Geopolitica·info

Con il supporto di Ministero degli Affari Esteri e della Cooperazione Internazionale

Con la collaborazione scientifica di CEMAS

GovTech

Governare l'era tecnologica: l'Italia tra cybersecurity, intelligenza artificiale e nuove sfide internazionali

A cura di Alessandro Savini e Gregorio Stiglianò

www.geopolitica.info

Il report 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.

INDICE

Cyberspazio conteso: attori, conflitti e vulnerabilità

Alessandra Russo

Introduzione

Il cyberspazio è da anni dominio interessato da un alto grado di conflittualità, caratterizzato dalla frammentazione del monopolio sull'uso della forza e nel quale nell'ultima decade si sono moltiplicati attori e minacce. Nel cyberspazio operano Stati, attori minori ad essi affiliati, cybercriminali, hacktivisti, e attori non statali capaci di condurre operazioni anche complesse e ad alto impatto con costi relativamente bassi. Questa diversificazione di attori è favorita dall'asimmetria intrinseca del cyberspazio, dalle numerose vulnerabilità dei sistemi informatici e dalla difficoltà di attribuzione degli attacchi, elementi che rendono la difesa assai più onerosa dell'attacco. Le campagne cibernetiche contemporanee mirano a influenzare equilibri politici e strategici attraverso attività prolungate di spionaggio, manipolazione informativa e sabotaggio di infrastrutture critiche.

La difesa del cyberspazio è cruciale per la sicurezza e la resilienza degli Stati, data l'interdipendenza tecnologica strutturale tra infrastrutture critiche e sistemi informatici. La concentrazione di servizi globali su pochi provider accresce i rischi sistemici, aumentando le conseguenze potenziali di attacchi anche relativamente semplici. Conflitti in corso come la guerra russo-ucraina e il conflitto israelo-palestinese mostrano come il cyberspazio sia estensione del fronte: esso è usato in preparazione e a supporto delle operazioni convenzionali per indebolire infrastrutture critiche, diffondere disinformazione ed esercitare pressione su popolazioni e governi avversari. L'impatto operativo delle operazioni nel cyberspazio resta tuttavia contenuto e complementare rispetto alla dimensione cinetica dei conflitti.

In questo quadro l'Italia è un attore particolarmente esposto ma anche sempre più proattivo. Gli indirizzi fissati dalla Strategia Nazionale di Cybersicurezza 2022-2026 puntano al progressivo rafforzamento del coordinamento inter-istituzionale, in cui l'azione italiana si inserisce nei quadri UE e NATO per contribuire alla definizione di standard comuni e meccanismi di risposta collettiva alle minacce cibernetiche. L'Italia risulta esposta a un volume crescente di minacce cibernetiche: negli ultimi anni si è verificato un aumento significativo di eventi ad alto impatto come infiltrazioni nei sistemi, esfiltrazioni di dati e attività attribuibili ad attori altamente sofisticati. In reazione a quest'esposizione la postura nazionale si sta orientando verso un approccio proattivo fondato su prevenzione, riduzione delle vulnerabilità sistemiche e sviluppo di infrastrutture resilienti dotate di capacità di ripristino rapido. Sul piano esterno la Farnesina ha rafforzato il proprio ruolo nella cybersicurezza e nella diplomazia digitale per mezzo della costituzione della nuova Direzione Generale per le questioni cibernetiche, l'informatica e l'innovazione tecnologica, struttura che presidia le politiche internazionali in materia di sicurezza cibernetica, contrasto alla disinformazione e intelligenza artificiale, oltre a coordinare la gestione e l'innovazione tecnologica dell'amministrazione centrale e della propria rete estera. La priorità strategica dell'Italia non è dunque l'eliminazione totale del rischio, bensì lo sviluppo della capacità di limitare l'impatto degli attacchi e garantire la continuità dei servizi essenziali e delle funzioni critiche dello Stato attraverso una gestione proattiva dell'ecosistema digitale nonché attraverso la cooperazione in campo internazionale e inter-istituzionale nell'ambito della difesa e della diplomazia cibernetica.

Diversificazione di attori e minacce nel cyberspazio

Il cyberspazio, definito come dominio globale all'interno dell'ambiente informativo costituito da reti interdipendenti di infrastrutture informatiche e dati (*ivi* compreso Internet), reti di telecomunicazione, e sistemi informatici[1], è ormai da molti anni a pieno titolo un dominio a sé in cui si svolgono sovente operazioni di "zona grigia"[2] e di guerra ibrida.[3] La sicurezza del cyberspazio è oggi indissolubilmente connessa a quella degli Stati e delle loro infrastrutture critiche. Già nel 2016 l'allora Segretario Generale della NATO, Jens Stoltenberg – a seguito del Summit di Varsavia, riconoscendo il dominio cyber come quinto dominio di conflittualità – affermava che un cyber attacco di particolare gravità avrebbe potuto costituire motivo di attivazione dell'Articolo 5 del Trattato dell'Alleanza Atlantica, al pari di un attacco armato convenzionale.[4]

Per questo motivo, negli ultimi due decenni il cyberspazio è stato oggetto di crescente contestazione contribuendo (e subendo a propria volta) una progressiva frammentazione del tradizionale monopolio statale sull'uso della forza, vedendo una diversificazione e moltiplicazione degli attori e delle minacce operanti al suo interno. Nel corso degli ultimi dieci anni il panorama delle minacce si è notevolmente ampliato e diversificato: se nella decade 2005-2015 l'attenzione era rivolta principalmente a un numero limitato di Stati e ad alcune organizzazioni cybercriminali, ad oggi è presente una varietà molto più ampia di

[1] Catherine A. Theohary, *Defense Primer: Cyberspace Operations*, Congressional Research Service, 2024, https://www.congress.gov/crs-product/IF10537.

[2] Operazioni ostili che si collocano in uno "spazio operativo tra guerra e pace" che sovente consistono in una serie di faits accomplis e che sono in grado di raggiungere obiettivi strategici anche significativi senza mai arrivare alla guerra aperta. Queste operazioni rimangono sotto la soglia che giustificherebbe una risposta militare, si sviluppano gradualmente nel tempo, sono spesso di difficile attribuzione e mirano a evitare reazioni decisive colpendo obiettivi limitati (Morris et al., 2019, pp. 8–10).

[3] La guerra ibrida vede la commistione di strumenti militari convenzionali e non convenzionali come, oltre agli attacchi cibernetici, operazioni clandestine, uso di forze irregolari, campagne di disinformazione, coercizione economica, lawfare, e sabotaggi a infrastrutture critiche (Hoffman, 2007, p. 58).

[4] "Warsaw Summit Communiqué", North Atlantic Treaty Organization (NATO), 9 luglio 2016, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique.

attori. Il panorama delle minacce contemporaneo continua a vedere come maggiori entità attori statali in grado di condurre attacchi sofisticati, vedasi il caso celeberrimo di Stuxnet nel 2010 contro l'Iran;[5] ma anche operazioni complesse e sostenute nel tempo di cyberspionaggio e infiltrazione. Vi è altresì una moltitudine di attori minori che possono essere affiliati o sponsorizzati da Stati, di cui un esempio tra i moltissimi è il gruppo *Fancy Bear* affiliato alla Russia.[6] Nel cyberspazio operano organizzazioni militanti e terroristiche come Hamas ed Hezbollah,[7] ma anche attori come gruppi cybercriminali e hacktivisti, sia affiliati a Stati – come Cina e Russia – sia indipendenti come l'ormai celebre *Anonymous*, che utilizzano il cyberspazio come piattaforma per condurre attività legate ad attivismo politico aggressivo.[8] Inoltre, i confini tra le diverse tipologie di attori nel cyberspazio risultano sempre più sfumati. In particolare, alcuni Stati ricorrono intenzionalmente a una pluralità di attori intermedi, gruppi affiliati o proxy per condurre operazioni cibernetiche, al fine di preservare la cosiddetta *plausible deniability*, ossia la possibilità di negare in modo credibile il proprio coinvolgimento diretto e di eludere responsabilità politiche, giuridiche o militari legate all'attribuzione delle operazioni.[9] Parallelamente, attori tradizionalmente riconducibili alla criminalità informatica possono operare sotto coperture

[5] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404, https://doi.org/10.1080/09636412.2013.816122.

[6] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 agosto 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[7] Daniel Byman and Eric McCaleb, "Understanding Hamas's and Hezbollah's Uses of Information Technology," Center for Strategic and International Studies (CSIS), 24 ottobre, 2023, https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology.

[8] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 371; *ENISA Threat Landscape 2025*, European Union Agency for Cybersecurity (ENISA), 2025, https://www.enisa.europa.eu/sites/default/files/2025-.

[9] Sébastien Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security," *Contemporary Security Policy* 40, no. 3 (2019): 368–381, https://doi.org/10.1080/13523260.2019.1581458.

ideologiche o politiche, contribuendo a confondere ulteriormente la distinzione tra attività criminali, operazioni di influenza e azioni ostili riconducibili a interessi statali. La convergenza e la sovrapposizione in termini di strumenti, tecniche, e tipi attacchi usati da questi attori complicano ulteriormente il cyberspazio.[10] Difatti, attori statali, para-statali e privati nel cyberspazio non si concentrano più esclusivamente su singoli attacchi, ma su campagne prolungate che comprendono più operazioni collegate tra loro. Queste campagne mirano a ottenere risultati strategici, come lo spostamento dell'equilibrio relativo del potere nazionale sfruttando operazioni di zona grigia e di guerra ibrida senza dover ricorrere al conflitto armato.[11] In un contesto di conflitto armato, invece, il dominio cibernetico vede operazioni svolte in parallelo a quelle svolte nei domini tradizionali (terrestre, marittimo, e aereo) in preparazione o a supporto alle operazioni convenzionali, come è evidente nel caso dei cyberattacchi alla Georgia nel 2008 e le operazioni precedenti e condotte durante l'invasione russa dell'Ucraina del 2022. L'attuale panorama del cyberspazio si caratterizza per un'elevata complessità e densità di attori. Pur mantenendo una posizione centrale in termini di capacità e risorse, gli Stati vedono progressivamente erodersi la propria autorità, sicurezza e, soprattutto, il tradizionale monopolio sull'uso legittimo della forza nel dominio cibernetico. Tale dinamica è alimentata dall'emergere di attori statali e non statali di diversa natura, dimensione e livello di sofisticazione, che adottano strategie e conducono operazioni sempre più audaci e ad alto rischio, con il potenziale di generare effetti destabilizzanti sull'equilibrio e sulla stabilità del sistema internazionale.[12]

[10] ENISA, Threat Landscape 2025.

[11] Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," Journal of Strategic Studies 45, no. 4 (2022): 534–567, https://doi.org/10.1080/01402390.2020.1732354

[12] Sébastien Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security,"

Asimmetria e vulnerabilità

La molteplicità di attori sin qui evidenziata è favorita da alcune caratteristiche strutturali del cyberspazio, in particolare dall'asimmetria delle capacità e dalla persistente difficoltà di attribuzione degli attacchi. L'asimmetria consente ad attori dotati di risorse tecniche ed economiche relativamente limitate di competere con, e arrecare danni a, controparti significativamente più potenti attraverso l'impiego di strumenti cibernetici. Le barriere di ingresso per molte tipologie di attacco informatico risultano relativamente basse, generando un vantaggio strutturale per gli attori dotati di capacità cibernetiche offensive. Per tali attori, la conduzione delle operazioni comporta costi e livelli di rischio significativamente inferiori rispetto a quelli sostenuti dai soggetti chiamati a difendere i propri sistemi, i quali devono invece affrontare investimenti elevati e continuativi per proteggere una superficie di attacco ampia ed eterogenea, composta da sistemi, reti e infrastrutture interconnesse.[13] Tale asimmetria è ulteriormente accentuata dalla natura intrinsecamente vulnerabile del cyberspazio, caratterizzato da una diffusione pervasiva di vulnerabilità e da una molteplicità di punti di accesso e vettori di attacco, che rendono complessi e onerosi gli sforzi necessari a garantirne la sicurezza.[14]

Un esempio emblematico di attacco a basso costo e ad alto impatto è rappresentato dai Distributed Denial of Service (DDoS), la cui esecuzione può comportare per l'aggressore un costo estremamente contenuto, talvolta pari a poche decine di dollari. Al contrario, le misure necessarie per prevenirli, mitigarli e gestirne gli effetti possono richiedere investimenti significativamente

[13] Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/pubs/monographs/MG877.html.

[14] Sébastien Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security,", pp. 270-271.

più elevati, spesso nell'ordine di decine di migliaia di dollari.[15] Gli attacchi DDoS mirano a rendere indisponibili servizi digitali legittimi saturando deliberatamente la capacità di gestione del traffico dell'obiettivo – ad esempio un sito web o un servizio online – attraverso un volume massivo di richieste simultanee, compromettendone l'accessibilità per gli utenti autorizzati. Una minaccia di natura più sofisticata è rappresentata dalle cosiddette Advanced Persistent Threats (APT), ossia campagne cibernetiche prolungate e mirate, finalizzate a operazioni di spionaggio, esfiltrazione di dati sensibili o sabotaggio. Tali operazioni si caratterizzano per l'impiego di tecniche di infiltrazione avanzate, per l'elevato grado di persistenza e furtività, e sono generalmente condotte da attori altamente qualificati – spesso riconducibili a Stati o a gruppi che agiscono per loro conto – ai danni di obiettivi specifici, quali infrastrutture critiche, aziende strategiche o apparati governativi.[16] Accanto a queste tipologie di minaccia esistono anche gli attacchi che sfruttano vulnerabilità zero-day, ovvero difetti e vulnerabilità software non ancora noti al fornitore e per i quali non esiste una patch disponibile[17] e i cosiddetti *ransomware*, ovvero attacchi volti al sequestro di dati e alla contestuale richiesta pagamento di un riscatto sovente effettuati da cybercriminali. Al fine di contrastare il fenomeno dei *ransomware*, l'Italia – rappresentata da MAECI e ACN – partecipa alla *Counter Ransomware Initiative*: un'iniziativa multilaterale informale lanciata nel 2021 che riunisce

[15] Alexander Klimburg, The Darkening Web: The War for Cyberspace (New York: Penguin Publishing Group, 2017), 48.

[16] Asad Ahmad, Jamie Webb, Kevin C. Desouza, and James Boorman, "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security* 86 (2019): 402–418, https://doi.org/10.1016/j.cose.2019.07.001.

[17] Lillian Ablon and Andy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits (Santa Monica, CA: RAND Corporation, 2017).

circa 60 Paesi che istituisce meccanismi di condivisione di informazioni, ricerche e linee guida operative.[18]

Da ultimo, è bene notare come la rapida diffusione ed evoluzione dell'intelligenza artificiale (IA) sta trasformando il cyberspazio, fornendo strumenti potenti sia per la difesa sia per l'offesa. Sul fronte difensivo, l'IA potenzia il rilevamento di vulnerabilità e minacce, accelera le risposte agli incidenti e consente processi di difesa automatizzati e adattivi.[19] Sul fronte offensivo, invece, l'IA facilita l'individuazione di debolezze nei sistemi avversari e l'esecuzione di operazioni su larga scala in maniera rapida e automatizzata, come evidenziato da recenti episodi di cyberspionaggio attribuiti a gruppi di matrice cinese che hanno impiegato agenti di IA per condurre attacchi sofisticati.[20]

Il cyberspazio nei conflitti contemporanei: la guerra russo-ucraina, il conflitto israelo-palestinese e le operazioni israelo-statunitensi contro l'Iran

La crescente frammentazione del cyberspazio e la pluralità di attori e minacce al suo interno si riflettono nei conflitti in corso, in cui il dominio cibernetico diventa parte integrante di quelli tradizionali. La guerra russo-ucraina, il conflitto israelo-palestinese e le recenti operazioni israelo-statunitensi contro l'Iran avviate nel marzo 2026 evidenziano come l'uso della forza nel cyberspazio –

[18] "Diplomazia Cibernetica," Ministero degli Affari Esteri e della Cooperazione Internazionale, 2026a, https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/.
[19] Ranjit Kaur, Dejan Gabrijelčič, and Tomaž Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion* 97 (2023): 101804, https://doi.org/10.1016/j.inffus.2023.101804; *Relazione Annuale 2026 sulla Politica dell'Informazione per la Sicurezza*, Sistema di informazione per la sicurezza della Repubblica, 2026, https://www.sicurezzanazionale.gov.it/data/cms/posts/1163/attachments/4d8b721a-3c8f-456c-9bce-cbe649e7522b/download?view=true.
[20] *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign*, Anthropic, 2025, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

anche in scenari di guerra – non sia monopolio esclusivo degli Stati, ma oggetto di contesa da parte di molteplici attori.

Nel conflitto russo-ucraino, le operazioni cibernetiche sono pianificate e condotte in coordinamento con attacchi convenzionali, con l'obiettivo di generare distruzione, confusione e disgregazione nelle capacità avversarie. Tra i principali vettori figurano attacchi distruttivi (*wiper* che cancellano dati o rendono i sistemi inutilizzabili), attacchi volti a interrompere servizi e infrastrutture critiche come i DDoS, operazioni di *data weaponisation*, spionaggio, *hack-and-leak* e campagne di disinformazione. Anche in questo contesto si osserva una marcata fluidità tra attori statali e non statali: operano in sinergia "eserciti cibernetici" composti da volontari, gruppi di hacktivisti, gruppi criminali ed entità affiliate agli Stati, complicando l'attribuzione degli attacchi, la definizione di responsabilità e l'implementazione di misure efficaci di protezione e deterrenza. Ad esempio, la Federazione Russa ha esperienza di lungo corso nello sfruttamento del cyberspazio e nel ricorso ad attori terzi nelle sue operazioni cibernetiche, come testimoniato dai casi emblematici degli attacchi contro l'Estonia nel 2007 e la Georgia nel 2008[21], e contro l'Ucraina stessa con l'impiego del distruttivo *malware* NotPetya nel 2017.[22] Tuttavia, nell'invasione su larga scala dell'Ucraina del febbraio 2022 la Russia ha impiegato capacità cibernetiche in misura più limitata rispetto alle aspettative della comunità internazionale, senza condurre operazioni su vasta scala in grado di incidere in modo determinante sull'andamento del conflitto. Le operazioni più rilevanti hanno riguardato attacchi DDoS condotti dal GRU[23] russo contro siti

[21] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60, https://doi.org/10.5038/1944-0472.4.2.3; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 371.

[22] Greenberg, "The Untold Story of NotPetya".

[23] "*Glavnoe Razvedyvatel'noe Upravlenie":* traducibile in italiano come "Direzione Principale dell'Intelligence Militare".

governativi, bancari e di difesa ucraini nelle settimane precedenti e immediatamente successive all'invasione del febbraio 2022.[24] L'obiettivo principale era sabotare servizi critici e diffondere disinformazione, sebbene la portata e la durata di tali attacchi siano risultate limitate rispetto all'impatto delle operazioni militari convenzionali sul campo.[25] Le attività cibernetiche hanno accompagnato le operazioni russe per tutto il corso del conflitto: nel primo semestre del 2025, il CERT-UA ha registrato un incremento dei cyberattacchi (3.018 rispetto ai 2.575 della fine del 2024) e un'evoluzione delle tattiche e tecniche impiegate, con l'emergere di nuovi gruppi e l'adozione di strumenti basati su intelligenza artificiale.[26] Tra le modalità osservate vi sono malware per il furto di dati, diffusione di file malevoli tramite archivi, esfiltrazione di credenziali dai browser e campagne di spionaggio e sabotaggio dirette a enti pubblici e infrastrutture critiche, attività simili a quelle tracciate in Europa già a partire dal 2023 (*Ivi*).

L'Ucraina ha adottato un approccio difensivo e cooperativo nel cyberspazio, mobilitando competenze interne e supporto internazionale per contrastare i cyberattacchi russi. Grandi aziende private americane, tra cui Amazon e Microsoft, hanno rafforzato le capacità difensive ucraine, sebbene alcune iniziative siano state rallentate da cambiamenti politici negli Stati Uniti. Kyiv ha inoltre promosso la creazione di una "armata informatica" composta da professionisti e volontari, impegnati in operazioni che includono falsi allarmi,

[24] Andrew E. Kramer, "Hackers Bring Down Government Sites in Ukraine," *The New York Times*, 14 gennaio, 2022, https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html.

[25] Kateryna Fendorf and Justin Miller, "Tracking Cyber Operations and Actors in the Russia-Ukraine War," Council on Foreign Relations, 2025, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[26] "New Cyber Threats: Who and How Enemy Groups Attack," State Service of Special Communications and Information Protection of Ukraine, 2025, https://cip.gov.ua/ua/news/novi-kiberzagrozi-kogo-i-yak-atakuyut-vorozhi-ugrupovannya.

infiltrazioni di telecamere di sorveglianza nelle aree occupate e profili social ingannevoli per ottenere informazioni geolocalizzate dei soldati russi.[27] Le attività ucraine nel cyberspazio mirano anche alla propaganda e al sostegno internazionale, fungendo da estensione del fronte operativo: azioni prevalentemente simboliche, ma strategicamente rilevanti, che contribuiscono a mantenere pressione sull'avversario e a supportare le operazioni convenzionali. In questo contesto l'Italia ha contribuito allo sforzo ucraino stanziando circa 1 milione di euro nell'ambito del *Tallinn Mechanism*, un'iniziativa informale e multilaterale che dal 2023 sistematizza e coordina il supporto civile all'Ucraina in materia di cybersicurezza in risposta alle conseguenze dell'aggressione russa. Di questi fondi, circa 900.000 € sono destinati al potenziamento delle infrastrutture digitali e della resilienza informatica della regione di Ternopil e 100.000 € a supporto dell'ufficio di coordinamento TMPO[28] a Kiev per rafforzare le capacità di difesa cyber dell'Ucraina a livello regionale e nazionale.[29]

Il Medio Oriente è un'ulteriore area ad altissima volatilità nella quale la dimensione militare e quella economico-energetica interagiscono con la competizione informativa. Il conflitto israelo-palestinese rappresenta un esempio significativo di guerra estesa anche al dominio cibernetico, in cui entrambi gli attori coinvolti hanno utilizzato e tutt'ora impiegano operazioni informatiche di disinformazione e influenza, nonché paralisi delle infrastrutture di comunicazione e servizi civili del nemico. Hamas, attore non statale, ha

[27] Fendorf and Miller, "Tracking Cyber Operations and Actors in the Russia-Ukraine War."

[28] Acronimo di *Tallinn Mechanism Project Office*.

[29] "Italy Contributes Nearly €1 Million to Strengthen Cybersecurity in Ternopil Region," Ministero degli Affari Esteri e della Cooperazione Internazionale, 2026b, https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2026/01/litalia-contribuisce-con-circa-1-milione-di-euro-al-rafforzamento-della-sicurezza-informatica-della-regione-di-ternopil/.

sviluppato capacità cibernetiche per perseguire i propri obiettivi riducendo rischi e costi rispetto ad attacchi tradizionali suscettibili di provocare risposte immediate. Nel corso del conflitto, l'organizzazione ha impiegato strumenti cibernetici per spionaggio, diffusione di panico e disinformazione, interruzione temporanea di servizi israeliani e propaganda digitale. Nelle prime settimane del conflitto, gli attacchi informatici contro obiettivi israeliani sono aumentati del 52%, concentrandosi soprattutto su siti governativi e di difesa. Le operazioni sono state condotte con diversi mezzi. Tra gli esempi rilevanti, il 7 ottobre 2023 si sono verificati attacchi DDoS che hanno reso temporaneamente indisponibili siti di media (es. Jerusalem Post), istituti bancari e domini amministrativi israeliani, rivendicati da hacktivisti religiosi filo-palestinesi e filo-russi collegati alla rete Killnet.[30] Hamas ha inoltre evoluto le proprie capacità di spionaggio mediante pratiche sofisticate di ingegneria sociale e applicazioni malevole, come finti software per eventi sportivi o app di incontri, utilizzati per raccogliere intelligence sul personale militare israeliano.[31] Le piattaforme digitali israeliane sono state obiettivi privilegiati di hacktivisti filo-palestinesi. Ad esempio, AnonGhost ha sfruttato vulnerabilità dell'app Red Alert per intercettare comunicazioni e inviare notifiche false, tra cui falsi messaggi sull'imminente arrivo di una bomba nucleare, e ha diffuso versioni malevole dell'app capaci di rubare contatti, messaggi, registri di chiamata e dati di telefoni e SIM. Alcune vulnerabilità sono state sfruttate anche per manipolare schermi pubblicitari, mostrando simboli politici come la bandiera palestinese.[32] Hamas ha inoltre condotto operazioni di sottrazione e diffusione di dati (hack-and-leak), come

[30] Omer Yoachimik and Jorge Pacheco, "DDoS Threat Report for 2023 Q3", Cloudflare, 26 ottobre, 2023, https://blog.cloudflare.com/ddos-threat-report-2023-q3/.
[31] Byman and McCaleb, "Understanding Hamas's and Hezbollah's Uses of Information Technology."
[32] Omer Yoachimik and Jorge Pacheco, "DDoS Threat Report for 2023 Q3".

l'attacco all'Ono Academic College, e azioni di defacement, sostituendo contenuti di siti web israeliani con messaggi di odio e propaganda.

Nonostante la frequenza e varietà delle operazioni, l'impatto complessivo delle attività cibernetiche di Hamas sembra essere stato contenuto dalla robustezza delle difese informatiche israeliane. Parallelamente, Israele ha condotto operazioni cibernetiche contro siti palestinesi, sebbene le sue attività nel cyberspazio siano state maggiormente orientate a colpire Stati ritenuti sostenitori di Hamas, come Iran e Libano. Israele ha inoltre fatto ricorso ad attori terzi per operazioni nel cyberspazio. Un esempio è il gruppo hacker Predatory Sparrow, considerato agente israeliano, autore di attacchi contro il sistema finanziario iraniano (Sepah Bank e Nobitex) con distruzione di cryptoasset per quasi 100 milioni di dollari.[33] Anche le ostilità del giugno 2025 fra Iran e Israele caratterizzate da attacchi convenzionali e missilistici sono state accompagnate da un intenso ricorso a operazioni cibernetiche e a campagne di hacktivismo coordinato volte a colpire tanto infrastrutture critiche quanto obiettivi finanziari e informativi.

Da ultimo, l'operazione *Epic Fury* condotta congiuntamente da Stati Uniti e Israele contro l'Iran a partire dalla fine del febbraio 2026 e gli attacchi successivi mostrano una simile traiettoria di integrazione sistematica delle operazioni cibernetiche agli attacchi cinetici con un uso del dominio digitale per degradare comunicazioni, sensori e capacità di comando e controllo militare iraniane, nonché per condurre azioni di influenza psicologica sulla popolazione.[34] Gli

[33] Andy Greenberg, "Israel-Tied Predatory Sparrow Hackers Are Waging Cyberwar on Iran's Financial System," *Wired*, 18 giugno 2025, https://www.wired.com/story/israels-predatory-sparrow-hackers-are-waging-cyberwar-on-irans-financial-system/.

[34] Kuhu Badgi and Lauryn Williams, "How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?" Center for Strategic and International Studies (CSIS), 3 marzo 2026, https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran.

attacchi a servizi governativi, infrastrutture militari e media ufficiali con attacchi di *defacement* sono stati affiancati da operazioni più sofisticate: un esempio è la compromissione dell'app religiosa BadeSaba, usata per diffondere messaggi anti-regime proprio nel momento dell'offensiva aerea sull'Iran creando disorientamento sia fisico che informativo (*Ivi*). Quest'ultimo ha risposto imponendo un blocco pressoché totale di internet a livello nazionale per limitare l'efficacia delle campagne di influenza occidentali e per rafforzare il controllo interno dell'informazione. Anche in questo contesto il dominio cyber si configura come un'estensione del fronte materiale del conflitto con un impatto operativo limitato e con una funzione prevalentemente destabilizzante e di supporto alle azioni cinetiche tradizionali.

Vulnerabilità sistemiche e implicazioni per l'Italia

La facilità di accesso a strumenti di attacco ha reso il cyberspazio un dominio policentrico dall'alto grado di frammentazione del monopolio sull'uso della forza legittima, in cui attori e minacce si sono moltiplicati e diversificati sfruttando vulnerabilità sistemiche e costi d'ingresso sempre più bassi. L'interdipendenza e l'integrazione tecnologica tra infrastrutture critiche e sistemi pubblici e privati amplificano il potenziale distruttivo degli attacchi, mentre la difficoltà di attribuzione e previsione delle minacce ne rende costose e complicate prevenzione e difesa. Inoltre, l'accentramento dei servizi digitali globali in pochi provider accresce il rischio sistemico, poiché la loro compromissione può generare effetti a catena. Da ultimo, l'altissimo grado di interconnessione delle reti globali rende fondamentale saper prevenire e gestire le minacce in grado di infiltrarsi verso l'esterno tramite Internet, come fu nel grave caso di NotPetya.[35] Come emerge dai casi analizzati, le operazioni cibernetiche hanno

[35] Greenberg, "The Untold Story of NotPetya".

principalmente una funzione destabilizzante, si collocano al di sotto della soglia del conflitto e sono spesso condotte da attori proxy affiliati a Stati. Nel contesto dei conflitti militari, tali operazioni non modificano in modo determinante l'andamento delle azioni sul campo, ma servono piuttosto a esercitare pressione agendo in parallelo alle operazioni convenzionali per logorare la resilienza interna dell'avversario. Le tensioni geopolitiche e i conflitti aumentano frequenza e impatto degli attacchi cibernetici, rendendo lo sviluppo di resilienza e capacità di rapido ripristino elementi strategici essenziali nelle politiche di difesa del dominio digitale.[36]

Anche l'Italia è esposta e regolarmente colpita da cyberattacchi, una situazione che riflette le tendenze globali sinora delineate di crescente sofisticazione e aggressività nel cyberspazio. Dati ufficiali dell'Agenzia per la Cybersicurezza Nazionale (ACN) evidenziano un'intensificazione significativa delle minacce: nel primo semestre del 2025 si sono registrati 1.549 eventi (+53% rispetto al 2024) e 346 incidenti a impatto confermato (+98%), un incremento superiore a quello già osservato nel 2024 (+89,1%).[37] Gli attacchi mirano sia a soggetti privati sia pubblici, interessando furto di dati e credenziali, esfiltrazione di informazioni sensibili e minacce persistenti di tipo APT attribuibili ad attori statali.[38] Evidenze ancor più recenti confermano e rafforzano ulteriormente questo quadro: la Relazione annuale del sistema di informazione per la Sicurezza della Repubblica del 2026 segnala il ruolo crescente di attori altamente sofisticati, spesso riconducibili ad attori statali, che conducono attività di tipo APT e operazioni

[36] *Global Cybersecurity Outlook 2026*, World Economic Forum, 2026, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
[37] *Relazione annuale 2024*, Agenzia per la Cybersicurezza Nazionale (ACN), 2025, https://www.acn.gov.it/portale/relazione-annuale/2024.
[38] *Relazione Annuale 2025 sulla Politica dell'Informazione per la Sicurezza*, Sistema di informazione per la sicurezza della Repubblica, 2025, https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2025.

mirate contro settori strategici nazionali come infrastrutture digitali e amministrazioni centrali dello Stato italiano[39]. Le minacce che l'Italia affronta mostrano altresì un'evoluzione sul piano tecnico e operativo: allo sfruttamento di vulnerabilità *zero-day* si affiancano tecniche più tradizionali come *phishing* e tentativi di ingegneria sociale, nonché azioni digitali ostili di matrice spionistica sofisticate e difficilmente attribuibili (*Ivi*). A ciò si aggiunge l'impatto delle tecnologie emergenti, in particolare dell'IA, che amplificano sia le capacità difensive sia offensive nel dominio cibernetico.

Sul piano della governance nazionale l'Italia ha compiuto passi significativi per rafforzare il coordinamento delle proprie politiche in ambito cyber. L'ACN continua a esercitare un ruolo strategico nella definizione e nel monitoraggio della cybersicurezza nazionale, promuovendo, tra le altre cose, il recepimento e l'implementazione della normativa europea di settore. Il Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI) ha invece istituito la Direzione Generale per le questioni cibernetiche, l'informatica e l'innovazione tecnologica con la sua riforma organizzativa in vigore dal 15 novembre 2025, rafforzando il ruolo centrale dello Stato nel presidio e nella regolamentazione del dominio digitale.[40] Il perimetro di competenze assegnato alla Direzione Generale mostra una catena di responsabilità che unifica dimensione esterna e interna: trattazione delle politiche internazionali sulla sicurezza cibernetica e impiego dei mezzi cibernetici anche con riferimento al contrasto alla disinformazione; presidio delle tematiche sull'intelligenza artificiale; sicurezza cibernetica del MAECI; gestione e sviluppo delle tecnologie informatiche; digitalizzazione e

[39] Relazione Annuale 2026 sulla Politica dell'Informazione per la Sicurezza, Sistema di informazione per la sicurezza della Repubblica.

[40] "Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica," Ministero degli Affari Esteri e della Cooperazione Internazionale, 2026, https://www.esteri.it/it/ministero/struttura/dgct/.

gestione delle infrastrutture; cifra e comunicazioni; promozione dell'innovazione tecnologica nell'amministrazione centrale e nelle sedi all'estero.

Il MAECI ha inoltre consolidato la *cyber diplomacy* come capacità istituzionale fondamentale e permanentemente integrata nelle funzioni centrali del Ministero,[41] intesa come l'uso di strumenti diplomatici tradizionali e digitali per promuovere uno spazio cibernetico libero, sicuro e rispettoso dei diritti umani nel quale vi possa essere piena applicazione del diritto internazionale. Il MAECI è impegnato nella diplomazia cibernetica su molteplici fronti: in ambito UE con l'attuazione del *Cyber Diplomacy Toolbox*, in ambito ONU partecipa ai negoziati sullo sviluppo di norme di comportamento responsabile degli Stati e sull'applicabilità del diritto internazionale al cyberspazio, anche nel quadro del nuovo Meccanismo Globale attivo dal 2026; in ambito NATO contribuisce all'attuazione del *Cyber Defence Pledge* e alla definizione di guide e procedure per la risposta ad attacchi cyber; in ambito OSCE promuove le misure di costruzione della fiducia; e infine in ambito G7 sostiene la cooperazione internazionale per un ambiente informatico aperto, sicuro e stabile.[42]

Parallelamente a queste iniziative l'Italia sta evolvendo la propria postura strategica passando nella gestione delle minacce cyber da un approccio reattivo a uno più proattivo e preventivo. La strategia nazionale mira a identificare e mitigare vulnerabilità sistemiche in sistemi e infrastrutture critiche, garantendo la resilienza nazionale attraverso capacità di rilevamento precoce, risposta e ripristino rapido, elementi considerati altrettanto cruciali quanto la prevenzione stessa. L'obiettivo non è l'eliminazione totale del rischio, bensì la riduzione

[41] MAECI, "Diplomazia Cibernetica"
[42] *Ibid*

dell'impatto sistemico e dei tempi di recupero, preservando la continuità dei servizi essenziali e l'integrità complessiva del sistema nazionale.

Riferimenti bibliografici

Ablon, L., e Bogart, A. (2017). *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. RAND.

Agenzia per la cybersicurezza nazionale. (2025). *Relazione annuale 2024*. ACN. https://www.acn.gov.it/portale/relazione-annuale/2024

Ahmad, A., Webb, J., Desouza, K. C., e Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Anthropic (2025). *Disrupting the first reported AI-orchestrated cyber espionage campaign*. https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf

Badgi, K., e Williams, L. (2026). *How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?* https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran

Byman, D., e McCaleb, E. (2023). *Understanding Hamas's and Hezbollah's Uses of Information Technology*. https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology

European Union Agency for Cybersecurity. (2025). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

Fendorf, K., e Miller, J. (2025). *Tracking Cyber Operations and Actors in the Russia-Ukraine War*. Council on Foreign Relations. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Harknett, R. J., e Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies Arlington, VA. https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Kaur, R., Gabrijelčič, D., e Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. Penguin Publishing Group.

Kramer, A. E. (2022). Hackers Bring Down Government Sites in Ukraine. *The New York Times*. https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. https://www.rand.org/pubs/monographs/MG877.html

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Ministero degli Affari Esteri e della Cooperazione Internazionale. (2026). *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/

Ministero degli Affari Esteri e della Cooperazione Internazionale. (2026a). *Diplomazia Cibernetica – Ministero degli Affari Esteri e della Cooperazione Internazionale*. https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/

Ministero degli Affari Esteri e della Cooperazione Internazionale. (2026b). *Italy Contributes Nearly €1 Million to Strengthen Cybersecurity in Ternopil Region – Ministero degli Affari Esteri e della Cooperazione Internazionale*. https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2026/01/litalia-contribuisce-con-circa-1-milione-di-euro-al-rafforzamento-della-sicurezza-informatica-della-regione-di-ternopil/

Morris, L. J., Mazarr, M. J., Hornung, J., Pézard, S., Binnendijk, A., e Kepe, M. (2019). *Gaining competitive advantage in the gray zone: Response options for coercive aggression below the threshold of major war*. RAND Corporation.

North Atlantic Treaty Organization (NATO). (2016). Warsaw Summit Communiqué. July 9, 2016. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique.

Sistema di informazione per la Sicurezza della Repubblica. (2025). *Relazione Annuale 2025 sulla Politica dell'Informazione per la Sicurezza*. https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2025

Sistema di informazione per la Sicurezza della Repubblica. (2026). *Relazione Annuale 2026 sulla Politica dell'Informazione per la Sicurezza*. https://www.sicurezzanazionale.gov.it/data/cms/posts/1163/attachments/4d8b721a-3c8f-456c-9bce-cbe649e7522b/download?view=true

State Service of Special Communications and Information Protection of Ukraine. (2025). *New cyber threats: Who and how enemy groups attack*. State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/novi-kiberzagrozi-kogo-i-yak-atakuyut-vorozhi-ugrupovannya

Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*, *40*(3), 368–381. https://doi.org/10.1080/13523260.2019.1581458

Theohary, C. A. (2024). *Defense Primer: Cyberspace Operations*. https://www.congress.gov/crs-product/IF10537

World Economic Forum. (2026). *World Economic Forum Global Cybersecurity Outlook 2026*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Cyberspazio e IA come nuovi pilastri della sicurezza euro-atlantica: approccio NATO e UE a confronto

Pierluigi Paganini

Executive Summary

NATO e Unione Europea (UE) hanno progressivamente integrato il cyberspazio e l'intelligenza artificiale (IA) come pilastri strutturali delle rispettive strategie di sicurezza, riconoscendone il ruolo decisivo negli equilibri di potere contemporanei, nei meccanismi di deterrenza e nella resilienza degli Stati. Pur condividendo obiettivi strategici, i due attori adottano approcci distinti ma complementari: la NATO privilegia l'impiego cyber e dell'IA come moltiplicatori di capacità militari e strumenti di deterrenza operativa nei conflitti multidominio; l'Unione Europea, invece, li inquadra anche come ambiti di sovranità, regolazione e tutela, ponendo l'accento sulla protezione dell'economia digitale, delle infrastrutture critiche e dei diritti fondamentali.

Nell'approccio della NATO, cyberspazio e IA operano su tre livelli strettamente interconnessi: tattico-operativo, come supporto diretto alle operazioni militari; operativo-strategico, in quanto abilitatori di processi decisionali accelerati e di superiorità informativa; e politico-strategico, attraverso cui contribuiscono alla deterrenza, alla segnalazione e alla credibilità dell'Articolo 5. In questo quadro, l'Alleanza ha progressivamente "operazionalizzato" il cyberspazio come dominio militare, sviluppando meccanismi di difesa collettiva, capacità cyber sovrane volontarie (Sovereign Cyber Effects Provided Voluntary by Allies - SCEPVA) e una strategia sull'IA fondata su principi di uso responsabile, controllo umano significativo e rispetto del diritto internazionale.

L'UE adotta invece una visione olistica e regolatoria, imperniata su un solido quadro normativo – tra cui NIS2, DORA, AI Act, Digital Services Act, Digital

Markets Act – volto a rafforzare la resilienza, la sicurezza del mercato unico e l'autonomia strategica europea. Tale approccio mira a bilanciare innovazione tecnologica, esigenze di sicurezza e tutela dei diritti fondamentali, generando convergenze di principio con la NATO ma anche potenziali frizioni, in particolare sui tempi dell'azione regolatoria, sulla sovranità tecnologica e sull'ambito di applicazione delle regole in materia di intelligenza artificiale.

Per l'Italia, membro di entrambe le organizzazioni, la principale sfida – ma anche l'opportunità strategica – consiste nell'integrare queste due visioni in una strategia nazionale coerente e credibile. Ciò implica un duplice sforzo di allineamento alle politiche e ai quadri regolatori dell'UE da un lato, e agli standard operativi e dottrinali della NATO, dall'altro. In parallelo, risulta essenziale rafforzare le capacità industriali, tecnologiche e operative nei domini cyber e dell'IA, accompagnando tali investimenti con un'attenzione sistemica alla resilienza delle infrastrutture critiche. La capacità dell'Italia di posizionarsi come attore proattivo nella cooperazione multilaterale e di contribuire a definire un equilibrio sostenibile tra innovazione tecnologica, sicurezza e tutela dei valori democratici sarà determinante per consolidarne il peso politico e la credibilità nel contesto euro-atlantico.

Cyberspazio e intelligenza artificiale nel quadro del conflitto contemporaneo

Il conflitto armato nel XXI secolo è sempre meno confinato al campo di battaglia tradizionale e si configura sempre più come conflitto multidominio, in cui terra, mare, aria, spazio e cyberspazio risultano profondamente interconnessi[1][2]. In questo contesto, un attacco informatico può precedere, accompagnare o, in

[1] M. C. Libicki, *Cyberspace in Peace and War* (Annapolis: Naval Institute Press, 2021)

[2] G. Giannopoulos et al., *The landscape of hybrid threats: A conceptual model*. European Commission, Joint Research Centre (2021)

alcuni casi, sostituire un'azione militare convenzionale, incidendo direttamente sulla condotta e sugli esiti delle operazioni[3].

NATO e UE considerano il cyberspazio non solo come un nuovo teatro operativo, ma come una dimensione abilitante di tutti gli altri domini[4][5]. All'interno di questo quadro, l'intelligenza artificiale agisce come un amplificatore: consente l'analisi di grandi quantità di dati (sensori, comunicazioni, social media), l'individuazione di pattern di attacco latenti, la previsione dei comportamenti avversari e il supporto a processi decisionali più rapidi e informati[6]. In altri termini, trasforma il dato grezzo in vantaggio operativo e strategico.

Nel pensiero strategico della NATO, cyber e IA assumono pertanto rilevanza su tre livelli distinti ma strettamente interconnessi:

1. Livello tattico operativo: si tratta del livello più vicino al campo di battaglia e riguarda l'impiego diretto di capacità cyber e intelligenza artificiale a supporto delle operazioni militari.

In termini concreti, ciò si traduce nell'impiego di:

- sistemi autonomi o semi-autonomi, quali droni terrestri, navali o aerei che sfruttano l'IA per la navigazione, l'identificazione degli obiettivi e l'elusione delle minacce;

[3] J. Healey, *Cyber Effects in Warfare: Categorizing the Where, What, and Why*. Texas National Security Review (2024), https://tnsr.org/wp-content/uploads/2024/08/TNSR-Journal-Vol-7-Issue-4-HEALY.pdf

[4] NATO, *NATO 2022 Strategic Concept*. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

[5] European Commission, The EU's Cybersecurity Strategy for the Digital Decade (2020). https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[6] J. Smith, G. Allen, *Artificial intelligence and the future of warfare*. International Security, 46(3), 7–45 (2022)

- capacità avanzate di difesa cibernetica, basate su algoritmi di intelligenza artificiale in grado di rilevare intrusioni nei sistemi militari in tempo reale e rispondere automaticamente;
- operazioni di cyber deception, che prevedono la creazione di reti, segnali o dati falsi per ingannare l'avversario, ad esempio simulando concentrazioni di forze inesistenti. In sintesi, a questo livello cyber e IA fungono da moltiplicatori di forza, consentendo alle unità sul terreno di operare in modo più rapido, preciso e resiliente in contesti operativi ad alta complessità[7].

2. Livello operativo strategico: a questo livello riguarda il coordinamento delle operazioni su vasta scala e su archi temporali estesi. In tale ambito assumono un ruolo centrale le capacità C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), sempre più abilitate e potenziate dall'IA[8]. L'obiettivo è quello di ottenere una fused situational awareness, ossia un processo di integrazione e analisi di dati provenienti da fonti eterogenee (sensori, intelligence, sistemi) attraverso l'impiego di tecnologie digitali e algoritmi di IA, al fine di generare una comprensione unificata, completa e in tempo reale dello scenario operativo. Tale capacità è funzionale a decisioni più rapide e a risposte proattive in ambienti caratterizzati da elevata complessità e incertezza.

In termini operativi, ciò si traduce, ad esempio in:

[7] Skingsley, J., Offensive Cyber Operation: States' Perceptions of Their Utility and Risks. Chatham House (2023). https://www.chathamhouse.org/sites/default/files/2023-09/230919-offensive-cyber-operations-skingsley.pdf

[8] NATO, Summary of NATO's revised Artificial Intelligence (AI) Strategy (2024). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

- integrazione, tramite IA, di dati provenienti da satelliti, radar, droni e intelligence umana per fornire ai livelli di comando un quadro operativo e coerente e continuamente aggiornato;
- impiego di sistemi di decision support in grado di suggerire opzioni operative, valutando, valutando rischi, tempi di esecuzione e possibili reazioni dell'avversario.

3. Livello politico-strategico: al livello più alto, cyberspazio e intelligenza artificiale assumono una funzione eminentemente politico-strategica, diventando strumenti attraverso i quali Stati e alleanze comunicano forza, limiti e intenzioni agli avversari. In questo ambito, cyber e IA sono centrali nei meccanismi di deterrenza e di segnalazione strategica, contribuendo a definire quali comportamenti siano considerati accettabili e quali, invece, possano innescare una risposta, anche al di sotto della soglia dell'uso della forza militare convenzionale. La NATO utilizza questi domini per:

- dissuadere potenziali avversari, comunicando che un attacco cyber grave potrebbe attivare una risposta collettiva;
- rafforzare la credibilità dell'Articolo 5, adattandolo anche a minacce ibride e cyber;
- inviare segnali strategici, ad esempio dichiarando posture di difesa cibernetica o capacità di risposta coordinata[9].

Un esempio concreto è il messaggio secondo cui un cyber attacco con effetti paragonabili a quelli di un attacco armato potrebbe essere considerato tale ai fini

[9] M. Taddeo, The limits of deterrence in cyberspace. Philosophy & Technology, 30(3), 339–355 (2017).

della difesa collettiva. Anche senza rivelare dettagli operativi, questo tipo di dichiarazioni ha un forte valore politico.

L'approccio dell'Unione Europea

Nell'UE l'intelligenza artificiale è considerata una tecnologia trasversale il cui impatto su sicurezza, competitività e resilienza dipende direttamente dalla qualità della regolamentazione[10][11]. Il cyberspazio, invece, è ormai riconosciuto come un dominio strategico: il fondamento dell'economia digitale, della tutela dei processi democratici e dell'erogazione dei servizi pubblici essenziali[12] .

Questa visione "olistica" si sviluppa secondo quattro assi strategici principali, sostenuti da un robusto quadro normativo e da strumenti di finanziamento europeo:

- Protezione del mercato unico digitale: attraverso il Digital Services Act (DSA)[13] e il Digital Markets Act (DMA)[14], l'UE rafforza il quadro di responsabilità e trasparenza delle piattaforme digitali, introducendo obblighi stringenti in materia di trasparenza, moderazione dei contenuti e responsabilità alle piattaforme digitali, riducendo vulnerabilità a disinformazione, interferenze straniere e attacchi ibridi[15]. Questi regolamenti, entrati in vigore nel 2024, mirano a ridurre l'uso delle

[10] European Commission, European approach to artificial intelligence (2025). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[11] European Parliament, Defence and artificial intelligence (2025). https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
[12] Council of the European Union. A Strategic Compass for Security and Defence (2022). https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
[13] https://digital-strategy.ec.europa.eu/it/policies/digital-services-act
[14] https://digital-markets-act.ec.europa.eu/about-dma_en
[15] S. Bradshaw, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, (2019). https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf

piattaforme digitali come strumenti di manipolazione dei processi democratici. Il nuovo sistema di supervisione, coordinato a livello UE, segna un passaggo da un approccio frammentato a una governance europea integrata dello spazio digitale.

- Sviluppo di una base industriale e tecnologica europea autonoma: i concetti di "digital sovereignty" e "open strategic autonomy" orientano la strategia dell'UE volta a ridurre le dipendenze da fornitori extra-UE in ambiti chiave come cloud, semiconduttori e IA[16]. Programmi come il Digital Europe Programme e l'European Defence Fund (EDF) canalizzano risorse significative verso attività di ricerca e sviluppo (R&S) di soluzioni europee in ambito secure cloud, edge computing e cybersecurity. In questo quadro, un ruolo centrale è attribuito ai meccanismi di certificazione e qualificazione promossi a livello europeo – attraverso l'ENISA per esempio – per garantire l'impiego di tecnologie affidabili in contesti sensibili. La Dichiarazione di Berlino sulla sovranità digitale (2025) rafforza questa impostazione, sottolineando la necessità di scalare infrastrutture comuni come Software Heritage per la tutela del "software commons" europeo[17].
- Rafforzamento della resilienza delle infrastrutture critiche: la Direttiva NIS2 (2022/2555)[18], segna un salto di qualità rispetto alla precedente NIS, ampliando in modo significativo il perimetro settoriale delle infrastrutture considerata critiche a livello europeo. La direttiva estende infatti gli

[16] P. Hentzen, *Cybersecurity & digital sovereignty: What about Europe?* In Stormshield (2025) https://www.stormshield.com/news/cybersecurity-and-digital-sovereignty-can-europe-regain-control/

[17] European Commission, *European approach to artificial intelligence* (2025). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

obblighi di sicurezza a un numero molto più ampio di settori critici – complessivamente 18 – e introduce requisiti più stringenti in materia di gestione del rischio, notifica tempestiva degli incidenti significativi e adozione di misure di protezione attiva. Il recepimento da parte degli Stati membri, previsto entro il 17 ottobre 2024, mira a garantire un approccio più integrato alla cybersecurity, capace di includere sia ambienti IT sia OT (Operational Technology). Questo aspetto è particolarmente rilevante per settori come energia e trasporti, nei quali l'intelligenza artificiale può abilitare meccanismi avanzati di anomaly detection predittiva e di risposta automatizzata agli incidenti[19].

- Definizione di regole che bilancino innovazione, sicurezza e diritti fondamentali: L'AI Act (Regolamento 2024/1689)[20] introduce un approccio risk-based per sistemi IA, con obblighi di accuracy, robustness e cybersecurity per applicazioni ad alto rischio, escludendo però esplicitamente usi "puramente militari". Parallelamente, lo Strategic Compass[21] e il Cyber Diplomacy Toolbox[22] rafforzano la capacità di risposta a minacce ibride, con sanzioni mirate contro attori statali e non statali responsabili di attacchi significativi, e un Foreign Information Manipulation and Interference (FIMI) Toolbox per contrastare disinformazione e propaganda[23]. In questo quadro si inserisce il rafforzamento della dimensione diplomatica del cyberspazio, che vede gli Stati membri, tra cui l'Italia, impegnati nella definizione di norme

[19] M. Magnini, *Cybersecurity and resilience: How IT, OT and AI are changing the game* in Aidia (2025). https://aidia.it/en/news/cybersecurity-resilienza-it-ot-ai-nis2-italia/

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

[21] https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[22] https://www.cyber-diplomacy-toolbox.com

[23] S. Biscop, *The Strategic Compass: Entering the fray?* In Egmont Institute (2021). https://egmontinstitute.be/app/uploads/2021/09/spb-149-Sven.pdf?type=pdf

internazionali, confidence-building measures e meccanismi di risposta condivisi.

La NATO dunque interpreta cyberspazio e IA prevalentemente come strumenti militari, operativi e di deterrenza, mentre l'UE li considera pilastri di sicurezza, di sovranità economica e di potere normativo. Per l'Italia, la sfida consiste nell'integrare queste due dimensioni in una strategia nazionale coerente, allineando settore pubblico e privato al quadro regolatorio europeo, sviluppando capacità operative e industriali compatibili con le esigenze NATO/EDF, valorizzando al contempo eccellenze nazionali e promuovendo partenariati pubblico-privati, nonché iniziative di cyber-diplomazia per mantenere un ruolo rilevante nei processi decisionali multilaterali[24]

In particolare, la recente riforma del Ministero degli Affari Esteri e della Cooperazione Internazionale, che ha visto tra le altre cose l'istituzione della Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica, rappresenta un passaggio chiave nel rafforzamento del ruolo della Farnesina nella cyber diplomacy. Tale evoluzione consente all'Italia di integrare in modo più strutturato politica estera, sicurezza e innovazione tecnologica, potenziando la propria capacità di incidere nei processi multilaterali e nella governance globale del cyberspazio[25].

L'evoluzione dell'approccio della NATO

L'evoluzione dell'approccio NATO al cyberspazio rappresenta molto più che un aggiornamento tecnico delle capacità di difesa digitale: essa ha progressivamente ridefinito il concetto stesso di "difesa collettiva" in un contesto

[24] Agenzia per la Cybersicurezza Nazionale, Strategia Nazionale di Cybersicurezza 2022-2026.

[25] "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/.

in cui attori statali e non statali possono infliggere produrre effetti strategici senza oltrepassare fisicamente i confini dell'Alleanza[26].

A partire dai primi anni 2010, la NATO ha superato una concezione del dominio cyber limitata principalmente alla protezione delle reti e alla gestione tecnica degli incidenti, riconoscendo il cyberspazio come dominio operativo politico-strategico a pieno titolo alla stregue di terra, mare, aria e spazio. I Summit del Galles (2014) e di Varsavia (2016) hanno segnato questo passaggio, culminando nel riconoscimento che un attacco informatico particolarmente grave possa integrare i presupposti per l'attivazione dell'Articolo 5 del Trattato di Washington, riconoscendo di fatto che un'operazione cyber potrebbe avere effetti paragonabili a un attacco militare tradizionale[27]. A ragione di ciò, le operazioni cyber offensive sono state spostate dal piano degli "incidenti di sicurezza" a quello dei potenziali atti di guerra, con implicazioni dirette in termini di deterrenza, risposta graduata ed escalation management

Su questa base, la NATO ha rafforzato la propria architettura di cyber defence lungo tre direttrici principali.

In primo luogo, sul piano politico-strategico, la Comprehensive Cyber Defence Policy (aggiornata nel 2021)[28] definisce i principi cardine dell'approccio NATO: protezione delle reti e dei sistemi dell'Alleanza, assistenza coordinata agli Alleati colpiti da attacchi significativi, integrazione del cyber nei processi di pianificazione operativa, di deterrenza e di difesa. Pur riaffermando che la responsabilità primaria della difesa cibernetica sia nazionale, la policy chiarisce

[26] M. N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (Cambridge: Cambridge University Press, 2017)

[27] NATO. (2016). Warsaw Summit Communiqué. Brussels. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

[28] L. Damiano e E. Scatto, Nato, la nuova "Cyber Defence Policy": ecco le priorità dell'Alleanza nella difesa dello spazio cibernetico in Agenda Digitale (2021). https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-dellalleanza-nella-difesa-dello-spazio-cibernetico/

che la sicurezza collettiva dipende dalla capacità dell'Alleanza di coordinare posture nazionali, mutual assistance e decisione politica.

In secondo luogo, sul piano dottrinale e formativo, il NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Tallinn si è affermato come vero e proprio "laboratorio" per la sperimentazione concettuale, l'addestramento e l'elaborazione normativa. Attraverso esercitazioni complesse come "Locked Shields" e "Crossed Swords", wargame tecnico-legali e programmi di formazione e ricerca avanzata, il CCDCOE contribuisce a sviluppare una comprensione operativa del conflitto nel cyberspazio e a testare sul campo procedure di incident response multinazionali. In questo contesto, il Tallinn Manual rappresenta il riferimento più influente sull'applicabilità del diritto internazionale – compreso quello dei conflitti armati – alle operazioni cyber oggi in fase di revisione alla luce delle pratiche statali più recenti e delle nuove questioni emerse nella guerra tra Russia e Ucraina[29].

Infine, sul piano operativo, la NATO ha avviato una concreta "operazionalizzazione" del dominio cyber, incoraggiando gli Alleati a mettere a disposizione, su base volontaria e reversibile (SCEPVA) ovvero capacità specifiche come attacchi difensivi. disruption di infrastrutture avversarie, raccolta intelligence o defensive cyber operations, per essere integrate nei piani operativi NATO. Questo approccio, consolidato dai Summit di Bruxelles (2021) e Vilnius (2023), e che rappresenta il passaggio concreto e definitivo del riconoscimento del cyberspazio come dominio operativo e integrato, consente di integrare capacità cyber nazionali nei piani operativi NATO senza creare una

[29] CCDCOE. The Tallinn Manual. (2018). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/research/tallinn-manual/ccdcoe

forza cyber centralizzata, preservando la sovranità nazionale ma aumentando l'efficacia collettiva.

Al Vertice di Vilnius, gli Alleati hanno rafforzato il ruolo della cyber defence nella postura complessiva di deterrenza e difesa dell'Alleanza, approvando un nuovo quadro concettuale volto a integrare più strettamente le dimensioni politica, militare e tecnica. Contestualmente, è stato rilanciato il Cyber Defence Pledge, con obiettivi nazionali più ambiziosi in materia di protezione delle infrastrutture critiche. In questo contesto, la NATO ha inoltre avviato la Virtual Cyber Incident Support Capability (VCISC), una capacità virtuale di supporto rapido progettata per assistere gli Stati membri nella gestione e nella mitigazione di attività cyber malevole significative, attraverso la fornitura di expertise specialistica, coordinamento e, ove necessario, supporto operativo.

Parallelamente, l'Alleanza ha intensificato le esercitazioni congiunte dedicate alla protezione delle infrastrutture critiche civili e militari, come dimostrano le recenti iniziative nel Baltico, e ha avviato lo sviluppo del NATO Integrated Cyber Defence Centre (NICC) con l'obiettivo di rafforzare la protezione delle reti NATO e alleate e di migliorare l'impiego del cyberspazio come dominio operativo a supporto dei comandi militari.

Questa architettura, pur mantenendo una struttura decisionale intergovernativa, consolida un paradigma di cyber deterrence fondato su una combinazione di deterrence "by denial" e "cost imposition":

- "by denial" perché mira a ridurre l'efficacia degli attacchi attraverso resilienza, ridondanza, capacità avanzate di rilevamento e risposta coordinata;
- "by cost imposition" perché segnala la possibilità di una risposta collettiva – non necessariamente simmetrica né limitata al dominio cibernetico – ad

attacchi gravi contro infrastrutture alleate, aumentando il rischio percepito da potenziali avversari.

In questo modo, la NATO adatta il concetto di deterrenza alle specificità del cyberspazio combinando difesa robusta e capacità di risposta congiunta, nel rispetto del diritto internazionale e con l'obiettivo di garantire interoperabilità e flessibilità nella gestione dei conflitti ibridi[30][31].

Le recenti crisi internazionali hanno evidenziato come attori statali e gruppi proxy sfruttino le proprie capacità cyber per condurre operazioni sotto soglia, rafforzando la rilevanza della capacità della NATO di integrare rapidamente strumenti cyber nelle proprie posture di deterrenza e difesa. Questo contesto ha accelerato lo sviluppo di capacità di risposta coordinata e il rafforzamento della resilienza delle infrastrutture critiche, anche alla luce delle minacce emergenti provenienti da scenari quali il Medio Oriente e l'Europa orientale.

Per quanto riguarda l'intelligenza artificiale, l'adozione della prima strategia NATO in merito nel 2021, seguita dalla revisione del 2024, segna un passaggio significativo nel modo in cui l'Alleanza Atlantica interpreta il rapporto tra innovazione tecnologica, sicurezza e valori condivisi. Per la prima volta, l'IA viene affrontata non solo come un insieme di strumenti capaci di aumentare l'efficacia militare, ma come una tecnologia dirompente che richiede una cornice politica, etica e normativa chiara. La strategia, infatti, non si limita a individuare potenziali applicazioni operative, ma definisce le condizioni entro cui tali applicazioni devono essere sviluppate e impiegate, in coerenza con il diritto internazionale e con i principi fondanti dell'Alleanza.

[30] M. Taddeo, The limits of deterrence in cyberspace. Philosophy & Technology, 30(3), 339–355 (2017).

[31] V. Psychogiou. Cyberspace: Is NATO doing enough? in Finabel (2023). https://finabel.org/wp-content/uploads/2023/01/Cyberspace_Is-NATO-doing-enough-_-Vasiliki-Psychogiou_DAN.pdf

Al centro dell'approccio NATO vi sono i Principles of Responsible Use (PRU), che rappresentano il perno concettuale dell'intera strategia. I principi di legalità, responsabilità e accountability, spiegabilità e tracciabilità, affidabilità, governabilità e mitigazione dei bias non costituiscono un mero esercizio dichiarativo, ma mirano a orientare concretamente lo sviluppo, l'adozione e l'uso dei sistemi di IA in ambito militare. Essi operano su piani differenti ma strettamente interconnessi[32]

Sul piano giuridico-normativo, la NATO riafferma il primato del diritto internazionale umanitario, del diritto dei conflitti armati. L'Alleanza riconosce esplicitamente che l'opacità decisionale dei sistemi algoritmici può entrare in tensione con i principi di distinzione, proporzionalità e attribuzione della responsabilità individuale, impegnandosi a evitare l'adozione di sistemi che rendano impossibile garantire tali presupposti.

Sul piano tecnico-organizzativo, i PRU si traducono in requisiti operativi concreti, quali auditabilità dei sistemi, possibilità di verifiche indipendenti, robustezza rispetto ad attacchi avversariali e manipolazioni dei dati, nonché l'adozione di meccanismi di sicurezza come fail safe e kill switch. Questi requisiti assumono particolare rilevanza per i sistemi in grado di produrre effetti letali o strategici, nei quali errori o comportamenti imprevisti dell'IA potrebbero avere conseguenze gravi e irreversibili.

Infine, sul piano politico-strategico, la strategia NATO trasmette un messaggio chiaro tanto agli alleati quanto ai potenziali avversari: la competizione nell'IA militare non deve trasformarsi in una corsa priva di regole. L'obiettivo è ridurre il rischio di escalation incontrollata, prevenire incidenti e favorire un minimo di prevedibilità strategica in un contesto internazionale sempre più instabile.

[32] J. Smith, G. Allen, Artificial intelligence and the future of warfare. International Security, 46(3), 7–45 (2022)

In termini di impiego operativo, la NATO considera l'IA un moltiplicatore di capacità, utile per il supporto decisionale (C4ISR), la difesa cyber avanzata, i sistemi autonomi, la robotica, e per la dimensione cognitiva e informativa del conflitto. Pur ampliando i margini di autonomia tecnologica, l'Alleanza ribadisce il principio del "meaningful human control", riconoscendo che la sfida centrale consiste nel bilanciare innovazione tecnologica, efficacia militare e coesione politica tra Stati membri.

Convergenze, frizioni e spazi di sinergia NATO-UE

Sul piano dei principi, le convergenze tra NATO e UE sono significative. Entrambe riconoscono l'IA come una "general purpose technology" di rilevanza strategica il cyberspazio come un dominio essenziale per la sicurezza collettiva e la necessità di integrare considerazioni etiche nell'impiego militare dell'IA[33]. NATO e UE condividono inoltre l'enfasi sulla cooperazione con industria e mondo della ricerca e sull'importanza di sviluppare standard comuni in materia di sicurezza, governance dei dati, robustezza dei sistemi e tutela della privacy.

Un'analisi più attenta mette tuttavia in luce alcune aree di frizione strutturale:

1. Tempi e cultura regolatoria: l'UE privilegia un approccio ex ante, fondato su regole dettagliate e vincolanti, mentre la NATO tende ad adottare principi operativi più flessibili e adattivi. Questa divergenza può generare tensioni quando l'implementazione di soluzioni algoritmiche a fini difensivi deve soddisfare simultaneamente requisiti NATO di interoperabilità e vincoli UE in materia di dati, sicurezza e responsabilità[34].

[33] S. Biscop, The Strategic Compass: Entering the fray? In Egmont Institute (2021). https://egmontinstitute.be/app/uploads/2021/09/spb-149-Sven.pdf?type=pdf
[34] Vallor, S. Blind spots in AI governance: Military AI and the EU's regulatory oversight gap in European Security Think Tank (2025) https://esthinktank.com/2025/10/03/blind-spots-in-ai-governance-military-ai-and-the-eus-regulatory-oversight-gap/

2. Sovranità tecnologica e dipendenze: l'UE promuove l'open strategic autonomy e la riduzione delle dipendenze da fornitori extra-UE, mentre la NATO opera all'interno di un mercato transatlantico fortemente integrato, nel quale la tecnologia statunitense mantiene un ruolo dominante. Questa asimmetria richiede compromessi pratici per garantire interoperabilità operativa senza compromettere le ambizioni europee di autonomia tecnologica[35].
3. Ambito di applicazione della governance dell'IA: i Principles of Responsible Use (PRUs) della NATO e il quadro normativo europeo sull'intelligenza artificiale non coincidono pienamente. È possibile, ad esempio, che un sistema di sorveglianza basato su IA risulti conforme ai PRUs in un'operazione NATO, ma entri in conflitto con le norme UE sulla protezione dei dati o sulla trasparenza algoritmica[36]. Questa discrepanza può tradursi in incertezze giuridiche o blocchi operativi, rendendo necessaria un'armonizzazione dei criteri di valutazione e delle procedure di conformità.

Nonostante tali frizioni, gli spazi di sinergia restano ampi. L'Unione Europea può fornire alla NATO un patrimonio di standard civili avanzati in materia di sicurezza, privacy e data governance, mentre la NATO offre un contesto operativo unico per testare, validare e comprendere i limiti e i rischi delle tecnologie cyber e di IA in scenari ad alta intensità. La complementarità tra capacità normative europee e sperimentazione operativa atlantica rappresenta

[35] P. Hentzen, Cybersecurity & digital sovereignty: What about Europe? In Stormshield (2025) https://www.stormshield.com/news/cybersecurity-and-digital-sovereignty-can-europe-regain-control/

[36] Vallor, S. Blind spots in AI governance: Military AI and the EU's regulatory oversight gap in European Security Think Tank (2025) https://esthinktank.com/2025/10/03/blind-spots-in-ai-governance-military-ai-and-the-eus-regulatory-oversight-gap/

uno dei principali moltiplicatori di efficacia del rapporto NATO–UE nel dominio digitale.

Implicazioni, opportunità e criticità per l'Italia

L'Italia occupa una posizione strategica peculiare nell'architettura euro-atlantica, sia per la sua collocazione geopolitica nel Mediterraneo allargato – a ridosso di teatri di crisi in Nord Africa e Medio Oriente e come frontiera sud della NATO – sia per il suo duplice ancoraggio istituzionale a NATO e UE.

Alla luce dell'evoluzione del contesto strategico internazionale, caratterizzato dall'intensificarsi delle minacce ibride, dal protrarsi del conflitto russo-ucraino e dalle recenti dinamiche di instabilità in Medio Oriente, tale posizione assume una rilevanza ancora maggiore, rafforzando il ruolo dell'Italia quale attore chiave per la sicurezza euro-atlantica e per la gestione delle crisi nel dominio cibernetico. In questo contesto, la Direzione Generale per le Questioni Cibernetiche della Farnesina si configura come un perno per una cyber diplomacy proattiva, consentendo all'Italia di promuovere la stabilità regionale anche attraverso iniziative di capacity building nel Mediterraneo e di contribuire al contrasto delle minacce ibride connesse ai conflitti in corso[37].

Questa posizione comporta responsabilità specifiche e richiede una strategia nazionale capace di integrare coerentemente le dimensioni cyber e IA nei quadri euro-atlantici. In primo luogo, è essenziale sviluppare una dottrina nazionale su cyberspazio e IA in ambito difesa che sia pienamente compatibile con i PRU della NATO, con il diritto internazionale umanitario e con il quadro regolatorio europeo. Ciò implica una chiara definizione di ruoli e responsabilità tra forze armate, agenzie di intelligence, strutture di cybersecurity civile e autorità di

[37] A. De Pedys, Ecco com'è cambiata la nostra missione con la riforma cyber e digitale voluta dal ministro Tajani in Cybersecurity Italia (2026). https://www.cybersecitalia.it/farnesina-de-pedys-maeci-ecco-come-cambiata-la-nostra-missione-con-la-riforma-cyber-e-digitale-voluta-dal-ministro-tajani/62753/

regolazione, nonché l'adozione di criteri nazionali per garantire il "meaningful human control" sui sistemi a potenziale impiego letale e la supervisione umana sulle decisioni automatizzate critiche[38]. A questo si affianca la necessità di implementare procedure strutturate di audit, certificazione e verifica per i sistemi IA impiegati in contesti operativi ad alto rischio.

In secondo luogo, l'Italia deve sfruttare pienamente i canali di innovazione multilaterale offerti dall'ecosistema NATO e UE. Ciò include la partecipazione attiva a iniziative NATO come il Defence Innovation Accelerator for the North Atlantic (DIANA) e il NATO Innovation Fund, con progetti focalizzati su data fusion, sistemi autonomi, cyber defence predittiva e contrasto alla disinformazione, nonché un coinvolgimento strutturato nei consorzi dell'European Defence Fund (EDF) e nei progetti PESCO in ambiti quali cyber defence cooperativa, sistemi di comando e controllo resilienti, secure cloud militare e servizi spaziali abilitati da IA[39]

Parallelamente, è fondamentale costruire un sistema nazionale di resilienza digitale facendo leva sul quadro normativo e operativo dell'UE – in particolare NIS2, il Cybersecurity Act e le iniziative sullo European Cyber Shield – per rafforzare la protezione di infrastrutture critiche nei settori energetico, dei trasporti, spaziale e industriale, promuovendo una più stretta integrazione tra capacità di difesa e protezione civile[40].

[38] NATO Parliamentary Assembly . NATO and AI. (2024). https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc

[39] War College / Defence Finance Monitor. Artificial intelligence in defence: NATO and EU strategies and funding mechanisms in Defence Finance Monitor. (2025). https://defencefinancemonitor.substack.com/p/artificial-intelligence-in-defence

[40] M. Magnini, Cybersecurity and resilience: How IT, OT and AI are changing the game in Aidia (2025). https://aidia.it/en/news/cybersecurity-resilienza-it-ot-ai-nis2-italia/

Infine, la gestione delle criticità industriali e capacitive richiede un'attenzione mirata. L'ecosistema italiano della difesa e della cybersecurity è ricco di eccellenze riconosciute, ma rimane frammentato e spesso sotto-capitalizzato rispetto ai grandi player transnazionali. Per cogliere appieno le opportunità offerte dai programmi NATO e UE, l'Italia deve rafforzare le proprie filiere industriali in ambiti chiave quali IA, semiconduttori, edge computing e cybersecurity, investire in formazione e retention di talenti in data science, AI e cyber operations, e garantire alle PMI innovative un accesso effettivo ai programmi strategici, evitando il rischio di marginalizzazione.

Per l'Italia, la sfida non consiste soltanto nell'adottare gli approcci di NATO e Unione Europea al cyberspazio e all'intelligenza artificiale, ma nel contribuire attivamente a plasmarli, valorizzando la propria tradizione giuridica, l'esperienza maturata nella gestione delle crisi ibride nel Mediterraneo e le competenze industriali e accademiche nazionali. In questa prospettiva, il Paese può evolvere da policy taker a policy shaper, rafforzando il proprio ruolo nei processi decisionali multilaterali anche attraverso un utilizzo più strutturato degli strumenti di diplomazia tecnologica e una presenza qualificata nei principali fori internazionali. In un contesto in cui le alleanze multilaterali saranno sempre più valutate per la loro capacità di integrare tecnologia, valori e coesione politica, la qualità della strategia italiana in ambito cyber e IA rappresenterà un indicatore chiave di credibilità e di peso sia nella NATO sia nell'Unione Europea.

Conclusioni

Il cyberspazio e l'intelligenza artificiale stanno ridefinendo in profondità la natura della sicurezza internazionale e dei conflitti armati. In risposta, NATO e Unione Europea hanno sviluppato approcci distinti ma complementari, fondati

sull'integrazione di deterrenza, resilienza e regolazione. Negli ultimi anni, il rapido deterioramento del contesto geopolitico – segnato dal conflitto russo-ucraino, dall'intensificarsi delle attività cyber da parte di attori statali e proxy e dalle recenti crisi in Medio Oriente – ha ulteriormente confermato come il dominio digitale rappresenti un'arena di competizione strategica permanente, in cui operazioni sotto soglia possono generare effetti significativi sulla stabilità internazionale.

Per l'Italia, il successo in tale contesto dipenderà dalla capacità di integrare gli indirizzi multilaterali con politiche nazionali coerenti, investimenti adeguati e una governance efficace delle tecnologie emergenti. In questa prospettiva, il rafforzamento del ruolo della Farnesina nel campo della cyber diplomacy – anche attraverso la riforma che ha visto, tra le altre cose, l'istituzione della Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica – rappresenta un passaggio chiave per assicurare un approccio realmente integrato tra politica estera, sicurezza e innovazione. In un sistema internazionale sempre più instabile, il dominio digitale e l'intelligenza artificiale si configurano come elementi centrali della sovranità e della difesa collettiva.

Più in generale, l'Italia ha l'opportunità di evolvere da semplice destinatario di indirizzi strategici a attore capace di contribuire attivamente alla definizione di regole e pratiche nel cyberspazio e nell'intelligenza artificiale, valorizzando la propria posizione geopolitica, le competenze industriali e il capitale diplomatico. Il rafforzamento del coordinamento interistituzionale, l'aggiornamento continuo delle strategie nazionali e una partecipazione più incisiva nei forum multilaterali saranno determinanti per consolidare tale ruolo in un contesto sempre più competitivo e tecnologicamente avanzato.

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale. (2022). Strategia Nazionale di Cybersicurezza 2022-2026.

Biscop, S. (2022). The Strategic Compass: Entering the fray? Egmont Institute.

Bradshaw, S., & Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. Computational Propaganda Research Project.

Breton, T. (2020). Europe: The key to our sovereignty. European Commission.

Center for AI Policy. (2024, July 15). NATO updates AI strategy and includes emphasis on AI safety. https://www.centeraipolicy.org/work/nato-updates-ai-strategy-and-includes-emphasis-on-ai-safety

CCDCOE. (2018). The Tallinn Manual. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/research/tallinn-manual/ccdcoe

CCDCOE. (2021, May 5). The CCDCOE invites experts to contribute to the Tallinn Manual 3.0. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/ccdcoe

CCDCOE. (2025). CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

Council of the European Union. (2022). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Damiano L., Scatto E. (2021). Nato, la nuova “Cyber Defence Policy”: ecco le priorità dell’Alleanza nella difesa dello spazio cibernetico in Agenda Digitale. https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-dellalleanza-nella-difesa-dello-spazio-cibernetico/

DataGuard. (2025, February 4). Strengthening cybersecurity through the EU's NIS2 Directive. https://www.dataguard.com/blog/strengthening-cybersecurity-through-the-eu-nis2-directive

Darktrace. (2025, December 17). Implications of NIS2 on cybersecurity and AI. https://www.darktrace.com/blog/the-implications-of-nis2-on-cyber-security-and-ai

De Pedys, A. (2026). Ecco com’è cambiata la nostra missione con la riforma cyber e digitale voluta dal ministro Tajani in Cybersecurity Italia. https://www.cybersecitalia.it/farnesina-de-pedys-maeci-ecco-come-cambiata-

la-nostra-missione-con-la-riforma-cyber-e-digitale-voluta-dal-ministro-tajani/62753/

European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade. Publications Office of the European Union. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2025, November 18). EU cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commission. (2025, November 18). European approach to artificial intelligence. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Parliament. (2025). Defence and artificial intelligence (EPRS_BRI(2025)769580). https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

European Union. (2022). A Strategic Compass for Security and Defence. European External Action Service.

Floridi, L., & Taddeo, M. (2014). The rise of the information ethics. Nature, 509(7501), 429–430.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). The landscape of hybrid threats: A conceptual model. European Commission, Joint Research Centre.

Haley, J., Cyber Effects in Warfare: Categorizing the Where, What, and Why. Texas National Security Review (2024). https://tnsr.org/wp-content/uploads/2024/08/TNSR-Journal-Vol-7-Issue-4-HEALY.pdf

Hentzen P. (2025). Cybersecurity & digital sovereignty: What about Europe? Stormshield https://www.stormshield.com/news/cybersecurity-and-digital-sovereignty-can-europe-regain-control/

Industrial Cyber. (2025, April 14). NATO allies boost cyber defense coordination, focus on improving critical infrastructure resilience. https://industrialcyber.co/critical-infrastructure/nato-allies-boost-cyber-defense-coordination-focus-on-improving-critical-infrastructure-resilience/

Libicki, M. C. (2016). Cyberspace in peace and war. Naval Institute Press.

Magnini, M. (2025, December 16). Cybersecurity and resilience: How IT, OT and AI are changing the game. Aidia. https://aidia.it/en/news/cybersecurity-resilienza-it-ot-ai-nis2-italia/

Ministry of Defence Finland. (2022, March 20). The Strategic Compass of the EU. https://defmin.fi/en/areas-of-expertise/international-defence-cooperation/eu-cooperation/the-strategic-compass-of-the-eu

Montreal AI Ethics Institute. (2025, October 13). NATO Artificial Intelligence Strategy. https://montrealethics.ai/nato-artificial-intelligence-strategy/

Missiroli, A. (2019). NATO and the EU: Cooperation in a changing security environment. NATO Review.

NATO. (2016). Warsaw Summit Communiqué. Brussels. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

NATO. (2016). Cyber Defence Pledge. North Atlantic Treaty Organization.

NATO. (2021). NATO Artificial Intelligence Strategy. Brussels.

NATO. (2022). NATO 2022 Strategic Concept. Madrid. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

NATO. (2023, July 10). Vilnius Summit Communiqué. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique

NATO. (2024, July 9). Summary of NATO's revised Artificial Intelligence (AI) strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

NATO. (2024, July 10). NATO releases revised AI strategy. https://www.nato.int/en/news-and-events/articles/news/2024/07/10/nato-releases-revised-ai-strategy

NATO Allied Command Transformation. (2023, December 11). Cyber defence. https://www.act.nato.int/activities/cyber/act.nato

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

NATO Parliamentary Assembly. (2024). NATO and AI (Report 058 STC). https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc

Psychogiou, V. (2023). Cyberspace: Is NATO doing enough? Finabel. https://finabel.org/wp-content/uploads/2023/01/Cyberspace_Is-NATO-doing-enough-_-Vasiliki-Psychogiou_DAN.pdf

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Skingsley, J. (2023). Offensive Cyber Operation: States' Perceptions of Their Utility and Risks. Chatham House. https://www.chathamhouse.org/sites/default/files/2023-09/230919-offensive-cyber-operations-skingsley.pdf

Smeets, M. (2018). The strategic promise of offensive cyber operations. Strategic Studies Quarterly, 12(3), 90–113.

Smith, J., & Allen, G. (2022). Artificial intelligence and the future of warfare. International Security, 46(3), 7–45.

Strategic Compass of the European Union. (n.d.). Pillar 2: Secure. https://www.strategic-compass-european-union.com/2_Secure_Strategic_Compass.html

Taddeo, M. (2017). The limits of deterrence in cyberspace. Philosophy & Technology, 30(3), 339–355.

Vallor, S. (2025, October 2). Blind spots in AI governance: Military AI and the EU's regulatory oversight gap. European Security Think Tank. https://esthinktank.com/2025/10/03/blind-spots-in-ai-governance-military-ai-and-the-eus-regulatory-oversight-gap/

War College / Defence Finance Monitor. (2025, July 15). Artificial intelligence in defence: NATO and EU strategies and funding mechanisms. Defence Finance Monitor. https://defencefinancemonitor.substack.com/p/artificial-intelligence-in-defence

World Congress on EU Policing. (2025, April 30). EU's approach to cyber and AI. CoESPU. https://www.coespu.org/articles/eus-approach-cyber-and-ai

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 statali e para-

[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, 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-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

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

[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 dell'IA, e se il cyberspazio costituisce il terreno permanente della competizione,

[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

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, aumenta la pressione a scegliere standard, infrastrutture e *stack* tecnologici che

[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/.

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

Sovranità digitale e proiezione internazionale: l'Italia tra cyber diplomacy e governance dell'intelligenza artificiale

Alessandro Savini

L'Italia nell'era della competizione digitale tra potenze

Gli sviluppi degli ultimi anni hanno reso evidente come l'ordine internazionale stia attraversando una fase di profonda riconfigurazione. Il ritorno della logica di potenza, la crisi del multilateralismo cooperativo e l'emergere di una pluralità di attori interessati a contestare l'ordine liberale costituito hanno restituito centralità alla competizione tra grandi potenze, articolata su più dimensioni — economica, tecnologica, militare, normativa — e su una pluralità di teatri regionali. Il *Munich Security Report* 2025 ha descritto tale dinamica come *multipolarization*, intendendo con tale termine sia lo spostamento di potere verso un numero crescente di attori in grado di influenzare le grandi questioni globali, sia l'aumento delle polarizzazioni tra Stati e all'interno di essi[132]. In tale scenario, la dimensione digitale ha cessato da tempo di costituire un mero sottoprodotto della globalizzazione economica per assumere il rango di terreno strutturante della competizione internazionale, su cui si gioca una parte significativa della redistribuzione del potere globale.

La rivalità sistemica tra Stati Uniti e Repubblica Popolare Cinese ne costituisce l'asse principale: l'escalation delle misure statunitensi di *export control* sui semiconduttori avanzati, la risposta cinese in materia di terre rare, l'affermazione di campioni industriali come DeepSeek e BYD e la corsa ai modelli di intelligenza artificiale (IA) di frontiera hanno trasformato la filiera tecnologica

[132] Tobias Bunde, Sophie Eisentraut e Leonard Schütte, a cura di, Munich Security Report 2025: Multipolarization (Monaco di Baviera: Munich Security Conference, 2025). https://securityconference.org/assets/02_Dokumente/01_Publikationen/2025/MSR_2025/Multipolarization_–_Munich_Security_Report_2025.pdf

in una infrastruttura geopolitica a tutti gli effetti[133]. Il Rapporto Draghi sul futuro della competitività europea, presentato al Parlamento Europeo nel settembre 2024, ha quantificato il divario continentale: il 70% dei modelli fondazionali di IA è stato sviluppato negli Stati Uniti dal 2017 e tre soli *hyperscaler* statunitensi controllano oltre il 65% del mercato cloud mondiale[134]. Si afferma così una dinamica che alcuni osservatori hanno descritto come *AI nationalism*: l'orientamento strategico degli Stati a innalzare l'intelligenza artificiale a infrastruttura critica di interesse nazionale da presidiare e sviluppare in modo endogeno. Ad essa si accompagna l'ingresso di nuovi protagonisti — dall'Arabia Saudita all'India agli Emirati Arabi Uniti — che mirano a inserirsi nello spazio aperto dal confronto sino-statunitense[135]. A questo quadro si sovrappongono altri fattori: l'intensificarsi delle operazioni cibernetiche *state-sponsored* e ibride, in particolare a partire dall'aggressione russa all'Ucraina; la proliferazione degli strumenti commerciali di intrusione cibernetica e dei sistemi di sorveglianza algoritmica; la fragilità delle catene globali del valore in segmenti critici; l'emergere del cyberspazio quale dominio operativo, formalmente riconosciuto come tale dalla NATO al Vertice di Varsavia del 2016[136]. L'Unione Europea, dal canto suo, ha progressivamente metabolizzato l'urgenza di una propria sovranità tecnologica, traducendola in un crescente attivismo regolativo e industriale: dall'*AI Act al Cyber Solidarity Act*, dal *Chips Act* al più recente pacchetto sulla sovranità tecnologica annunciato per il maggio 2026, che riunisce sotto un unico

[133] Center for Strategic and International Studies, A World Dividing. Winning the Economic and Tech Race. Global Forecast 2024 (Washington, DC: CSIS, 2024); Gregory C. Allen, "DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race," CSIS Report, marzo 2025. https://features.csis.org/global-forecast-economic-tech-race/

[134] Mario Draghi, The Future of European Competitiveness. Part A: A Competitiveness Strategy for Europe (Bruxelles: Commissione Europea, settembre 2024). https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[135]ISPI, Rapporto sul 2026, cit.; ISPI, "Europa e IA: il superpotere logora chi non ce l'ha," Commentary, 18 novembre 2024.

[136]NATO, "Warsaw Summit Communiqué," 9 luglio 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

ombrello strategico *Cloud and AI Development Act*, *Chips Act 2.0* e una strategia dedicata all'*open-source*[137].

Per l'Italia, la posta in gioco è duplice. Sul piano interno si tratta di tutelare la sovranità digitale, la resilienza delle infrastrutture critiche e la competitività di un tessuto produttivo a forte vocazione manifatturiera ma ancora frammentato sul versante dell'innovazione tecnologica avanzata. Sul piano esterno, l'obiettivo è consolidare un profilo diplomatico capace di concorrere alla definizione delle regole globali del cyberspazio e dell'IA, in coerenza con il quadro di valori europeo e atlantico.

La *cyber diplomacy* italiana: dall'architettura nazionale ai consessi multilaterali

L'efficacia della *cyber diplomacy* di uno Stato dipende, in prima istanza, dalla solidità della propria architettura cyber interna. L'Italia ha conosciuto in questo ambito un percorso di progressiva razionalizzazione, culminato nell'adozione del Decreto-Legge 14 giugno 2021, n. 82, convertito nella Legge n. 109/2021, che ha ridefinito l'intero impianto della cybersicurezza nazionale e istituito l'Agenzia per la Cybersicurezza Nazionale (ACN)[138]. L'architettura risultante poggia su quattro pilastri istituzionali: il Presidente del Consiglio dei Ministri, titolare dell'alta direzione e responsabile generale delle politiche di cybersicurezza; il Comitato Interministeriale per la Cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza; il Nucleo per la Cybersicurezza, deputato alla prevenzione e alla gestione delle crisi cibernetiche; l'ACN, in qualità di Autorità nazionale per la cybersicurezza, presso la quale opera lo CSIRT Italia ed è

[137] Cfr. Anu Bradford, The Brussels Effect: How the European Union Rules the World (New York: Oxford University Press, 2020).

[138] Decreto-Legge 14 giugno 2021, n. 82, "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale," Gazzetta Ufficiale n. 140 del 14 giugno 2021.

incardinato il Centro di Valutazione e Certificazione Nazionale (CVCN). L'architettura è stata ulteriormente rafforzata con il recepimento della direttiva NIS2 — attuata dal Decreto Legislativo 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024 — che ha ampliato significativamente il perimetro applicativo, coinvolgendo circa 50.000 nuovi soggetti tra entità essenziali e importanti, distribuiti su 18 settori critici e altamente critici e ha confermato l'ACN quale Autorità nazionale competente NIS e Punto di contatto unico[139]. Tale impianto, accompagnato dall'istituzionalizzazione della *European Cyber Crises Liaison Organisation Network* (EU-CyCLONe), arricchisce il bagaglio di strumenti tecnici e giuridici che l'Italia porta con sé nei consessi internazionali.

Al centro di questa architettura si colloca l'ACN, istituita nel 2021 e cresciuta in pochi anni fino ad assumere il ruolo di principale Autorità nazionale in materia di cybersicurezza. L'Agenzia svolge funzioni che spaziano dalla tutela della sicurezza nazionale nello spazio cibernetico alla protezione dei sistemi informativi delle infrastrutture critiche e degli operatori di servizi essenziali, dall'adozione di linee guida e standard tecnici alla certificazione di prodotti e servizi ICT, dalla gestione del CSIRT Italia per la risposta agli incidenti alla promozione della consapevolezza, della formazione e della ricerca nel settore[140]. A partire dall'adozione della Strategia Nazionale di Cybersicurezza 2022-2026[141] — articolata in 82 misure operative finanziate da un fondo dedicato istituito con la Legge di Bilancio 2023[142] — l'ACN ha progressivamente consolidato un profilo

[139] Decreto Legislativo 4 settembre 2024, n. 138, Gazzetta Ufficiale n. 230 del 1° ottobre 2024, di recepimento della direttiva (UE) 2022/2555; cfr. ACN, "NIS — Network Information Security," https://www.acn.gov.it/portale/en/nis.

[140] Decreto-Legge n. 82/2021, art. 7; per un quadro complessivo cfr. ACN, Relazione annuale al Parlamento, edizioni 2023 e 2024.

[141] https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6?t=1719931791748

[142]Legge 29 dicembre 2022, n. 197, art. 1, comma 899; cfr. ACN, "Strategia nazionale di cybersicurezza: pubblicato il DPCM per la ripartizione dei fondi triennio 2025-2027," 21 ottobre 2025; Cfr. Cybersecurity360,

che combina la dimensione tecnico-operativa con quella di policy nazionale e internazionale. La Strategia individua nella *cyber diplom*acy uno degli obiettivi qualificanti dell'azione di Sistema, riconoscendo nella cooperazione internazionale uno strumento fondamentale per accrescere la resilienza collettiva e la postura del Paese.

Sul piano dell'azione esterna, l'ACN è stabilmente coinvolta in una pluralità di consessi multilaterali. L'Agenzia ha promosso l'istituzione del *G7 Cybersecurity Working Group* durante la Presidenza italiana del 2024, rappresenta il Paese nella *Counter Ransomware Initiative* (CRI) e contribuisce all'*Horizontal Working Party on Cyber Issues* del Consiglio dell'Unione, dove i suoi funzionari ricoprono il ruolo di *National Liaison Officer* presso ENISA. Siede inoltre nel board dell'*European Cybersecurity Competence Centre* (ECCC), assicurando un raccordo costante con le politiche industriali europee del settore[143]. Nel novembre 2025 l'Agenzia ha aderito al *Working Party on Digital Security Policy* dell'*Organization for Economic Cooperation and Development* (OCSE), forum di cooperazione multilaterale focalizzato sulle dimensioni economiche e sociali della cybersicurezza[144]. La dimensione bilaterale costituisce un ulteriore tassello dell'azione internazionale dell'Agenzia, che negozia protocolli d'intesa con omologhi di Paesi terzi e sviluppa programmi congiunti di *capacity building*, come testimoniato, tra l'altro, dalle missioni di alto livello presso il *Canadian Centre for Cyber Security* e dagli accordi di cooperazione siglati con partner alleati[145].

"Strategia nazionale di cybersicurezza: gli obiettivi da raggiungere entro il 2026 per la resilienza del Paese," 10 dicembre 2024.

[143]ACN, "International Relations — Relazioni Internazionali," https://www.acn.gov.it/portale/relazioni-internazionali; Cfr. Amel Attatfa, Karen Renaud e Stefano De Paoli, "Cyber Diplomacy: A Systematic Literature Review," Procedia Computer Science 176 (2020): 60-69.

[144]ACN, "Sicurezza digitale, l'Italia al tavolo OCSE con l'ACN," 5 novembre 2025, https://www.acn.gov.it/portale/w/sicurezza-digitale-l-italia-al-tavolo-ocse-con-l-acn

[145]ACN, "Canada: delegazione di ACN in missione," 25 novembre 2022, https://www.acn.gov.it/notizie/contenuti/canada-delegazione-acn-missione.

Sul piano ONU, l'Italia ha partecipato attivamente ai lavori dei *Group of Governmental Experts* (GGE) e dell'*Open-ended Working Group* (OEWG), contribuendo alla codificazione del cosiddetto *framework of responsible state behaviour*, fondato su undici norme volontarie, misure di *confidence-building*, applicazione del diritto internazionale e *capacity building*. Il secondo OEWG (2021-2025) si è concluso l'8 luglio 2025 con l'adozione consensuale del *Final Report* e con l'istituzione di un nuovo meccanismo permanente — il *Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs* — che ha tenuto la propria sessione organizzativa il 30-31 marzo 2026 e celebrerà la prima sessione sostanziale dal 20 al 24 luglio 2026[146]. Nell'intervento del 1° novembre 2025 in Prima Commissione dell'Assemblea Generale, l'Ambasciatore Leonardo Bencini, Rappresentante Permanente d'Italia presso la Conferenza del Disarmo, ha riaffermato l'impegno italiano per un cyberspazio aperto, interoperabile, sicuro e resiliente, rispettoso dei diritti umani e regolato dal pieno dispiegamento del diritto internazionale[147]. Tale orientamento si fonda sul *Position Paper* sul Diritto Internazionale e il Cyberspazio del 2021[148], redatto dal MAECI in collaborazione con la Presidenza del Consiglio, che codifica la posizione italiana su questioni nodali quali l'attribuzione degli attacchi informatici, la *due diligence* e l'applicabilità del principio di non intervento alle operazioni cibernetiche.

Il profilo italiano nei consessi multilaterali presenta tratti distintivi che meritano di essere esplicitati. Pur non disponendo della massa critica industriale e tecnologica delle grandi potenze, l'Italia ha sviluppato una postura caratterizzata

[146]DiploFoundation, "UN Global Mechanism on Cybersecurity in 2026," Digital Watch Observatory, https://dig.watch/processes/un-gge.

[147]OnuItalia, "Disarmo: Bencini per cyberspazio aperto e rispettoso dei diritti umani," 1° novembre 2025.

[148] MAECI, Italian Position Paper on International Law and Cyberspace, novembre 2021. https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

dalla coerenza tra dimensione normativa e dimensione operativa, dalla credibilità del proprio ecosistema istituzionale — in particolare l'ACN, riconosciuta in tempi rapidi come interlocutore qualificato a livello europeo — e dalla capacità di agire come ponte tra la dimensione transatlantica e quella mediterranea. La Presidenza G7 del 2024 ha mostrato come Roma sia in grado, quando dispone di una piattaforma istituzionale adeguata, di promuovere iniziative concrete che vengono adottate dai partner e si traducono in formati di cooperazione duraturi. La sfida, sul medio periodo, sarà quella di trasformare tale capacità di iniziativa in una proiezione strutturata, capace di influenzare in modo continuativo la formazione delle norme e degli standard internazionali e non solo di partecipare ai processi decisionali altrui.

In ambito europeo, l'Italia opera all'interno del *Cyber Diplomacy Toolbox* dell'Unione, lo strumento adottato nel 2017 e progressivamente raffinato che sistematizza le misure diplomatiche — incluse le *restrictive measures* — attivabili in risposta ad attività cyber malevole. L'entrata in applicazione della direttiva NIS2, recepita nell'ordinamento italiano nel 2024 e l'adozione del *Cyber Solidarity Act* hanno ulteriormente rafforzato l'architettura europea della resilienza cibernetica, ponendo le basi per la costruzione di un *EU Cyber Shield* articolato in *Security Operations Center* nazionali e transfrontalieri. A questo impianto si aggiunge la proposta di revisione del *Cybersecurity Act* presentata dalla Commissione Europea il 20 gennaio 2026 e nota come *Cybersecurity Act 2* (CSA2), che è destinata a ridisegnare ulteriormente i contorni dell'architettura cyber europea[149]. La proposta è articolata attorno a quattro pilastri: il rafforzamento del mandato dell'ENISA quale punto unico di riferimento UE in materia di cybersicurezza; la riforma del *European Cybersecurity Certification Framework*

[149] Commissione Europea, Proposta di regolamento relativo al regolamento dell'UE sulla cibersicurezza. 20 gennaio 2026. https://digital-strategy.ec.europa.eu/it/library/proposal-regulation-eu-cybersecurity-act

(ECCF) con tempistiche vincolanti dodici mesi dalla richiesta della Commissione e una nuova certificazione di *cyber posture* volta a facilitare la conformità NIS2 transfrontaliera; l'introduzione di un primo quadro orizzontale per la sicurezza delle catene di approvvigionamento ICT nei settori critici, con l'identificazione di *key ICT assets* e meccanismi di gestione del rischio non tecnico legato a fornitori provenienti da giurisdizioni sensibili; la limitazione della facoltà degli Stati membri di aggiungere requisiti nazionali in presenza di schemi UE armonizzati[150]. Il pacchetto, attualmente al vaglio del legislatore europeo e accompagnato da modifiche mirate alla NIS2, è destinato a incidere in misura significativa sui mercati delle telecomunicazioni e dei servizi cloud e a ridefinire le competenze delle Autorità nazionali. Per l'Italia, il negoziato CSA2 rappresenta un test decisivo: si tratterà di tutelare l'autonomia operativa dell'ACN — già consolidata come Autorità di riferimento nazionale — di fronte a un'architettura che amplia significativamente i poteri di ENISA e di valorizzare la posizione italiana nella definizione del nuovo regime di supply chain security, segmento in cui il sistema produttivo nazionale presenta sia vulnerabilità sia eccellenze esportabili.

Il versante atlantico rappresenta per l'Italia uno dei terreni più dinamici e, al tempo stesso, più delicati dell'attuale congiuntura. L'Alleanza Atlantica sta attraversando una fase di profonda ridefinizione, segnata dalla pressione esercitata dalla nuova Amministrazione statunitense per un riequilibrio del *burden sharing*, dall'aspettativa di un progressivo spostamento del baricentro strategico USA verso il teatro indo-pacifico e dall'esigenza correlata di rafforzare

[150] CMS Law-Now, "Strengthening EU cyber resilience: an overview of the new cybersecurity package", 3 febbraio 202. https://cms.law/en/lux/legal-updates/strengthening-eu-cyber-resilience-an-overview-of-the-new-cybersecurity-package

il cosiddetto pilastro europeo[151]. Il Vertice dell'Aia del 24-25 giugno 2025 ne ha rappresentato il passaggio più significativo: i trentadue Alleati hanno concordato l'obiettivo di portare la spesa per la difesa al 5% del PIL entro il 2035, articolato in un 3,5% destinato alle capacità militari *core* e in un 1,5% riservato a investimenti in infrastrutture critiche, cybersicurezza, mobilità militare e innovazione tecnologica duale[152]. Si tratta del più consistente incremento programmato dalla fine della Guerra Fredda, accompagnato da un *Rapid Adoption Action Plan* che impegna l'Alleanza a immettere nuove tecnologie nei sistemi operativi alleati entro ventiquattro mesi dal loro sviluppo.

L'accordo dell'Aia presenta per l'Italia implicazioni di rilievo, sia sul piano strategico sia su quello industriale e tecnologico. La premier Giorgia Meloni ha sottoscritto la dichiarazione finale, qualificando gli impegni come «necessari e sostenibili» e ottenendo, insieme ai partner europei, una flessibilità decennale per il raggiungimento del target[153]. Tuttavia, il quadro pone questioni di coerenza fra ambizione e capacità di esecuzione: passare dall'attuale livello di spesa, pari a circa l'1,5-1,6% del PIL, al 5% entro il 2035 richiederà un incremento stimato in circa cento miliardi di euro nell'arco del decennio, di cui circa sessantasei in difesa stretta e trentatré in sicurezza in senso ampio. La componente allargata dell'1,5% — destinata a infrastrutture critiche, cybersicurezza, mobilità militare e innovazione — apre però uno spazio significativo per la valorizzazione delle competenze nazionali in materia cyber e di intelligenza artificiale: ed è proprio in questo perimetro che l'ACN, l'ecosistema FAIR-PNRR, i campioni industriali

[151] Juan C. Castilla, “Burden sharing: real solidarity or arbitrary mathematics in NATO and the EU?” in Real Instituto Elcano, 30 luglio 2025. https://www.realinstitutoelcano.org/en/analyses/burden-sharing-real-solidarity-or-arbitrary-mathematics-in-nato-and-the-eu/

[152] NATO, The Hague Summit Declaration, 25 giugno 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration

[153] Euronews, Meloni, vertice Nato: aumento spesa militare può essere “circolo virtuoso per l'economia italiana”, 25 giugno 2025. https://it.euronews.com/my-europe/2025/06/25/meloni-vertice-nato-aumento-spesa-militare-puo-essere-circolo-virtuoso-per-leconomia-itali

(Leonardo, Fincantieri, Telespazio) e le PMI ad alto contenuto tecnologico possono trovare un terreno di crescita coerente con la rinnovata postura alleata[154].

La trasformazione in atto si accompagna a una più strutturale ridefinizione della postura alleata. La transazionalizzazione dell'approccio statunitense alla NATO, le tensioni sull'interpretazione condizionata dell'articolo 5, l'emergere di formati ad hoc fra Alleati *like-minded* e il ridimensionamento dell'ombrello di sicurezza tradizionalmente garantito da Washington sollecitano una riflessione più ampia sul modello di interoperabilità — anche tecnologica — e di sicurezza collettiva[155]. Per Roma, ciò significa porsi alcune questioni operative non differibili: in primo luogo, come tutelare l'autonomia decisionale nazionale rispetto a un'architettura industriale e tecnologica della difesa storicamente sbilanciata verso fornitori statunitensi, considerato che le vendite militari estere USA all'Europa sono passate da 11 miliardi di dollari nel periodo 2017-2021 a 68 miliardi nel solo 2024; in secondo luogo, come integrare gli investimenti NATO con i meccanismi del Fondo Europeo di Difesa, dello strumento SAFE e dell'*European Defence Industry Programme*, evitando duplicazioni e valorizzando la complementarità tra dimensione transatlantica ed europea; in terzo luogo, come tradurre la *Revised Artificial Intelligence Strategy* del 2024 — fondata sui sei *Principles of Responsible Use* — in concrete capacità *AI-enabled* del comparto difesa nazionale, garantendo la coerenza con il quadro regolativo dell'*AI Act* e la Legge n. 132/2025. La capacità dell'Italia di posizionarsi come anello solido del pilastro europeo della NATO — e non come mero *price-taker* di scelte altrui — dipenderà dalla qualità di queste tre

[154] Agenda Digitale, "2035: la NATO verso una nuova era di deterrenza strategica", 30 giugno 2025. https://www.agendadigitale.eu/sicurezza/2035-la-nato-verso-una-nuova-era-di-deterrenza-strategica/

[155] Beyond the Horizon ISSG, "NATO Summit The Hague 2025: Strategic Outcomes and Key Issues", 2 luglio 2025. https://behorizon.org/nato-summit-the-hague-2025-strategic-outcomes-and-key-issues/

risposte e dalla velocità con cui sapranno tradursi in scelte di bilancio, di politica industriale e di diplomazia tecnologica.

Su questo sfondo, la partecipazione italiana al *Defence Innovation Accelerator for the North Atlantic* (DIANA) e al *NATO Innovation Fund* (NIF) acquisisce un valore strategico rinnovato. Roma contribuisce stabilmente all'acceleratore e al fondo di venture capital multi-sovrano da un miliardo di euro, ospita siti DIANA presso istituzioni di ricerca nazionali e accede così alle filiere tecnologiche transatlantiche. Per consolidare tale presenza, sarà cruciale aumentare la quota italiana di *start-up* e PMI selezionate nei bandi DIANA e di investimenti veicolati dal NIF, anche tramite una più stretta sinergia con il Polo Strategico Nazionale, il CVCN e gli strumenti di sostegno alla *dual-use innovation* recentemente predisposti dal Ministero della Difesa.

Accanto ai consessi istituzionali, l'Italia partecipa a iniziative multilaterali tematiche che integrano il quadro classico della *cyber diplomacy*. La *Counter Ransomware Initiative* — lanciata nel 2021 e che riunisce circa sessanta Paesi — vede MAECI e ACN coordinare la partecipazione italiana al contrasto di una minaccia che colpisce in modo crescente entità pubbliche e private[156]. Sul versante della proliferazione e dell'uso irresponsabile degli strumenti commerciali di intrusione cibernetica, l'Italia ha aderito nel 2024 al *Pall Mall Process*, l'iniziativa informale lanciata congiuntamente da Regno Unito e Francia che riunisce ventisei Stati e numerosi attori non governativi attorno a un codice di condotta volontario per il settore degli *spyware* commerciali. La partecipazione a tali consessi consente all'Italia di concorrere alla definizione di standard di

[156] ACN, "Counter Ransomware Initiative (CRI)," https://www.acn.gov.it/portale/relazioni-internazionali/cri.

comportamento responsabile e di rafforzare la rete di partenariati operativi su minacce specifiche.

La riforma del MAECI e il *cyber capacity building* come strumento di proiezione

Il più significativo passaggio istituzionale del biennio 2024-2026 sul versante della *cyber diplomacy* italiana è rappresentato dalla riforma organizzativa del Ministero degli Affari Esteri e della Cooperazione Internazionale, disposta con il Decreto del Presidente della Repubblica 3 settembre 2025, che ha modificato il D.P.R. 95/2010[157]. Entrata in vigore il 1° gennaio 2026, la riforma costituisce il punto di approdo di un percorso avviato con il Decreto Ministeriale 7 dicembre 2023, n. 1202/3361 — che aveva istituito un'Unità per l'innovazione tecnologica e la sicurezza cibernetica — e si traduce nella creazione di una nuova Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica (DGCT), affidata alla guida del Ministro Plenipotenziario Alessandro De Pedys. La nuova architettura, presentata come operazione «a costo zero», deriva dalla soppressione della precedente Direzione Generale per l'amministrazione, l'informatica e le comunicazioni e dall'integrazione delle funzioni di policy internazionale in materia cyber e di gestione tecnica delle infrastrutture digitali della Farnesina e della rete diplomatico-consolare. Il Vicepresidente del Consiglio e Ministro degli Esteri, On. Antonio Tajani, ha descritto l'operazione come la trasformazione del MAECI in un «ministero bi-capite, con una testa politica — che si occuperà anche di intelligenza artificiale — e una testa economica».

[157]Decreto del Presidente della Repubblica 3 settembre 2025, modificativo del D.P.R. 18 luglio 2010, n. 95; Cfr. Cybersecurity360, "La Farnesina apre alla direzione generale per la cyber security di ministeri e ambasciate," 8 gennaio 2026. https://www.cybersecurity360.it/cybersecurity-nazionale/la-farnesina-apre-alla-direzione-generale-per-la-cyber-security-di-ministeri-e-ambasciate/

La DGCT, articolata su due Direzioni Centrali, riunisce competenze in precedenza distribuite tra diverse strutture, integrando — nelle parole del primo Direttore Generale — «competenze tecnologiche, giuridiche, economiche e strategiche in un'unica visione coerente»[158]. L'obiettivo dichiarato è quello di riconoscere che la diplomazia contemporanea non si esercita più soltanto nei consessi tradizionali, ma anche nelle reti, nei forum tecnici, nei tavoli di standardizzazione e nei processi di definizione delle regole globali del cyberspazio. La componente politica della Direzione presidia i rapporti internazionali in materia di sicurezza cibernetica, intelligenza artificiale e governance digitale; la componente tecnica è deputata al miglioramento dell'impiego dei mezzi informatici nella sede centrale e nelle ambasciate, consolati e rappresentanze permanenti. Il coordinamento con la Presidenza del Consiglio dei Ministri e con l'ACN — presso la quale opera un funzionario diplomatico in raccordo permanente — è espressamente previsto dal nuovo regolamento, evitando sovrapposizioni di competenze.

Cuore strategico della rinnovata azione del MAECI è l'ecosistema italiano di *cyber capacity building*, costituito due anni prima della riforma dalla Farnesina insieme all'ACN, che riunisce istituzioni, aziende e università in grado di realizzare progetti all'estero[159]. Tale strumento risponde a una duplice esigenza: contribuire alla stabilità internazionale offrendo soluzioni innovative ai partner — in particolare nel Mediterraneo allargato e in Africa — e proiettare il sistema

[158]CyberSecItalia, "Farnesina, De Pedys (MAECI): ecco com'è cambiata la nostra missione con la riforma cyber e digitale voluta dal Ministro Tajani," 2025, https://www.cybersecitalia.it/farnesina-de-pedys-maeci-ecco-come-cambiata-la-nostra-missione-con-la-riforma-cyber-e-digitale-voluta-dal-ministro-tajani/62753/

[159]CyberSecItalia, "Farnesina, De Pedys (MAECI): ecco com'è cambiata la nostra missione con la riforma cyber e digitale voluta dal Ministro Tajani," 2025, https://www.cybersecitalia.it/farnesina-de-pedys-maeci-ecco-come-cambiata-la-nostra-missione-con-la-riforma-cyber-e-digitale-voluta-dal-ministro-tajani/62753/.

produttivo nazionale in un mercato globale della sicurezza digitale in forte espansione. Come osservato dallo stesso Direttore Generale, «nessuna strategia internazionale può essere efficace se non coinvolge in modo strutturato il mondo imprenditoriale» e i partenariati pubblico-privati devono divenire «meccanismi permanenti di dialogo, scambio informativo e progettazione congiunta». Sul versante operativo, l'ecosistema si integra con le iniziative di *capacity building* promosse dalle Nazioni Unite — tra cui il gruppo dedicato istituito nel quadro del nuovo *Global Mechanism* — e con i programmi europei finanziati dallo strumento *Global Gateway*.

L'investimento sul *capacity building* riflette una lettura sofisticata della competizione internazionale contemporanea. In un'epoca in cui la concorrenza tra attori sistemici per l'influenza nel Sud Globale si gioca anche e soprattutto su infrastrutture digitali, standard tecnici e modelli di governance — con la Cina che esporta soluzioni di *smart city* e *safe city* e altri attori emergenti che propongono approcci alternativi alla regolazione delle piattaforme — il *cyber capacity building* rappresenta per l'Italia uno strumento di *soft power* tecnologico capace di tradursi in influenza politica e in posizionamento industriale[160]. Diversamente da un approccio puramente assistenziale, il modello italiano coniuga la dimensione formativa con quella commerciale, valorizzando la presenza di campioni nazionali nel settore della cybersicurezza e dell'aerospazio e ponendosi in continuità con il Piano Mattei per l'Africa, lanciato dal Governo italiano nel 2024 quale cornice strategica per i partenariati con il continente africano[161]. La sfida sarà quella di assicurare massa critica e sostenibilità finanziaria: a oggi i bilanci dedicati restano significativamente inferiori rispetto a quelli mobilitati da attori

[160] Sul ruolo dei partenariati digitali nella competizione tra grandi potenze Cfr. CSIS, Beyond U.S.-China Technology Competition (Washington, DC: CSIS, 2024)

[161] Presidenza del Consiglio dei ministri, Piano Mattei per l'Africa: Strategia, presentazione, gennaio 2024. https://www.governo.it/it/piano-mattei

come Francia, Germania e Regno Unito e a fortiori dalle grandi potenze sistemiche.

La riforma del MAECI introduce, sul piano giuridico, una dimensione ulteriore: l'intelligenza artificiale e la cybersicurezza divengono oggetto di sovranità amministrativa e di politica estera, con implicazioni rilevanti in tema di *export control*, *compliance* aziendale e coordinamento con l'*AI Act* europeo[162]. Le imprese impegnate in progetti internazionali di IA dovranno interfacciarsi con la nuova Direzione Generale per autorizzazioni e protocolli e le tecnologie di intelligenza artificiale potranno essere assoggettate a regimi analoghi a quelli previsti per i prodotti a duplice uso. La nuova architettura colloca infine l'Italia tra il numero ridotto di Paesi europei dotati di una struttura diplomatica unitaria dedicata alle questioni cyber e tecnologiche, in linea con esperienze quali quella del *Bureau of Cyberspace and Digital Policy* del Dipartimento di Stato statunitense o degli *Ambassador for Cyber Affairs* di numerosi partner UE.

La governance italiana dell'intelligenza artificiale

Il quadro italiano per l'intelligenza artificiale si è progressivamente strutturato attorno a tre pilastri complementari: la Strategia Italiana per l'Intelligenza Artificiale 2024-2026, la Legge n. 132/2025 e l'architettura di governance fondata sul ruolo congiunto di AgID e ACN. La Strategia, pubblicata il 22 luglio 2024 dall'Agenzia per l'Italia Digitale (AgID) e dal Dipartimento per la trasformazione digitale, sostituisce il Programma strategico 2022-2024 e si presenta come strumento di supporto al legislatore in una fase di particolare densità normativa, segnata dalla recente pubblicazione dell'AI Act europeo

[162] Gabriele Gallo Cassarino, "Cyber-diplomacy e AI: la nuova compliance internazionale nel riordino del MAECI," Diritto.it, 3 novembre 2025. https://www.diritto.it/cyber-diplomacy-intelligenza-artificiale-compliance/

(Regolamento UE 2024/1689)[163]. Il documento, redatto da un Comitato di quattordici esperti coordinato da Gianluigi Greco, Presidente di AIxIA, articola le proprie azioni strategiche in quattro macroaree — Ricerca, Pubblica Amministrazione, Imprese e Formazione — sostenute da un sistema di monitoraggio dell'attuazione e da un'analisi del contesto regolativo nazionale ed europeo.

Sul fronte della ricerca, la Strategia enfatizza l'importanza di rafforzare la cooperazione internazionale e gli investimenti in ricerca fondazionale e applicata, valorizzando il ruolo dell'accademia italiana — al settimo posto a livello mondiale per produzione scientifica nel settore — e promuovendo la creazione di dataset e modelli rilasciati in open source[164]. Il principale strumento attuativo è il Partenariato Esteso PNRR, *Future Artificial Intelligence Research* (FAIR), dotato di 114,5 milioni di euro per il triennio 2023-2025 e articolato in dieci *spoke* tematici, che riunisce 25 soggetti tra cui quattro enti di ricerca (CNR, Fondazione Bruno Kessler, INFN, Istituto Italiano di Tecnologia), quattordici università e sette imprese (Bracco, Deloitte, Expert.ai, Intesa Sanpaolo, Leonardo, Lutech, STMicroelectronics)[165]. Lo squilibrio rispetto ad altre economie europee resta tuttavia sensibile: a titolo esemplificativo, la sola Germania ha annunciato un finanziamento di 500 milioni di euro nel 2024 per coprire 150 nuove cattedre in IA, mentre studi recenti documentano come l'Europa abbia attratto solo il 6% dei finanziamenti globali per *start-up* IA nel primo semestre 2024, con il 70% del

[163]AgID, Strategia Italiana per l'Intelligenza Artificiale 2024-2026 (Roma: Presidenza del Consiglio dei ministri — Dipartimento per la Trasformazione Digitale, 2024). https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf.

[165] Fondazione FAIR — Future Artificial Intelligence Research, https://fondazione-fair.it/; Cfr. https://www.cnr.it/it/nota-stampa/n-11769/nasce-la-fondazione-fair-con-sede-al-cnr-di-pisa-gestira-114-milioni-di-euro-del-pnrr-sull-intelligenza-artificiale

mercato *cloud* dominato da *hyperscaler* americani[166]. Per la Pubblica Amministrazione si delinea un decalogo operativo per l'adozione di sistemi di IA, sviluppato nel Piano Triennale per l'Informatica nella PA 2024-2026 e accompagnato da Linee Guida specifiche oggetto di consultazione pubblica nel 2025. Per le imprese — in particolare per le piccole e medie imprese, che costituiscono l'ossatura del sistema produttivo nazionale — la Strategia prevede l'istituzione di una Fondazione per l'Intelligenza Artificiale incaricata della gestione di facilitatori (strumenti, infrastrutture e risorse), il consolidamento delle *start-up* ad alto contenuto tecnologico e la definizione di sandbox normative per la sperimentazione controllata di soluzioni innovative. Sul fronte della formazione, infine, la Strategia individua nell'alfabetizzazione digitale e nei percorsi di *reskilling* e *upskilling* le leve fondamentali per evitare l'insorgere di nuovi divari di conoscenza.

Con l'approvazione definitiva il 17 settembre 2025 e l'entrata in vigore il 10 ottobre dello stesso anno, la Legge n. 132/2025 — «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» — colloca l'Italia come primo Stato membro dell'Unione Europea ad essersi dotato di un quadro normativo organico allineato all'*AI Act*, il Regolamento (UE) 2024/1689 entrato in vigore il 1° agosto 2024 e in fase di applicazione progressiva sino al pieno spiegamento previsto per agosto 2026[167]. Sul piano italiano, la legge si fonda su principi di uso antropocentrico, trasparente e sicuro dell'IA, intervenendo in modo organico su più settori — sanità, lavoro, pubblica amministrazione e giustizia, formazione e

[166] Cfr. ICT Security Magazine, "EU AI Act 2025: nuove regole GPAI e impatto globale sull'Intelligenza Artificiale," 13 settembre 2025; analisi di Bruegel e Carnegie Endowment for International Peace. https://www.ictsecuritymagazine.com/notizie/eu-ai-act-2025-gpai/

[167] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, GU L 2024/1689 del 12 luglio 2024; Cfr. Commissione Europea, "AI Act," https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

sport — e prevedendo garanzie di tracciabilità, responsabilità umana e centralità della decisione finale di una persona fisica[168].

Sul piano della governance, la norma designa l'ACN e l'AgID quali Autorità nazionali competenti: l'ACN esercita poteri ispettivi e sanzionatori sull'adeguatezza e la sicurezza dei sistemi e è altresì responsabile della promozione e dello sviluppo dell'IA per i profili di cybersicurezza, mentre l'AgID gestisce le notifiche e promuove l'adozione sicura e responsabile dell'IA presso cittadini e imprese[169]. La doppia designazione consolida il ruolo dell'ACN come perno della governance italiana sia per la cybersicurezza sia per l'intelligenza artificiale e ne valorizza la dimensione internazionale. È inoltre istituito un Comitato di coordinamento presso la Presidenza del Consiglio dei Ministri e si introduce un meccanismo di programmazione strategica: la Strategia nazionale per l'IA sarà predisposta e aggiornata con cadenza biennale dal Dipartimento per la trasformazione digitale, con il supporto di ACN e AgID e in collaborazione con le principali autorità settoriali (Banca d'Italia, CONSOB, IVASS, Garante per la protezione dei dati personali e Agcom). Un monitoraggio annuale al Parlamento ne rafforza la trasparenza.

Sul piano degli investimenti, la legge attiva un programma da 1 miliardo di euro destinato a *start-up* e PMI nei settori dell'intelligenza artificiale, della cybersicurezza e delle tecnologie emergenti, con l'obiettivo di accelerare il trasferimento tecnologico e rafforzare le filiere strategiche nazionali. Una clausola di salvaguardia approvata in sede parlamentare — che impedisce ai

[168] Per un'analisi del rapporto tra Regolamento (UE) 2024/1689 e Legge n. 132/2025 cfr. Sergio Lorusso, "Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025," Giustizia Insieme, gennaio 2026. https://www.giustiziainsieme.it/articolo/3766-indagini-e-giudizio-fra-regolamento-ue-2024-1689-ai-act-e-legge-n-132-del-2025

[169] Legge n. 132/2025, art. 20; Cfr. A&O Shearman, "Law No. 132 of 23 September 2025: Italy's Leadership in National AI Regulation," 21 novembre 2025. https://www.aoshearman.com/en/insights/law-no-132-of-23-september-2025-italys-leadership-in-national-ai-regulation

decreti attuativi di introdurre obblighi ulteriori rispetto all'*AI Act* — mira a scongiurare fenomeni di *gold plating* regolatorio e tutela le imprese da potenziali aggravi amministrativi[170]. Va segnalato, inoltre, l'articolo 21 della legge, che stabilisce specifici finanziamenti per l'applicazione sperimentale dei sistemi di IA ai servizi forniti dal MAECI, in coerenza con la riforma della Direzione Generale per le questioni cibernetiche e con l'obiettivo di integrare la dimensione tecnologica nelle attività della rete diplomatico-consolare.

Quanto all'integrazione dell'IA nelle imprese italiane, l'Osservatorio Artificial Intelligence del Politecnico di Milano e il rapporto AI 4 Italy realizzato da *The European House* — Ambrosetti e Microsoft documentano una progressiva diffusione delle soluzioni di IA, con un mercato in forte crescita ma una distribuzione asimmetrica tra grandi imprese e PMI[171]. La verticalizzazione della Strategia sulle filiere produttive e la condivisione di dati reali — unitamente alla promozione di approcci basati su dataset sintetici — mira a colmare tale *gap*, integrandosi con il Piano Transizione 5.0 che individua nell'IA uno dei pilastri tecnologici della modernizzazione industriale.

Il modello italiano si colloca, in prospettiva analitica, in uno spazio intermedio tra l'approccio statunitense — caratterizzato da una regolazione settoriale leggera e da un forte impulso al mercato — e quello cinese, fondato su una pianificazione industriale verticale e su un controllo statale pervasivo. L'Italia condivide con il quadro europeo l'opzione per una regolazione orizzontale a base di rischio, ma vi affianca tre elementi distintivi: la designazione di Autorità dotate di competenze tecniche consolidate (l'ACN, in particolare, si è imposta come

[170] CCC Hub, "La nuova legge sull'Intelligenza Artificiale: il quadro regolatorio per le imprese italiane," Compliance Hub, 5 novembre 2025. https://www.compliancehub.it/2025/11/05/la-nuova-legge-sullintelligenza-artificiale-il-quadro-regolatorio-per-le-imprese-italiane/

[171] AI 4 Italy: impatti e prospettive dell'Intelligenza Artificiale generativa per l'Italia e il Made in Italy (The European House — Ambrosetti, Microsoft, 2024). https://www.ambrosetti.eu/news/ai-4-italy-impatti-e-prospettive-dellintelligenza-artificiale-generativa-per-litalia-e-il-made-in-italy/

riferimento europeo nel settore della cybersicurezza in tempi rapidi), una clausola anti *gold plating* volta a tutelare la competitività delle imprese e un esplicito raccordo tra governance interna e proiezione internazionale tramite il MAECI. Resta tuttavia aperta una tensione strutturale: la capacità effettiva del Paese — e dell'Unione Europea nel suo complesso — di tradurre il primato regolatorio in massa critica industriale, in un contesto in cui il divario tra Europa e superpotenze in termini di investimenti, infrastrutture di calcolo e talenti continua ad ampliarsi. La letteratura recente ha messo in dubbio l'effettiva capacità dell'*AI Act* di replicare la portata globale del GDPR, evidenziando come il «*Brussels effect*» possa risultare attenuato dall'assenza di un'industria europea dei modelli fondazionali[172]. Il successo dell'impostazione italiana sarà dunque misurabile, sul medio periodo, dalla capacità di tradurre il quadro normativo in ecosistemi produttivi competitivi e in nicchie di eccellenza riconosciute a livello globale, anche attraverso l'accelerazione del trasferimento tecnologico tra ricerca pubblica e tessuto industriale e una maggiore integrazione con le iniziative europee di sovranità tecnologica.

Implicazioni e opportunità per l'Italia

La concomitanza tra la riforma del MAECI, l'adozione della Legge n. 132/2025 e la fase attuativa della Strategia Nazionale di Cybersicurezza 2022-2026 — alimentata da risorse del PNRR e dai fondi dedicati per il triennio 2025-2027 — configura una finestra di opportunità di particolare rilievo per il sistema-Paese. La nuova DGCT colloca l'Italia tra il numero ridotto di Paesi europei dotati di una struttura diplomatica unitaria dedicata alle questioni cyber e tecnologiche: il valore di tale architettura risiede nella capacità di tradurla in una proiezione normativa coerente, valorizzando il ruolo italiano nei tavoli ONU del *Global*

[172] Cfr. Charlotte Siegmann e Markus Anderljung, "The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market", Centre for the Governance of AI

Mechanism e nei processi UE di standardizzazione e cooperazione tecnologica. La presenza di un interlocutore unico contribuisce inoltre a ridurre i costi di coordinamento per gli stakeholder privati e accademici impegnati su scala internazionale.

Essere il primo Stato membro UE ad essersi dotato di un quadro nazionale allineato all'*AI Act* offre all'Italia un vantaggio reputazionale e operativo non trascurabile. Sul piano dell'industria, la prevedibilità normativa anticipata e l'approntamento di *sandbox* — anche con valenze duali, in coordinamento con il Ministero della Difesa — possono attrarre investimenti e stimolare la nascita di nuove imprese. Sul piano della politica estera, il primato consente di proporsi come partner privilegiato di Paesi terzi che si misurino con sfide regolative analoghe, segnatamente nell'area mediterranea e nei Balcani e di esportare modelli di compliance compatibili con il quadro europeo.

L'ecosistema costruito da MAECI e ACN per il *cyber capacity building* rappresenta un asset distintivo che può essere ulteriormente potenziato. Le opportunità risiedono nella sua integrazione con i programmi di cooperazione allo sviluppo — segnatamente il Piano Mattei per l'Africa[173] — e con le iniziative europee finanziate nel quadro del *Global Gateway*. Si tratta di consolidare un modello di diplomazia tecnologica con sostantività industriale, in cui le competenze pubbliche e private italiane si presentino in modo coordinato sui mercati emergenti, contribuendo al tempo stesso alla stabilità internazionale e alla crescita delle filiere nazionali.

La doppia designazione di ACN e AgID quali Autorità competenti per l'IA — in stretto raccordo con la DGCT del MAECI per la dimensione internazionale — apre

[173] Darlington Tshuma, *Digital Transformation: Aligning Italy's Piano Mattei with African Development Priorities*, IAI Papers, Roma, IAI, giugno 2025. https://www.iai.it/sites/default/files/iaip2507.pdf

la possibilità di costruire un modello italiano di governance integrata in cui cybersicurezza e intelligenza artificiale non siano trattate come silos regolativi separati, ma come componenti complementari di una medesima strategia di resilienza. Tale impostazione — coerente con quanto previsto dalla Strategia Nazionale di Cybersicurezza, che contempla la promozione di certificazioni e schemi di conformità nei settori EUCC ed ENISA — può favorire l'emergere di un sigillo italiano di affidabilità tecnologica spendibile anche sui mercati esteri.

Infine, la partecipazione italiana a DIANA e al *NATO Innovation Fund*, unitamente all'adesione alla *Revised AI Strategy* del 2024, offre alle imprese e ai centri di ricerca nazionali un accesso privilegiato all'ecosistema dell'innovazione transatlantica. L'opportunità è duplice: per un verso, contribuire allo sviluppo di capacità alleate fondate sui *Principles of Responsible Use*; per altro verso, valorizzare nicchie di eccellenza italiana — dall'ipersonica ai materiali avanzati, dalle biotecnologie ai sistemi autonomi — in un mercato della difesa caratterizzato da crescenti investimenti pubblici e da una progressiva integrazione dei fondi dell'*European Defence Fund* (EDF) con i meccanismi NATO.

Su queste basi, è possibile individuare alcune direttrici operative su cui l'azione italiana può consolidarsi nel breve-medio periodo. Una prima direttrice riguarda la strutturazione della *cyber diplomacy* come funzione permanente: la nuova DGCT può essere il fulcro di una rete di referenti cyber e tecnologici presso le principali Rappresentanze diplomatiche con un mandato di raccolta informativa, *advocacy* e supporto alle imprese, sul modello dei *digital attachés* sperimentato da partner europei[174]. Una seconda direttrice attiene

[174] Per il modello *digital attaché* si veda: TechMonitor, Tech ambassadors are redefining diplomacy for the digital era, 16 febbraio 2021. https://www.techmonitor.ai/policy/geopolitics/tech-ambassadors?cf-view; Tech Diplomacy Global Institute, The Rise of Tech Ambassadors: Redefining Modern Diplomacy, 7 novembre 2025. https://tdgi.org/the-rise-of-tech-ambassadors-redefining-modern-diplomacy/; Tech Diplomacy Global Institute, Tech Ambassadors Around the World: A Comparative Analysis, 11 novembre

al consolidamento del modello italiano di *capacity building*, attraverso la creazione di una piattaforma permanente di coordinamento MAECI-ACN-AgID-Difesa-Cooperazione Italiana, dotata di una *pipeline* pluriennale di progetti nel Mediterraneo allargato, in Africa e nei Balcani occidentali, integrata con il Piano Mattei e con i finanziamenti *Global Gateway*[175]. Una terza direttrice attiene al negoziato europeo: nei prossimi diciotto mesi si concentreranno passaggi decisivi (CSA2, attuazione del *Cyber Solidarity Act*, pacchetto sovranità tecnologica del maggio 2026, primo aggiornamento dell'*AI Act)* sui quali la posizione italiana dovrà essere preparata in modo strutturato, valorizzando l'esperienza maturata in qualità di primo Stato membro UE ad aver adottato un quadro nazionale allineato all'*AI Act*. Una quarta direttrice riguarda il versante atlantico: la finestra aperta dall'1,5% di spesa allargata stabilita all'Aia richiede una rapida individuazione di filiere e progetti italiani da candidare alle linee di finanziamento NATO e ai bandi DIANA, con particolare attenzione ai segmenti — IA per la difesa, *quantum*, materiali avanzati, sistemi autonomi, biotecnologie — in cui il sistema-Paese può esprimere nicchie di eccellenza. Una quinta direttrice, infine, attiene alla dimensione cognitiva e formativa: la qualità della *cyber diplomacy* dipenderà dalla capacità di formare una nuova generazione di diplomatici, funzionari e dirigenti dotati di competenze tecnologiche solide, attraverso programmi congiunti tra MAECI, Scuola Nazionale dell'Amministrazione, università italiane di eccellenza e centri di ricerca dell'ecosistema FAIR.

2025. https://tdgi.org/tech-ambassadors-around-the-world-a-comparative-analysis/. Per il caso specifico della Danimarca, si veda: https://um.dk/techamb/en/

[175] Commissione Europea, *Global Gateway Investment Package*, aggiornato 2025. https://international-partnerships.ec.europa.eu/policies/global-gateway_it

Conclusioni

L'Italia si trova in una fase di particolare rilevanza strategica, in cui la dimensione digitale è divenuta un elemento strutturale del proprio posizionamento internazionale. In un contesto globale segnato dalla crescente competizione tecnologica, dalla frammentazione geopolitica e dal ritardo europeo nelle filiere più avanzate, il Paese è chiamato a compiere scelte coerenti tra capacità nazionali, integrazione europea e proiezione multilaterale.

Sul piano interno, il consolidamento dell'architettura di cybersicurezza — con il rafforzamento del ruolo dell'ACN, l'attuazione della Strategia Nazionale e il recepimento della direttiva NIS2 — ha contribuito a definire una postura più matura e credibile anche a livello internazionale. In parallelo, l'integrazione tra cybersicurezza e intelligenza artificiale, sostenuta anche dalla recente normativa nazionale, delinea un modello di governance che considera queste due dimensioni come componenti complementari della resilienza del sistema-Paese. In questo quadro, la riforma del MAECI e l'istituzione di una direzione generale dedicata rappresentano un passaggio chiave, segnando il riconoscimento della centralità del digitale nella politica estera. Allo stesso tempo, lo sviluppo di iniziative di *cyber capacity building* rafforza la proiezione esterna dell'Italia, contribuendo sia alla stabilità internazionale sia al supporto del sistema produttivo nei mercati emergenti.

Permangono, tuttavia, alcune sfide rilevanti. In primo luogo, la necessità di garantire coerenza tra disegno strategico e implementazione operativa, evitando disallineamenti tra ambizioni e capacità di esecuzione. In secondo luogo, il tema della massa critica, con livelli di investimento in ricerca e innovazione ancora inferiori rispetto ai principali partner europei, che rischiano di limitare la traduzione del primato regolatorio in capacità industriale. Infine, la qualità del

coordinamento interistituzionale rappresenta un fattore decisivo per assicurare l'efficacia complessiva dell'architettura, valorizzando la complementarità tra i diversi attori coinvolti.

Le recenti evoluzioni a livello internazionale ed europeo offrono opportunità concrete per rafforzare il ruolo dell'Italia nella governance globale del digitale e dell'intelligenza artificiale, in linea con i principi di apertura, sicurezza e tutela dei diritti. Tre passaggi del prossimo biennio saranno particolarmente significativi: il negoziato sul *Cybersecurity Act 2*, che ridisegnerà il perimetro delle competenze cyber dell'Unione e l'autonomia operativa delle Autorità nazionali; la fase attuativa degli impegni del Vertice NATO dell'Aia, che imporrà scelte di bilancio e di politica industriale di portata storica e che potrà tradursi — se ben gestita — in un rilancio della filiera tecnologica nazionale; l'avvio operativo del *Global Mechanism* delle Nazioni Unite sulla sicurezza ICT. La capacità di cogliere queste opportunità dipenderà dalla qualità delle scelte strategiche dei prossimi anni, dalla coerenza tra strumenti diplomatici, industriali e regolativi e dal grado di coinvolgimento coordinato di istituzioni, industria e mondo accademico in una visione condivisa di sovranità digitale e proiezione internazionale. In un contesto segnato dalla transazionalizzazione dei rapporti transatlantici, dalla rivalità sistemica tra grandi potenze e dalla competizione per gli standard tecnologici globali, l'Italia ha gli strumenti per giocare un ruolo non subalterno: il banco di prova sarà la velocità con cui saprà tradurre l'architettura costruita negli ultimi anni in capacità di iniziativa autonoma e di *leadership* tematica nei consessi che contano.

Riferimenti bibliografici

ACN — Agenzia per la Cybersicurezza Nazionale. “Canada: delegazione di ACN in missione.” 25 novembre 2022. https://www.acn.gov.it/notizie/contenuti/canada-delegazione-acn-missione

ACN — Agenzia per la Cybersicurezza Nazionale. “NIS — Network Information Security.” https://www.acn.gov.it/portale/en/nis.

ACN — Agenzia per la Cybersicurezza Nazionale. “Sicurezza digitale, l’Italia al tavolo OCSE con l’ACN.” 5 novembre 2025. https://www.acn.gov.it/portale/w/sicurezza-digitale-l-italia-al-tavolo-ocse-con-l-acn

ACN — Agenzia per la Cybersicurezza Nazionale. “Strategia nazionale di cybersicurezza: pubblicato il DPCM per la ripartizione dei fondi triennio 2025-2027.” 21 ottobre 2025. https://www.acn.gov.it/portale/w/strategia-nazionale-di-cybersicurezza-pubblicato-il-dpcm-per-la-ripartizione-dei-fondi-triennio-2025-2027

ACN — Agenzia per la Cybersicurezza Nazionale. Strategia Nazionale di Cybersicurezza 2022-2026. Roma: Presidenza del Consiglio dei Ministri, 2022. https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6?t=1719931791748

Agenda Digitale, "2035: la NATO verso una nuova era di deterrenza strategica", 30 giugno 2025. https://www.agendadigitale.eu/sicurezza/2035-la-nato-verso-una-nuova-era-di-deterrenza-strategica/

AgID — Agenzia per l’Italia Digitale. Strategia Italiana per l’Intelligenza Artificiale 2024-2026. Roma: Presidenza del Consiglio dei Ministri — Dipartimento per la Trasformazione Digitale, 2024. https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf.

Allen, Gregory C. “DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race.” CSIS Report, marzo 2025. https://www.csis.org/analysis/deepseek-huawei-export-controls-and-future-us-china-ai-race

A&O Shearman. “Law No. 132 of 23 September 2025: Italy’s Leadership in National AI Regulation.” 21 novembre 2025. https://www.aoshearman.com/it-

it/insights/law-no-132-of-23-september-2025-italys-leadership-in-national-ai-regulation

Attatfa, Amel, Karen Renaud, Stefano De Paoli. “Cyber Diplomacy: A Systematic Literature Review.” Procedia Computer Science 176 (2020): 60-69. https://www.sciencedirect.com/science/article/pii/S1877050920318317

Bradford, Anu. The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press, 2020.

Beyond the Horizon ISSG, "NATO Summit The Hague 2025: Strategic Outcomes and Key Issues", 2 luglio 2025. https://behorizon.org/nato-summit-the-hague-2025-strategic-outcomes-and-key-issues/

Bunde, Tobias, Sophie Eisentraut, Leonard Schütte, a cura di. Munich Security Report 2025: Multipolarization. Monaco di Baviera: Munich Security Conference, 2025. https://securityconference.org/assets/02_Dokumente/01_Publikationen/2025/MSR_2025/Multipolarization_–_Munich_Security_Report_2025.pdf

Castilla Juan, “Burden sharing: real solidarity or arbitrary mathematics in NATO and the EU?” in Real Instituto Elcano, 30 luglio 2025. https://www.realinstitutoelcano.org/en/analyses/burden-sharing-real-solidarity-or-arbitrary-mathematics-in-nato-and-the-eu/

CCC Hub. “La nuova legge sull’Intelligenza Artificiale: il quadro regolatorio per le imprese italiane.” Compliance Hub, 5 novembre 2025. https://www.compliancehub.it/2025/11/05/la-nuova-legge-sullintelligenza-artificiale-il-quadro-regolatorio-per-le-imprese-italiane/.

Center for European Policy Analysis (CEPA). “Burying the Brussels Effect? AI Act Inspires Few Copycats.” 2025. https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats/

Center for Strategic and International Studies. A World Dividing. Winning the Economic and Tech Race. Global Forecast 2024. Washington, DC: CSIS, 2024. https://features.csis.org/global-forecast-economic-tech-race/

Commissione Europea. “AI Act — Shaping Europe’s Digital Future.” https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Commissione Europea, *Global Gateway Investment Package*, aggiornato 2025. https://international-partnerships.ec.europa.eu/policies/global-gateway_it

CyberSecItalia. “Farnesina, De Pedys (MAECI): ecco com’è cambiata la nostra missione con la riforma cyber e digitale voluta dal Ministro Tajani.” 2025. https://www.cybersecitalia.it/farnesina-de-pedys-maeci-ecco-come-cambiata-la-nostra-missione/62753/.

Cybersecurity360. “La Farnesina apre alla direzione generale per la cyber security di ministeri e ambasciate.” 8 gennaio 2026. https://www.cybersecurity360.it/cybersecurity-nazionale/la-farnesina-apre-alla-direzione-generale-per-la-cyber-security-di-ministeri-e-ambasciate/.

Dipartimento per la Trasformazione Digitale. “Approvata in via definitiva la legge italiana sull’Intelligenza Artificiale.” 31 ottobre 2025. https://innovazione.gov.it/notizie/articoli/approvata-in-via-definitiva-la-legge-italiana-sull-intelligenza-artificiale/.

DiploFoundation. “UN Global Mechanism on Cybersecurity in 2026.” Digital Watch Observatory. https://dig.watch/processes/un-gge.

Draghi, Mario. The Future of European Competitiveness. Part A: A Competitiveness Strategy for Europe. Bruxelles: Commissione Europea, settembre 2024. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

Euronews, Meloni, vertice Nato: aumento spesa militare può essere “circolo virtuoso per l'economia italiana”, 25 giugno 2025. https://it.euronews.com/my-europe/2025/06/25/meloni-vertice-nato-aumento-spesa-militare-puo-essere-circolo-virtuoso-per-leconomia-itali

Gallo Cassarino, Gabriele. “Cyber-diplomacy e AI: la nuova compliance internazionale nel riordino del MAECI.” Diritto.it, 3 novembre 2025. https://www.diritto.it/cyber-diplomacy-intelligenza-artificiale-compliance/

ICT Security Magazine. “EU AI Act 2025: nuove regole GPAI e impatto globale sull’Intelligenza Artificiale.” 13 settembre 2025. https://www.ictsecuritymagazine.com/notizie/eu-ai-act-2025-gpai/

Lorusso, Sergio. “Indagini e giudizio fra regolamento (UE) 2024/1689 (AI Act) e legge n. 132 del 2025.” Giustizia Insieme, gennaio 2026. https://www.giustiziainsieme.it/articolo/3766-indagini-e-giudizio-fra-regolamento-ue-2024-1689-ai-act-e-legge-n-132-del-2025

MAECI — Ministero degli Affari Esteri e della Cooperazione Internazionale. Position Paper on International Law and Cyberspace. Roma: MAECI, 2021. https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

NATO. “Summary of NATO’s Revised Artificial Intelligence (AI) Strategy.” 10 luglio 2024. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

NATO. “Warsaw Summit Communiqué.” 9 luglio 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO, The Hague Summit Declaration, 25 giugno 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration

Picotti, Lorenzo. “La nuova architettura di cybersicurezza nazionale. Note a prima lettura del decreto-legge n. 82 del 2021.” Federalismi.it, n. 24 (2021). https://www.federalismi.it/nv14/articolo-documento.cfm?artid=47078

Repubblica Italiana. Decreto Legislativo 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555 (NIS2). Gazzetta Ufficiale n. 230 del 1° ottobre 2024.

Repubblica Italiana. Decreto-Legge 14 giugno 2021, n. 82, convertito nella Legge 4 agosto 2021, n. 109. Gazzetta Ufficiale n. 140 del 14 giugno 2021.

Repubblica Italiana. Decreto del Presidente della Repubblica 3 settembre 2025, modificativo del D.P.R. 18 luglio 2010, n. 95. 2025.

Repubblica Italiana. Legge 23 settembre 2025, n. 132, “Disposizioni e deleghe al Governo in materia di intelligenza artificiale.” Gazzetta Ufficiale n. 223 del 25 settembre 2025.

Savini, Alessandro. “La NATO e il vantaggio tecnologico: pubblicata la prima strategia per l’IA.” Geopolitica.info, 6 aprile 2022. https://geopolitica.info/nato-vantaggio-tecnologico-pubblicata-la-prima-strategia-per-ia/

Siegmann, Charlotte, Markus Anderljung. “The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market.” Centre for the Governance of AI Technical Report, 2022. https://cdn.governance.ai/Brussels_Effect_GovAI.pdf

Stimson Center. “Cyber Diplomacy 2.0: From Process to Impact.” 12 agosto 2025. https://www.stimson.org/2025/cyber-diplomacy-2-0-from-process-to-impact/

Tech Diplomacy Global Institute, The Rise of Tech Ambassadors: Redefining Modern Diplomacy, 7 novembre 2025. https://tdgi.org/the-rise-of-tech-ambassadors-redefining-modern-diplomacy/

Tech Diplomacy Global Institute, Tech Ambassadors Around the World: A Comparative Analysis, 11 novembre 2025. https://tdgi.org/tech-ambassadors-around-the-world-a-comparative-analysis/.

TechMonitor, Tech ambassadors are redefining diplomacy for the digital era, 16 febbraio 2021. https://www.techmonitor.ai/policy/geopolitics/tech-ambassadors?cf-view

The European House — Ambrosetti e Microsoft. AI 4 Italy: impatti e prospettive dell’Intelligenza Artificiale generativa per l’Italia e il Made in Italy. 2024. https://www.ambrosetti.eu/news/ai-4-italy-impatti-e-prospettive-dellintelligenza-artificiale-generativa-per-litalia-e-il-made-in-italy/

Tshuma Darlington, *Digital Transformation: Aligning Italy's Piano Mattei with African Development Priorities*, IAI Papers, Roma, IAI, giugno 2025. https://www.iai.it/sites/default/files/iaip2507.pdf

L'approccio italiano al dominio spaziale interconnesso con il cyberspazio e le tecnologie emergenti

Valentina Chabert

Spazio: da dominio di interesse scientifico a terreno di competizione

Dagli anni Cinquanta ed in particolare a partire dai primi esperimenti di messa in orbita di satelliti durante l'era del bipolarismo nelle relazioni internazionali, il settore spaziale ha subìto profonde modifiche in termini di innovazione tecnologica e assetti cooperativi tra potenze spaziali. In particolare, gli ultimi decenni sono stati testimoni di una progressiva erosione del monopolio statale nel settore spaziale, in favore dell'ingresso di società private dotate di notevoli capacità tecniche, ingenti disponibilità di capitali e di una spinta innovativa tale per cui sembra prendere forma un modello di *governance* "dal basso verso l'alto",[176] guidato da società commerciali che promettono sviluppi tecnologici continui, rapidi e più economici rispetto al passato.[177] Su questa linea, l'entrata in una nuova fase della corsa allo spazio ha portato all'alternanza di una significativa cooperazione internazionale (la costruzione della Stazione Spaziale Internazionale ne è un esempio) con periodi di più intensa competizione tra potenze, mosse da differenti imperativi di natura securitaria, economica e geopolitica.[178] In un simile contesto, il progressivo sviluppo tecnologico ha svolto un ruolo chiave nell'identificazione dell'ambiente spaziale come infrastruttura critica. All'aumento del numero di satelliti in orbita è infatti corrisposta una crescente dipendenza umana da tali sistemi, tale per cui attualmente le

[176] P. Samson, Is the Earth's Orbit Becoming a Lawless Frontier?, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

[177] L. Dawson, *The politics and perils of space exploration. Who will compete, who will dominate?* Springer, 2nd edition, 2021, p. 44.

[178] Società Italiana per l'Organizzazione Internazionale (SIOI), *Alla conquista dell'ottavo continente: lo Spazio, La Comunità Internazionale,* Quaderno 21, Editoriale Scientifica Napoli, 2021, p. 46.

infrastrutture spaziali risultano fondamentali per le comunicazioni, la navigazione e l'osservazione della Terra, così come per la sincronizzazione delle transazioni finanziarie, i trasporti e le previsioni meteorologiche, tra gli altri aspetti.[179] I sistemi basati sullo spazio risultano altresì critici nel corso di operazioni militari, consentendo un comando e controllo sicuri, la navigazione, la raccolta di informazioni e l'allerta precoce delle minacce. Inoltre, le infrastrutture spaziali forniscono comunicazioni essenziali per il coordinamento delle forze, la guida di sistemi d'arma e il monitoraggio dei movimenti sul terreno dell'avversario. Pertanto, anche in prospettiva militare si riconferma il ruolo centrale dei sistemi spaziali, il cui eventuale danneggiamento potrebbe destabilizzare la prontezza militare, la risposta alle crisi e la coesione delle Forze Armate di uno Stato.[180]

Come emergerà nel corso del presente lavoro, affermandosi quale spina dorsale di alcune delle principali attività economiche moderne, l'infrastruttura spaziale è ugualmente oggetto di potenziali effetti dannosi derivanti da eventuali perdite di capacità, aprendo parallelamente a rischi e vulnerabilità non trascurabili da parte degli Stati.[181] La dimensione cibernetica diviene, a questo proposito, imprescindibile: nonostante un generale consenso sulla necessità di un'attenzione mirata alla connessione tra spazio extra-atmosferico e spazio cibernetico alla luce delle potenziali minacce alla sicurezza provenienti dalla vulnerabilità delle infrastrutture critiche spaziali e da attacchi mirati contro di esse, attualmente non si riscontrano linee guida dettagliate e specifiche per il

[179] Cfr. M. Spagnulo, *Capitalismo stellare. Come la nuova corsa allo spazio cambia la Terra*, Rubettino, 2023.
[180] J. Cournoyer, Securing the space-based assets of NATO members from cyberattacks. A framework to strenghten cybersecurity in outer space, *Royal Institute of International Affairs International Security Programme Research Paper,* 2025, pp. 6-8.
[181] B. Gallant, J. Miller, The Growth of the Space Economy and New Cyber Vulnerabilities, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

settore della sicurezza informatica destinate agli operatori di satelliti commerciali e in generale all'intera catena delle infrastrutture spaziali - dalle orbite ai segmenti di terra.[182] Tuttavia, la crescente dipendenza del settore spaziale dai sistemi informatici e il conseguente nesso "spazio-*cyber*" derivante dall'impiego di componenti *hardware* e *software*, dalla riconfigurazione dei satelliti in orbita, dall'utilizzo dell'intelligenza artificiale e di tecnologie quantistiche rendono le risorse e i dati spaziali sempre più suscettibili a nuove forme di vulnerabilità informatica, in un contesto spaziale sempre più congestionato, contestato e competitivo.[183] Le vulnerabilità descritte e le tendenze evolutive del settore spaziale interessano anche l'Italia, la cui infrastruttura spaziale si regge su una rete di aziende pionieristiche attive nel settore della difesa, piccole e medie imprese, *startup* d'avanguardia e un sistema di alleanze che si realizza tramite una stretta cooperazione con le principali potenze spaziali internazionali - gli Stati Uniti *in primis* - e una collaborazione strategica con l'Agenzia Spaziale Europea (ESA).[184]

In questo contesto, il lavoro porrà al centro l'approccio italiano al dominio spaziale come ambito strategico sempre più interconnesso con il cyberspazio e le tecnologie emergenti, volgendo lo sguardo alle crescenti interdipendenze tra le infrastrutture spaziali, la cybersicurezza e l'intelligenza artificiale. Si evidenzieranno in modo particolare i rischi e le vulnerabilità legate alla digitalizzazione dei sistemi spaziali – dalle orbite in cui stazionano i satelliti, ai dati e al cosiddetto *ground segment*, al fine di valutare le potenziali implicazioni in

[182] European Union Agency for Cybersecurity (ENISA), *Space Threat Landscape*, 2025, pp. 7-8.
[183] A. Shul, W. Wark, J. West, Securing the new Space Domain: An Introduction, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.
[184] K. Muti, O. Credi, G. La Rocca, Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity, *Istituto Affari Internazionali*, 2023, p. 5. Si veda anche A. Aresu, R. Mauro, *I cancelli del cielo. Economia e politica della grande corsa allo spazio 1950-2050*, Luiss University Press, 2022.

termini di sicurezza nazionale. Da ultimo, un'enfasi sull'interconnessione del settore spaziale con il dominio cibernetico intende mettere in risalto una concezione sempre più radicata dello spazio come estensione della dimensione *cyber*, idonea a configurarsi come nesso imprescindibile nei moderni scenari di competizione tecnologica.

Spazio extra-atmosferico e spazio cibernetico: convergenza securitaria e tecnologie emergenti

Nonostante sussistano differenze strutturali tra i due domini, il cyberspazio e lo spazio extra-atmosferico condividono una serie di analogie derivanti dalla loro natura aperta, condivisa e transfrontaliera.[185] Pertanto, una maggiore interdipendenza tra le due dimensioni dovuta all'incremento del numero di satelliti e la conseguente digitalizzazione dei sistemi spaziali hanno significativamente acuito i rischi di attacchi informatici contro le infrastrutture spaziali. In effetti, i satelliti sono spesso dotati di componenti *software* e di connessione ad internet. Inoltre, la maggior parte dei processi di progettazione, produzione, collaudo, lancio e gestione dei satelliti avviene tramite tecnologie digitali. A ciò è dunque seguita un'estensione della superficie di attacco, ossia dei punti di accesso potenzialmente sfruttabili da un aggressore per interrompere, danneggiare, disabilitare o assumere il controllo di un satellite. A titolo di esempio, alcuni studi hanno calcolato che un'eventuale indisponibilità del sistema di navigazione statunitense GPS potrebbe generare un impatto economico di circa 1 miliardo di dollari al giorno. Similmente, un attacco informatico ad un satellite potrebbe causare un'interruzione dei mercati finanziari, dei trasporti su strada, delle previsioni metereologiche, delle reti

[185] P. Meyer, Outer Space and Cyber Space: a Tale of Two Security Realms, in: A. M. Osula, H. Roigas (eds), *International Cyber Norms: Legal, Policy and Industry Perspectives*, NATO CCD COE Publications, 2016.

elettriche e addirittura del controllo del traffico aereo o di operazioni militari in corso.[186]

Tuttavia, la sicurezza informatica dei sistemi spaziali non si limita al satellite in orbita, bensì comprende l'intera catena di approvvigionamento, l'utente, i segmenti di terra e quelli spaziali durante l'intero ciclo di vita dell'infrastruttura, creando ulteriori livelli di complessità. I sistemi spaziali infatti consistono di tre componenti, tutte ugualmente necessarie al corretto funzionamento dell'infrastruttura: i satelliti in orbita, le comunicazioni e i dati inviati da e verso i satelliti e le stazioni di terra che controllano i satelliti o ricevono i dati e i segnali da essi. Dunque, le capacità informatiche risultano fondamentali per l'ambiente spaziale nel suo complesso e per la stabilità e la prevedibilità delle sue risorse.[187]

Sebbene gli attacchi informatici richiedano un alto grado di comprensione degli *asset* spaziali presi di mira, essi non esigono necessariamente risorse significative per essere portati a termine. I cyberattacchi contro i satelliti implicano di fatto una serie complessa di vulnerabilità che compromettono la stabilità e la funzionalità dei sistemi spaziali. Tra esse si distinguono il *jamming*, lo *spoofing* e il *Man-in-the-Middle* (MiTM). Il *jamming* prevede l'interruzione deliberata della connettività del server attraverso un'interferenza con i segnali di comunicazione, ottenuta trasmettendo energia elettromagnetica sulle stesse frequenze dei segnali bersaglio e sovraccaricando il ricevitore. In questo modo, viene impedito il recupero dei segnali attaccando il *downlink* tra il satellite e il ricevitore a terra o l'*uplink* tra la stazione di terra e il satellite. Il fine ultimo di un simile attacco consiste nell'intralciare trasmissioni, reti o servizi internet per

[186] C. Poirier, Understanding Cybersecurity in Outer Space, *CSS Analyses in Security Policy*, n. 343, 2024, p.2.
[187] V. Samson, The Cyber Counterspace Threat: Coming Out of the Shadows, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

interferire con le comunicazioni satellitari globali, con impatti estesi sino al diniego del servizio e all'interruzione di sistemi critici dipendenti dai satelliti sulla Terra o nello spazio. Sulla stessa linea, lo *spoofing* sfrutta una tecnica illusoria tale per cui l'attore altera i segnali di comunicazione per ingannare il destinatario, dando l'impressione di autenticità dei dati. La tecnica di attacco sfrutta i ricevitori *online,* facendo credere che i segnali decimati siano autentici e dunque mettendo in pericolo veicoli spaziali o satelliti alterandone la traiettoria per il tramite di dati ingannevoli. Per quanto riguarda le reti e i sistemi informatici spaziali, gli aggressori possono altresì manipolare i sensori o i dati da cui dipendono i sistemi o le reti: questi si basano su dati precisi per eseguire operazioni computerizzate automatizzate, raccogliere informazioni e comunicare dettagli significativi ai controllori di terra. Manipolando questi dati, gli aggressori possono causare operazioni automatizzate indesiderate, innescando un comportamento imprevedibile del veicolo spaziale o del satellite. Inoltre, i dati manipolati potrebbero inviare ai controllori di terra informazioni ingannevoli, minando l'affidabilità e l'integrità del veicolo spaziale. Da ultimo, un attacco *MitM* si verifica quando l'autore falsifica e intercetta i dati posizionandosi tra l'utente e il sistema.

I moderni attacchi informatici contro i sistemi spaziali risultano solitamente più difficili da rilevare, con conseguenze che vanno dalla negazione del servizio su vasta area o guasti mirati all'integrità dell'infrastruttura.[188] Non sono inoltre da escludere ulteriori modalità attraverso cui le capacità informatiche potrebbero essere impiegate deliberatamente al fine di danneggiare tanto i satelliti militari quanto quelli commerciali. Intrusioni informatiche potrebbero infatti consentire il controllo dei satelliti e la loro trasformazione in strumenti capaci di schiantarsi

[188] K. Yang, M. Hassan, A review of the legal nature of cyberattacks in outer space, *Acta Astronautica*, vol. 244, 2026, pp. 335-343.

contro altri *hardware* presenti in orbita, causando danni tali da renderli inutilizzabili.[189] È quanto è avvenuto nel 1998 a seguito del controllo, da parte di un gruppo di hacker, del satellite astronomico tedesco ROSAT, i cui pannelli solari sono stati puntati verso il sole e dunque distrutti, causando detriti che ancora oggi rappresentano un rischio per la sicurezza di altri oggetti e operatori in orbita. Più di recente, nel mese di novembre 2021, la Federazione Russa ha distrutto un satellite di epoca sovietica – il *Kosmos 1408* – per il tramite di un missile antisatellite che ha generato oltre 1500 frammenti e costretto gli astronauti presenti sulla Stazione Spaziale Internazionale a rifugiarsi nelle capsule di emergenza in via precauzionale. Infine, sul fronte cinese un simile episodio risale al 2007, con la deliberata distruzione da parte delle autorità di Pechino del satellite meteorologico *Fengyun-1C* attraverso un missile ASAT. Oltre a produrre più di 3500 frammenti di detriti ancora oggi in orbita, l'attacco contro il satellite ha messo in luce il rischio concreto di compromissione di ulteriori sistemi spaziali potenzialmente coinvolti.

Limitatamente alle conseguenze, oltre ai danni di natura non fisica gli attacchi informatici alle infrastrutture spaziali possono risultare in altrettanti danni significativi all'*hardware*. Offensive mirate contro sistemi satellitari sono suscettibili di danneggiare fisicamente i satelliti, deorbitandoli, provocando detriti in orbita, danni sulla Terra e interruzioni di servizi critici, con conseguenti danni a infrastrutture e talvolta vite umane. A questo proposito, l'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) ha stimato che le conseguenze derivanti da attacchi cibernetici contro infrastrutture critiche spaziali risulterebbero ulteriormente aggravate dal duplice uso degli *asset* satellitari, per cui tecnologie commerciali destinate all'uso civile potrebbero

[189] J. West, Where Outer Space Meets Cyberspace: A Human-Centric Look at Space Security, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

comunque essere impiegate come armi a sostegno di obiettivi geopolitici.[190] È quanto emerso, ad esempio, dall'attacco cibernetico al satellite Viasat nel 2022 a poche ore dall'invasione russa dell'Ucraina, responsabile dello spegnimento di decine di migliaia di modem in tutta Europa e dell'interruzione tanto di attività economiche, quanto di diverse funzioni vitali tra cui servizi di emergenza.[191]

Simili effetti a catena sono destinati a diventare più comuni con l'avvento dell'intelligenza artificiale e dell'*Internet of Things* (IoT), che crea complesse reti interconnesse di dispositivi informatici, macchine, dati, oggetti e persone fortemente dipendenti dai sistemi spaziali.[192]

Pertanto, la sicurezza informatica dei sistemi spaziali assume un ruolo fondamentale per garantire il corretto funzionamento dei servizi spaziali e delle infrastrutture di supporto.[193] Tuttavia, permangono numerose criticità al fine del raggiungimento di tale obiettivo. *In primis*, secondo quanto emerge dallo *Space Attacks Open Database Project*, una base dati che raccoglie informazioni relative ad attacchi pubblicamente noti contro satelliti tra il 1977 e il 2019, la divulgazione di episodi di offese cibernetiche non risulta essere una pratica consolidata.[194] In aggiunta, è solo con l'integrazione di studi specifici[195] e rapporti pubblicamente disponibili su singoli incidenti di sicurezza informatica nel dominio spaziale che si evince una più ampia targetizzazione di obiettivi commerciali, governativi e -

[190] ENISA, *cit.,* p. 8.
[191] *Ivi,* pp. 17-18.
[192] R. Mazzolin, Responding to the Cybersecurity Challenges of the New Space Environment, *CICI Cybersecurity and Outer Space Essay Series*, 2023.
[193] C. Poirier, Establishing a governance for cyber operations in outer space: Exploring challenges faced by space and cyber commands, *Acta Astronautica*, vol. 237, 2025, p. 236.
[194]Space Attacks Open Database Project. Disponibile al link: https://www.spacesecurity.info/space-attacks-open-database/.
[195] W. Wark, The Five Eyes and Space: A New Frontier for an Old Intelligence Alliance, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

soprattutto dagli anni 2000 - del *ground segment* dell'infrastruttura spaziale.[196] In secondo luogo, permangono incertezze relative al nesso tra gli ambiti giuridici dello spazio extra-atmosferico e del cyberspazio, con la potenziale sussistenza di una zona grigia in cui l'applicazione del diritto internazionale risulta poco chiara o carente. In effetti, il diritto fornisce un contributo essenziale alla *governance* senza tuttavia essere sufficiente a garantire una condivisione piena ed efficiente delle responsabilità tra gli attori che operano nel settore spaziale, complice la natura multiforme delle vulnerabilità e delle minacce informatiche, la multifunzionalità dei sistemi spaziali e l'interconnessione delle capacità spaziali con i servizi terrestri. Dunque, la cooperazione e il coordinamento tra operatori geograficamente dispersi e tra settori commerciali e governativi diventa essenziale e al contempo una sfida, anche all'interno di un singolo Stato o di un gruppo di alleati. A livello globale, inoltre, una simile sfida è ulteriormente complicata dalla competizione tra potenze e da una diversa percezione delle minacce, lasciando scoperto un fronte essenziale per il futuro del settore spaziale.[197]

In terzo luogo, come anticipato, le interferenze informatiche appaiono difficili da rilevare, da distinguere da fonti involontarie o naturali e complesse da attribuire a specifici attori. Il fatto che le capacità informatiche siano utilizzate non solo dagli Stati ma anche da attori non statuali inclusi *hacktivisti*, gruppi terroristici, *proxy* e criminali informatici, rende ancora più intricata l'individuazione e la persecuzione dei responsabili. Nel complesso, risulta dunque difficile prevenire simili attacchi a fronte della continua evoluzione delle minacce, degli attori coinvolti e dei punti di vulnerabilità, non limitati al software bensì inclusivi della

[196] ENISA, *cit.,* p. 29; C. Poirer, Understanding Cybersecurity in Outer Space, *cit.,* p.2.
[197] A. Shul, W. Wark, J. West, *cit.*

rete di componenti, servizi e fornitori delle catene di approvvigionamento dei sistemi satellitari.[198]

Alla luce di ciò, un aggiornamento delle strategie di tutela delle infrastrutture critiche che includa anche i sistemi spaziali nella loro interezza potrebbe avere un impatto significativo in termini di resilienza e preparazione alle minacce provenienti dal dominio cyberspaziale. A questo proposito, standard tecnici, di servizio e requisiti di condivisione delle informazioni, così come una migliore allocazione delle risorse per la mitigazione delle conseguenze derivanti da attacchi cibernetici, appaiono urgenti per il rafforzamento delle capacità di cybersicurezza dei sistemi spaziali. Non meno importante, infine, l'elemento umano, che rimane la chiave di volta per l'incremento di strategie efficaci di difesa cibernetica: un ecosistema solido capace di valorizzare al meglio esperti e professionisti del settore è quantomai essenziale per la formazione di una futura generazione di specialisti in grado di combinare un'elevata conoscenza informatica con la comprensione dei rischi e delle vulnerabilità derivanti dal settore spaziale, da realizzarsi in combinazione con il settore privato , il cui ruolo nella filiera spaziale è teso ad un progressivo incremento.[199]

Il ruolo dell'Italia nella filiera spaziale internazionale: verso la definizione di una profondità strategica

Con il lancio del San Marco 1 il 15 dicembre del 1964 grazie all'ingegno di un gruppo di ricercatori dell'Università "La Sapienza", l'Italia si è affermata come potenza nel teatro spaziale mantenendo una posizione di successo per tutti i decenni successivi, tanto a livello europeo con il contributo alla fondazione dell'Agenzia Spaziale Europea, quanto a livello internazionale.[200] L'ambizione di

[198] J. West, *cit.*
[199] B. Gallant, J. Miller, *cit.*
[200] S. Marchisio, Italy as the Launching State of the San Marco I, *Ordine Internazionale e Diritti Umani*, 2025.

portare l'Italia al centro dell'attenzione mondiale in ambito spaziale si è recentemente concretizzata con l'approvazione del Senato, lo scorso 20 dicembre 2023, del disegno di legge sul *Made in Italy*, che prevede interventi di valorizzazione, promozione e tutela delle eccellenze nazionali italiane anche nel campo della politica industriale del Paese, con iniziative volte a stimolare e proteggere la crescita delle filiere strategiche nazionali in vista delle sfide globali del presente. Al settore spaziale quale pilastro decisivo per il comparto industriale italiano è stata riservata un'attenzione particolare anche nell'ottica del raggiungimento dell'obiettivo più ampio di garantire un accesso autonomo europeo allo spazio. Un proposito che si intreccia nuovamente, nella storia dell'Italia, con il continente africano, da cui sono dipesi il protagonismo e l'iniziale avventura spaziale italiana e che ha visto un rinnovato interesse del paese in ambito spaziale soprattutto nei confronti del Kenya attraverso il Piano Mattei. A titolo di esempio, in conclusione dell'incontro a Roma con il presidente del Kenya William Ruto il 20 aprile scorso, il Premier Giorgia Meloni ha infatti affermato con decisione la volontà dell'Italia di potenziare il Centro Spaziale Luigi Broglio di Malindi, base operativa dell'Agenzia Spaziale Italiana (ASI), al fine di renderlo un *hub* continentale di formazione ed eccellenza tale da permettere all'Italia una proiezione nel continente africano, strategico per i lanci orbitali grazie alla sua vicinanza all'equatore.[201]

Al contempo, il protagonismo dell'Italia nel *dossier* spazio si espleta attraverso numerosi assetti collaborativi soprattutto in ambito europeo e occidentale, in modo particolare attraverso la cooperazione con la NASA. Di fatto, con un miliardo di euro di budget annuale, il supporto chiave è fornito dall'ASI, che

[201] AGEEI, Spazio, Italia-Kenya, Meloni incontra il Presidente Ruto, 21 aprile 2026. Disponibile al link: https://ageei.eu/spazio-italia-kenya-meloni-incontra-il-presidente-ruto-potenziare-il-centro-spaziale-luigi-broglio-a-malindi/.

svolge il compito di coordinare progetti relativi all'esplorazione spaziale, all'osservazione della Terra e all'abilitazione dell'industria spaziale. Al contempo, l'Italia risulta essere il terzo finanziatore dell'ESA, nonché tra i firmatari degli Accordi Artemis, grazie ai quali le imprese italiane hanno svolto un ruolo protagonista nella missione Artemis II lanciata il 1° aprile 2026 e ricopriranno altresì una posizione di prim'ordine per le successive missioni. Con la coordinazione dell'ASI, la Penisola ha infatti apportato un notevole contributo ad *Orion*, il modulo di servizio che insieme al *Space Launch System* della NASA ha costituito il fulcro di Artemis I; in Artemis II, Leonardo ha realizzato i pannelli fotovoltaici che compongono le ali del modulo e le unità di controllo e distribuzione della potenza, fondamentali per fornire alimentazione a tutta l'elettronica di bordo e alimentare *Orion* durante il viaggio di andata e ritorno dalla Luna; infine, nel sito di Thales Alenia Space a Torino sono in realizzazione per la NASA e l'ASI la prima casa sulla Luna per gli astronauti e il primo *lander* lunare europeo – *Argonaut* – progettato per l'ESA per il trasporto e l'atterraggio di carichi sulla superficie lunare.

Non meno importante, in termini legislativi la centralità del settore spaziale italiano si deve ad una riconfigurazione delle norme esistenti in materia a partire dal 2018, dapprima con la legge 7/2018 *Recante Misure per il Coordinamento della Politica Spaziale e Aerospaziale e Disposizioni concernenti l'Organizzazione e il Funzionamento dell'Agenzia Spaziale Italiana*, che ha previsto che la direzione e il coordinamento delle politiche spaziali e aerospaziali siano attribuiti al Presidente del Consiglio, mentre gli indirizzi di Governo ad un comitato interministeriale *ad hoc*.[202] In particolare, le telecomunicazioni, la navigazione e l'osservazione della Terra saranno oggetto delle politiche sviluppate nei prossimi

[202] Legge 11 gennaio 2018 n.7, pubblicata in G.U. n.34 del 10 febbraio 2018.

anni, in aggiunta alla *Strategia Nazionale di Sicurezza per lo Spazio* approvata dal COMINT nel luglio dello stesso anno.[203] Tra gli obiettivi strategici del documento, la garanzia della sicurezza delle infrastrutture spaziali e la tutela del comparto istituzionale, industriale e scientifico figurano tra le priorità del Paese. Più recentemente, con la legge 89 del 13 giugno 2025 recante *Disposizioni in materia di economia dello spazio*, anche l'Italia si è dotata di una disciplina delle attività spaziali condotte da operatori privati sul territorio nazionale e da operatori italiani al di fuori del territorio nazionale, sul modello già adottato da numerosi paesi europei ed extraeuropei.[204]

Con queste premesse, dall'interconnessione tra il settore spaziale e la cybersicurezza e le implicazioni securitarie descritte nel paragrafo precedente, emerge una chiara necessità per l'Italia di adattare il proprio approccio strategico integrando sicurezza spaziale e cibernetica. In modo particolare, un simile approccio risulta impellente alla luce dell'importanza che il settore spaziale ha rivestito e che occupa nel panorama economico attuale, frutto di una crescente attenzione all'operato di *startup*, piccole e medie imprese e società già attive nel campo dell'industria della difesa, che hanno assunto un ruolo via via più incisivo nel settore della *new space economy* e nelle partnership internazionali dell'Italia in ambito spaziale.

A tale scopo, il Ministero degli Esteri e della Cooperazione Internazionale (MAECI) ha progressivamente riconosciuto la rilevanza strategica del settore spaziale e la necessità di garantire la protezione delle infrastrutture critiche da

[203] Presidenza del Consiglio dei Ministri, Strategia nazionale di sicurezza per lo spazio, COMINT, 18 luglio 2019.

[204] Presidenza del Consiglio dei Ministri, Ufficio per le Politiche Spaziali e Aerospaziali, *Disposizioni in materia di economia dello spazio.* Disponibile al link: https://www.ufficiopolitichespaziali.gov.it/home/normativa/disposizioni-in-materia-di-economia-dello-spazio/.

minacce cibernetiche, promuovendo specifiche linee di indirizzo politico e partecipando a programmi di cooperazione con partner internazionali volti al rafforzamento della sicurezza spaziale e *cyber*. Il MAECI ha infatti riconosciuto come lo spazio rappresenti per l'Italia un motore di innovazione tecnologica, competitività e crescita economica attraverso una solida partecipazione ai principali programmi europei ed internazionali, sostenuta da uno sforzo diplomatico che ha permesso all'Italia di presiedere il Comitato delle Nazioni Unite per gli usi pacifici dello spazio extra-atmosferico (COPUOS) nel biennio 2026-2027.[205] Al fine di promuovere una maggiore cooperazione internazionale nell'utilizzo pacifico dello spazio e allo stesso tempo la sicurezza, il MAECI ha altresì intrapreso una ferma strategia diplomatica in ambito cibernetico, fondata sul multilateralismo e la condivisione di informazioni finalizzata a prevenire attacchi cibernetici e contribuire alla definizione di una governance del cyberspazio aperta, accessibile e rispettosa del diritto internazionale. L'impegno del MAECI si concretizza, tra gli altri fronti, nell'attuazione della *Strategia Nazionale di Cybersicurezza* nei fora multilaterali e nell'ambito di coalizioni informali, a livello europeo, onusiano, nell'Alleanza Atlantica, nel contesto dell'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) e in seno al G7. Considerate le principali minacce cibernetiche che potrebbero rappresentare una minaccia per la sicurezza del paese, la coordinazione del MAECI e dell'Agenzia per la Cybersicurezza Nazionale garantisce all'Italia la partecipazione alla *Counter Ransomware Initiative*, avviata informalmente nel 2021 con l'obiettivo di contribuire al fenomeno del furto di dati a scopo di estorsione. Attraverso il MAECI l'Italia ha poi aderito, nel 2023, al *Meccanismo di Tallin*, al fine di sistematizzare e coordinare le attività di assistenza civile

[205] MAECI, Spazio. Disponibile al link: https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/spazio/.

all'Ucraina nel campo della cybersicurezza a fronte delle conseguenze dell'aggressione russa. A tal proposito, l'Italia deterrà la presidenza del Meccanismo nei mesi di luglio-dicembre 2026, incentrando la propria attività sulla valorizzazione del partenariato pubblico-privato. Da ultimo, il MAECI ha promosso la presenza italiana a fianco di altri 26 paesi anche nel *Processo di Pall Mall*, un'iniziativa informale lanciata nel 2024 da Francia e Regno Unito per contrastare la proliferazione e l'utilizzo irresponsabile di prodotti commerciali di intrusione cibernetica.[206]

Altrettanto rilevante risulta il rafforzamento da parte dell'Italia della propria postura securitaria attraverso l'allineamento delle proprie strategie spaziali e di cybersicurezza con l'Alleanza Atlantica. La NATO ha infatti individuato lo spazio extra-atmosferico come quinto dominio operativo accanto allo spazio aereo, quello terrestre, quello marino e quello cibernetico, rendendo necessaria la protezione delle infrastrutture critiche posizionate in tale area o dipendenti dallo spazio stesso ai fini della sicurezza dell'Alleanza. A tal proposito, l'Italia ha integrato progressivamente i propri *asset* spaziali (come il sistema di comunicazione militare SICRAL) all'interno di architetture di rete orientate alla sicurezza e alla resilienza.[207] Al contempo, si registra un'intensa cooperazione con la NATO in termini di condivisione delle informazioni relative ad attacchi cibernetici e nell'ambito dei dati di *Space Domain Awareness* (SDA), contribuendo al monitoraggio di detriti, vettori e attività ostili in orbita che potrebbero

[206] MAECI, Diplomazia Cibernetica. Disponibile al link: https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/.

[207] Presidenza del Consiglio dei Ministri, *Government Guidelines on Space and Aerospace*, 14 gennaio 2025. Disponibile al link: https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_Meloni/Ufficio_ConsMilitare/GovernmentGuidelinesOnSpaceAndAerospace.pdf.

compromettere la sicurezza collettiva. Uno sforzo che a livello interno si è concretizzato nella firma di un accordo quadro nel mese di ottobre 2025 tra l'Agenzia Spaziale Italiana e l'Agenzia per la Cybersicurezza Nazionale (ACN) inteso a rafforzare contemporaneamente la resilienza cibernetica e la sicurezza del settore spaziale e aerospaziale italiano per il tramite di soluzioni di sicurezza avanzate, crittografia *quantum-resistant*, metodologie *zero trust* e attività per prevenire e contrastare minacce cibernetiche che potrebbero riguardare le infrastrutture spaziali e il relativo *downstream* applicativo.[208] Dal punto di vista industriale, in linea con la *Commercial Space Strategy* dell'Alleanza Atlantica, l'Italia ha recentemente consolidato i propri legami di sicurezza con alcuni alleati chiave, come dimostrato dai recenti dialoghi strategici sullo spazio con gli Stati Uniti conclusosi nel mese di aprile 2026.[209] Obiettivo finale dell'Italia risulta dunque quello di garantire la resilienza di servizi civili e militari essenziali per la sicurezza del paese, posizionandosi come partner tecnologico e strategico fondamentale per la difesa collettiva della NATO. In questo senso, la rilevanza strategica a cui è assurto lo spazio richiede infatti una presenza italiana di primo piano: a tale fine, ad un costante sviluppo delle proprie capacità tecnologiche e spaziali dovrà affiancarsi la protezione dei propri *asset* strategici e delle infrastrutture critiche spaziali, che potrebbero divenire *target* di specifiche e deliberate attività malevole di natura cibernetica volte a destabilizzare il paese e a minarne la sicurezza per il tramite degli strumenti della guerra cosiddetta "ibrida", a dimostrazione di quanto lo spazio sia divenuto un dominio operativo

[208] Agenzia Spaziale Italiana (ASI), Accordo tra ASI e ACN per rafforzare la cybersicurezza del settore spaziale e aerospaziale, 6 ottobre 2025. Disponibile al link: https://www.asi.it/2025/10/accordo-tra-asi-e-acn-per-rafforzare-la-cybersicurezza-del-settore-spaziale-e-aerospaziale/.

[209] US Department of State, Joint Statement on the Second US – Italy Space Dialogue, 17 aprile 2026. Disponibile al link: https://www.state.gov/releases/bureau-of-oceans-and-international-environmental-and-scientific-affairs/2026/04/joint-statement-on-the-second-u-s-italy-space-dialogue.

sul quale si proiettano tanto alleanze quanto fronti di competizione in essere sulla superficie terrestre.[210]

Conclusioni

Alla luce delle dinamiche analizzate, il dominio spaziale si configura non solo come un'infrastruttura critica autonoma, bensì come una vera e propria estensione del cyberspazio, con cui condivide vulnerabilità, logiche operative e crescente interdipendenza tecnologica. In questo senso, lo spazio extra-atmosferico assume il ruolo di *enabling domain*, ossia di moltiplicatore di capacità civili e militari che abilita funzioni essenziali per le economie contemporanee e, al contempo, rappresenta uno dei principali teatri della competizione tecnologica tra attori statali e non statali. La convergenza tra sistemi spaziali, cybersicurezza e tecnologie emergenti – *in primis* l'intelligenza artificiale – rafforza ulteriormente questa centralità, amplificandone tuttavia anche la superficie di attacco e la complessità della gestione del rischio.

Appare dunque necessario superare approcci settoriali e frammentati, al fine di promuovere una maggiore integrazione tra politiche spaziali e cibernetiche tramite strategie coordinate che tengano conto dell'intero ciclo di vita delle infrastrutture spaziali, includendo tanto i segmenti orbitali quanto quelli terrestri e digitali. Parallelamente, risultano imprescindibili investimenti mirati nel rafforzamento della sicurezza informatica dei sistemi spaziali e nell'adozione responsabile dell'intelligenza artificiale, al fine di garantire resilienza e capacità di risposta in un ambiente sempre più competitivo.

Infine, la natura intrinsecamente globale e interconnessa dello spazio impone un rafforzamento della cooperazione internazionale. La definizione di standard

[210] V. Chabert, *Guerre Spaziali. Conflitti e competizione per le risorse nell'era delle società private*, Ledizioni, 2025.

condivisi, meccanismi di fiducia reciproca e iniziative multilaterali nel campo della sicurezza *space-cyber* rappresentano elementi chiave per mitigare i rischi sistemici e prevenire escalation indesiderate. In questa prospettiva, l'Italia – forte del suo posizionamento industriale e delle sue alleanze strategiche – ha l'opportunità di contribuire attivamente alla costruzione di un quadro normativo e operativo più integrato, capace di rispondere alle sfide emergenti e di valorizzare appieno il potenziale dello spazio come dominio abilitante del futuro tecnologico.

Riferimenti bibliografici

AGEEI, Spazio, Italia-Kenya, Meloni incontra il Presidente Ruto, 21 aprile 2026. https://ageei.eu/spazio-italia-kenya-meloni-incontra-il-presidente-ruto-potenziare-il-centro-spaziale-luigi-broglio-a-malindi/.

Agenzia Spaziale Italiana (ASI), Accordo tra ASI e ACN per rafforzare la cybersicurezza del settore spaziale e aerospaziale, 6 ottobre 2025. https://www.asi.it/2025/10/accordo-tra-asi-e-acn-per-rafforzare-la-cybersicurezza-del-settore-spaziale-e-aerospaziale/.

A.Aresu, R. Mauro, *I cancelli del cielo. Economia e politica della grande corsa allo spazio 1950-2050*, Luiss University Press, 2022.

V. Chabert, *Guerre Spaziali. Conflitti e competizione per le risorse nell'era delle società private*, Ledizioni, 2025.

J. Cournoyer, Securing the space-based assets of NATO members from cyberattacks. A framework to strenghten cybersecurity in outer space, *Royal Institute of International Affairs International Security Programme Research Paper,* 2025.

L. Dawson, *The politics and perils of space exploration. Who will compete, who will dominate?* Springer, 2nd edition, 2021.

European Union Agency for Cybersecurity (ENISA), *Space Threat Landscape*, 2025.

B. Gallant, J. Miller, The Growth of the Space Economy and New Cyber Vulnerabilities, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

Legge 11 gennaio 2018 n.7, Gazzetta Ufficiale n.34, 10 febbraio 2018.

MAECI, Spazio. https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/spazio/.

MAECI, Diplomazia Cibernetica. Disponibile al link: https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/diplomazia_cyber_e_digitale/diplomazia-cibernetica/.

S. Marchisio, Italy as the Launching State of the San Marco I, *Ordine Internazionale e Diritti Umani*, 2025.

R. Mazzolin, Responding to the Cybersecurity Challenges of the New Space Environment, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

P. Meyer, Outer Space and Cyber Space: a Tale of Two Security Realms. In: A. M. Osula, H. Roigas (eds), *International Cyber Norms: Legal, Policy and Industry Perspectives*, NATO CCD COE Publications, 2016.

K. Muti, O. Credi, G. La Rocca, Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity, *Istituto Affari Internazionali*, 2023.

C. Poirier, Establishing a governance for cyber operations in outer space: Exploring challenges faced by space and cyber commands, *Acta Astronautica*, vol. 237, 2025.

C. Poirier, Understanding Cybersecurity in Outer Space, *CSS Analyses in Security Policy*, n. 343, 2024.

Presidenza del Consiglio dei Ministri, Government Guidelines on Space and Aerospace, 14 gennaio 2025. https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_Meloni/Ufficio_ConsMilitare/GovernmentGuidelinesOnSpaceAndAerospace.pdf.

Presidenza del Consiglio dei Ministri, Strategia nazionale di sicurezza per lo spazio, COMINT, 18 luglio 2019.

Presidenza del Consiglio dei Ministri, Ufficio per le Politiche Spaziali e Aerospaziali, *Disposizioni in materia di economia dello spazio.* https://www.ufficiopolitichespaziali.gov.it/home/normativa/disposizioni-in-materia-di-economia-dello-spazio/.

P. Samson, Is the Earth's Orbit Becoming a Lawless Frontier?, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

V. Samson, The Cyber Counterspace Threat: Coming Out of the Shadows, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

A.Shul, W. Wark, J. West, Securing the new Space Domain: An Introduction, *CIGI Cybersecurity and Outer Space Essay Series*, 2023.

Società Italiana per l'Organizzazione Internazionale (SIOI), *Alla conquista dell'ottavo continente: lo Spazio, La Comunità Internazionale,* Quaderno 21, Editoriale Scientifica Napoli, 2021.

Space Attacks Open Database Project. https://www.spacesecurity.info/space-attacks-open-database/.

M. Spagnulo, *Capitalismo stellare. Come la nuova corsa allo spazio cambia la Terra*, Rubettino, 2023.

US Department of State, Joint Statement on the Second US – Italy Space Dialogue, 17 aprile 2026. https://www.state.gov/releases/bureau-of-oceans-and-international-environmental-and-scientific-affairs/2026/04/joint-statement-on-the-second-u-s-italy-space-dialogue.

W. Wark, The Five Eyes and Space: A New Frontier for an Old Intelligence Alliance, *CICI Cybersecurity and Outer Space Essay Series*, 2023.

J. West, Where Outer Space Meets Cyberspace: A Human-Centric Look at Space Security, *CICI Cybersecurity and Outer Space Essay Series,* 2023.

K. Yang, M. Hassan, A review of the legal nature of cyberattacks in outer space, *Acta Astronautica*, vol. 244, 2026.

BIOGRAFIA DEI CURATORI E DEGLI AUTORI

Alessandro Savini consulente in materia di cybersecurity, ambito in cui ha maturato una solida esperienza in Cyber Strategy & Governance, supportando organizzazioni dei settori governativo e finanziario nel rafforzamento della propria postura di sicurezza attraverso la definizione di modelli di governance e framework di gestione del rischio. È Research Fellow del Centro Studi Geopolitica.info, dove coordina le attività del Programma Cyber & Tech. I suoi interessi di ricerca si concentrano sulla sicurezza del cyberspazio come dominio strategico, con particolare attenzione al ruolo dell'Italia nel contesto euro-atlantico e alle implicazioni per la sicurezza nazionale. Ha inoltre collaborato con diverse testate e piattaforme di settore, contribuendo con analisi e approfondimenti sui temi della cybersecurity, della geopolitica del digitale e delle tecnologie emergenti.

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.

Alessandra Russo ha ottenuto un dottorato di ricerca in “Istituzioni e Politiche”, conseguito con lode presso l’Università Cattolica del Sacro Cuore di Milano, nel Dipartimento di Scienze Politiche. La sua attività di ricerca si concentra sulle tecnologie emergenti, con particolare riferimento all’applicazione militare dell’intelligenza artificiale, al suo impatto a livello tattico-operativo e alle implicazioni per le dinamiche di sicurezza globale, la governance e le politiche pubbliche.

Pierluigi Paganini è uno dei più autorevoli esperti italiani e internazionali di sicurezza informatica e cyber intelligence. Per oltre dieci anni ha ricoperto un ruolo chiave in ENISA, l’Agenzia dell’Unione Europea per la Sicurezza delle Reti e dell'Informazione, occupandosi di cyber threat intelligence e partecipando ai principali gruppi di lavoro europei sulla cyber threat landscape. Paganini ha collaborato con numerosi enti governativi, tra cui il Ministero degli Affari Esteri e il Ministero dell’Economia e delle Finanze, contribuendo alla definizione di linee guida strategiche nazionali e internazionali. Un contributo di rilievo è la sua partecipazione al G7 del 2017 come co-autore della Dichiarazione di Lucca sulle norme di comportamento responsabile degli Stati nel cyberspazio, documento fondamentale nel dibattito sulla cyber diplomacy. Imprenditore di successo, ha fondato Cybaze, uno dei principali gruppi cyber privati italiani, realtà di spicco del settore poi acquisita dal gruppo Tinexta, consolidando così l’ecosistema nazionale della cybersecurity. Paganini è noto anche come fondatore di SecurityAffairs.com, blog nato oltre 14 anni fa e oggi riconosciuto tra le principali fonti mondiali di informazione, analisi tecnica e trend della cyber sicurezza. In ambito accademico, ricopre ruoli di responsabilità presso diverse università italiane, progettando e dirigendo master e programmi di formazione avanzata in cybersecurity (LUISS Guido Carli, Link Campus, UniPegaso, Mercatorum).

Valentina Chabert è dottoressa di ricerca in Diritto Internazionale presso Sapienza Università di Roma e analista di politica internazionale per numerose riviste, think tank e centri di ricerca nazionali ed internazionali. È cultrice della materia in Sicurezza e Studi Strategici presso l’Università LUMSA e in Relazioni Internazionali e Global Governance presso l’Università degli Studi Internazionali di Roma (UNINT). Ha svolto reportage in Ucraina, Caucaso Meridionale e Balcani e condotto attività di ricerca presso l’International Institute for the Unification of

Private Law (UNIDROIT), il Consiglio d'Europa, il Center of Analysis of International Relations di Baku e presso le università di Ginevra e Aix-en-Provence. È membro dell'Advisory Board del The Hague Research Institute for Eastern Europe, the South Caucasus and Central Asia.

Geopolitica·info

CENTRO STUDI