, in cui norme, capacità industriali, infrastrutture e sicurezza concorrano alla costruzione di autonomia strategica e influenza. In assenza di una sufficiente massa critica industriale però, la regolazione rischia di ridursi a governance priva di leva strategica.

In questo contesto, l'Italia si colloca come attore intermedio: sul piano infrastrutturale, la presenza di un ecosistema avanzato di high-performance computing e la selezione di "*IT4LIA*" al DAMA Tecnopolo di Bologna tra le prime

"*AI Factories*" europee[47] costituiscono un punto di leva per lo sviluppo di capacità di calcolo a supporto del sistema Paese.

Sul piano istituzionale e diplomatico, la principale novità del periodo 2025–2026 è rappresentata dalla riforma che ha introdotto la "Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica" presso il Ministero degli Affari Esteri e della Cooperazione Internazionale. L'attuale assetto della nuova Direzione della Farnesina[48] potrebbe fornire nuova linfa alla diplomazia cibernetica, attraverso la cooperazione internazionale su IA e digitale e con la partecipazione a iniziative multilaterali quali il "*Pall Mall Process*" e la "*Counter Ransomware Initiative*". Questa innovazione organizzativa consente di integrare in modo più coerente politica estera, requisiti tecnici e dimensione industriale.

Da questa configurazione emergono tre potenziali linee operative. La prima riguarda il *cyber capacity building* nella competizione globale, l'influenza si misura anche nella capacità di esportare competenze, standard e pratiche operative, in particolare verso aree ad alta esposizione come il Mediterraneo allargato e l'Africa, contribuendo a ridurre dipendenze coercitive e a costruire interoperabilità con ecosistemi euro-atlantici. La seconda è una *cyber diplomacy* in chiave europea: valorizzare asset come Bologna ed EuroHPC come piattaforme per progetti strategici basati su criteri stringenti di sicurezza, standardizzazione e trasferibilità, trasformando l'infrastruttura computazionale in leva geopolitica. La terza è una "diplomazia delle filiere" applicata all'IA, che integri controllo delle esportazioni, sicurezza della *supply chain* e resilienza *cyber* in una posizione

[47] "AI via IT4LIA AI Factory: l'Italia tra i leader europei dell'intelligenza artificiale," Agenzia per la Cybersicurezza Nazionale (ACN), 8 settembre 2025, https://www.acn.gov.it/portale/w/al-via-it4lia-ai-factory-l-italia-tra-i-leader-europei-dell-intelligenza-artificiale.
[48] "Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica," Ministero degli Affari Esteri e della Cooperazione Internazionale, https://www.esteri.it/it/ministero/struttura/dgct/.

coerente nei fori multilaterali, evitando che standard e normative diventino veicoli impliciti di dipendenza strategica.

Chiaramente, la dimensione multilaterale rimane essenziale. Nel 2025 si è concluso il ciclo dello "*UN Open-Ended Working Group*" sulla sicurezza delle ICT[49], con l'adozione del report finale e l'avvio di un meccanismo più permanente di dialogo, sostenuto anche dall'UE. In questo quadro, l'Italia dispone di un potenziale punto di sintesi tra capacità tecniche e proiezione diplomatica: la combinazione tra le nuove capacità della Farnesina in materia, le infrastrutture europee e le competenze nazionali consente, almeno in linea di principio, di collegare la dimensione normativa e multilaterale con iniziative operative, trasformando la competizione globale da vincolo esterno a spazio di iniziativa strategica.

[49] UN OEWG 2021–2025 Final Report, United Nations, 11 luglio 2025, https://dig.watch/resource/oewg-report-2021-2025.

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale (ACN). (2025). *Al via IT4LIA AI Factory: l'Italia tra i leader europei dell'intelligenza artificiale*. Consultabile su: https://www.acn.gov.it/portale/w/al-via-it4lia-ai-factory-l-italia-tra-i-leader-europei-dell-intelligenza-artificiale.

Ahmed R. et al. (2025). *Stablecoins and Safe Asset Prices*. BIS Working Papers No. 1270, Bank for International Settlements (BIS). Consultabile su: https://www.bis.org/publ/work1270.pdf

Allen, Gregory C. (2023). *China's New Strategy for Waging the Microchip Tech War.* Center for Strategic and International Studies (CSIS). Consultabile su: https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war.

Allen, Gregory. C. (2024). *Understanding the Biden Administration's Updated Export Controls.* Center for Strategic and International Studies (CSIS). Consultabile su: https://www.csis.org/analysis/understanding-biden-administrations-updated-export-controls

Bank for International Settlements (BIS). (2025). III. *The Next-Generation Monetary and Financial System.* BIS Annual Economic Report 2025. Consultabile su: https://www.bis.org/publ/arpdf/ar2025e3.htm.

Baughman, J. (2024). *The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield*. The Cyber Defense Review. Consultabile su: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012231/the-path-to-chinas-intelligentized-warfare-converging-on-the-metaverse-battlefi/.

Broinowski, A. (2024). *AUKUS Pillar 2*. Parliamentary Library, Parliament of Australia. Consultabile su: https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/FlagPost/2024/August/AUKUS_Pillar_2.

Brookings. (2021). *U.S.-China technology competition. A Brookings Global China Interview*. Consultabile su: https://www.brookings.edu/articles/u-s-china-technology-competition/

Center for a New American Security. (2024). “Promethean Rivalry: The World-Altering Stakes of Sino-American AI Competition.” Consultabile su: https://www.cnas.org/publications/reports/promethean-rivalry

Cybersecurity and Infrastructure Security Agency (CISA). (2024). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Consultabile su: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Cybersecurity and Infrastructure Security Agency (CISA). (2025). *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*. Consultabile su: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

Council on Foreign Relations. (2025). “China, the United States, and the AI Race.” Consultabile su: https://www.cfr.org/articles/china-united-states-and-ai-race

Electronic Code of Federal Regulations (eCFR). *15 CFR § 734.9 – Foreign-Direct Product (FDP) Rules*. Consultabile su: https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.9.

Federal Register. (2023). *Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Entity List Modification*. Consultabile su: https://www.federalregister.gov/documents/2023/10/25/2023-23055/implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and.

Groenewegen-Lau J. (2024). *Whole-of-nation innovation: Does China’s socialist system give it an edge in science and technology?* MERICS. Consultabile su: https://merics.org/en/report/whole-nation-innovation-does-chinas-socialist-system-give-it-edge-science-and-technology

Hammond G., Gara A. (2025). *Wall Street Wants a Market for AI Compute*. Financial Times. Consultabile su: https://www.ft.com/content/3e6b81e3-954d-4ac1-936b-00ea865bc98d

Hanso, T. (2025). *More Than Meets the AI: China’s Data Centre Strategy*. International Centre for Defence and Security (ICDS). Consultabile su: https://icds.ee/en/more-than-meets-the-ai-chinas-data-centre-strategy.

International Energy Agency (IEA). (2026). *Rare Earth Elements – Executive Summary*. Consultabile su: https://www.iea.org/reports/rare-earth-elements/executive-summary.

Kahl, Colin H. (2026). *The Myth of the AI Race.* Foreign Affairs. Consultabile su: https://www.foreignaffairs.com/united-states/myth-ai-race.

Kim T-Y., Dhir S., Dasgupta A., Scanziani A. (2025). *With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality*. International Energy Agency (IEA). Consultabile su: https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality.

Klinck H. (2025). *The Cold War Paradigm is Inadequate for U.S.-China Strategic Competition.* Ronald Reagan Institute. Consultabile su: https://www.reaganfoundation.org/reagan-institute/publications/the-cold-war-paradigm-is-inadequate-for-u-s-china-strategic-competition-vol6?utm_source=chatgpt.com

Kuo, K. (2025). *How China Is Reinventing the Future of Global Manufacturing*. World Economic Forum. Consultabile su: https://www.weforum.org/stories/2025/06/how-china-is-reinventing-the-future-of-global-manufacturing/.

Kurilla, M. (2024). *What Is the CHIPS Act?* Council on Foreign Relations. Consultabile su: https://www.cfr.org/articles/what-chips-act.

Latham & Watkins. (2025). *The GENIUS Act of 2025 Stablecoin Legislation Adopted in the US*. Consultabile su: https://www.lw.com/en/insights/the-genius-act-of-2025-stablecoin-legislation-adopted-in-the-us

Lipsky J., Kumar A. (2026). *What to Watch as China Prepares Its Digital Yuan for Prime Time*. Atlantic Council. Consultabile su: https://www.atlanticcouncil.org/blogs/econographics/what-to-watch-as-china-prepares-its-digital-yuan-for-prime-time/

Lounegov V. (2025). *How Tokenization of Assets Will Transform the Future of Finance*. World Economic Forum. Consultabile su: https://www.weforum.org/stories/2025/08/tokenization-assets-transform-future-of-finance

Miller C. (2022). *Chip War: The Fight for the World's Most Critical Technology*. New York: Scribner.

Ministry of Commerce of the People's Republic of China. (2023). *MOFCOM Regular Press Conference (6 luglio 2023).* Consultabile su: https://english.mofcom.gov.cn/News/PressConference/art/2023/art_36fb2d80e4b4453891bb8fc83e2b3c4e.html.

Ministry of Foreign Affairs of the People's Republic of China. (2025). *Global AI Governance Action Plan*. Consultabile su: https://www.fmprc.gov.cn/mfa_eng/xw/zyxw/202507/t20250729_11679232.html.

Moody D. (2024). *Transition to Post-Quantum Cryptography Standards*. National Institute of Standards and Technology (NIST). Consultabile su: https://csrc.nist.gov/pubs/ir/8547/ipd

National Cyber Security Centre (NCSC). (2025). *Next Steps in Preparing for Post-Quantum Cryptography*. Consultabile su: https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography

Reinsch W.A. (2025). *Understanding China's Quest for Quantum Advancement*. Center for Strategic and International Studies (CSIS). Consultabile su: https://www.csis.org/analysis/understanding-chinas-quest-quantum-advancement

Shin H.S. (2025). Tokenisation and the Future of the Monetary System. Bank for International Settlements (BIS). Consultabile su: https://www.bis.org/publ/arpdf/ar2025e3.htm

Soller H., Gschwendtner M., Shabani S., Svejstrup W. (2025). *The Year of Quantum: From Concept to Reality in 2025*. McKinsey & Company. Consultabile su: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

The White House. (2025). *America's AI Action Plan*. Consultabile su: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

United Nations. (2025). *UN OEWG 2021–2025 Final Report*. Consultabile su: https://dig.watch/resource/oewg-report-2021-2025.

U.S. Congress. (2018). *National Quantum Initiative Act*. Consultabile su: https://www.congress.gov/bill/115th-congress/house-bill/6227.

U.S. Cyber Command. (2022). *Cyber 101 – Defend Forward and Persistent Engagement.* Consultabile su: https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

U.S. Department of Commerce, Bureau of Industry and Security. (2022). *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC).* Consultabile su: https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples.

U.S. Department of Commerce, Bureau of Industry and Security. (2024). *Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications*. Consultabile su: https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military.

U.S. Department of Commerce, Bureau of Industry and Security. (2025). *Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls.* Consultabile su: https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens.

U.S. Department of Energy. (2025). Energy Department Announces $625 Million to Advance Next Phase of National Quantum Information Science Research Centers. Consultabile su: https://www.energy.gov/articles/energy-department-announces-625-million-advance-next-phase-national-quantum-information

U.S. Department of Justice, Office of Public Affairs. (2024). *Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers*. Consultabile su: https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state.

U.S. Department of State. (2025). *Pax Silica*. Consultabile su: https://www.state.gov/pax-silica

Wang Graylin A., Triolo P. (2025). *There can be no winners in a US-China AI arms race*. Consultabile su: https://www.technologyreview.com/2025/01/21/1110269/there-can-be-no-winners-in-a-us-china-ai-arms-race/

Xinhua News Agency. (2026). *China's Quantum Computing Development Enters New Stage*. Consultabile su: https://english.news.cn/20260513/01e78cf35c684afda7b7451d063970e6/c.html

BIOGRAFIA DELL'AUTORE

Gregorio Staglianò è ricercatore del Centro Studi Geopolitica.info per il programma Cyber e Tech. I suoi interessi di ricerca si concentrano sull'intersezione tra sicurezza cibernetica, tecnologie emergenti e competizione geopolitica tra le grandi potenze, con particolare attenzione alle implicazioni strategiche dell'innovazione tecnologica per la sicurezza internazionale e l'autonomia tecnologica europea. Si occupa di cybersecurity e governance dei rischi digitali anche per il settore privato. Scrive e interviene regolarmente su temi di politica internazionale, sicurezza digitale e innovazione tecnologica, contribuendo al dibattito pubblico e collaborando con centri di ricerca, riviste di analisi geopolitica e media

Geopolitica.info

CENTRO STUDI

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online Geopolitica.info e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

I Report del Centro Studi

I report del Centro Studi Geopolitica.info sono collezioni di saggi, realizzati dai ricercatori afferenti alle varie aree del Centro, dedicati ai grandi temi dell'attualità della politica internazionale. Pubblicati a cadenza trimestrale, i report si contraddistinguono per il rigore metodologico e la profondità analitica. Combinando insieme accessibilità e solidità scientifica, essi offrono analisi rigorose e tempestive sui principali dossier della scena globale.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info