GOVTECH

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

A cura di *Alessandro Savini*

21 MAGGIO 2026

Questo brief analizza il posizionamento dell'Italia nella competizione tecnologica internazionale, esaminando in chiave integrata la cyber diplomacy e la governance dell'intelligenza artificiale. Il documento ricostruisce l'architettura cyber italiana e il ruolo dell'ACN nei consessi multilaterali, approfondendo il significato strategico della riforma del MAECI con la nuova Direzione Generale per le questioni cibernetiche. Sul versante dell'IA, esamina la strategia nazionale, le priorità di investimento e il coinvolgimento di ricerca e imprese.

GovTech – Geopolitical Brief n. 61/maggio 2026

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

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

ISSN : 3103-3407

INDICE

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[1]. 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

[1] 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[2]. 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[3]. 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[4]. 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[5]. 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

[2] 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/

[3] 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

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

[5] 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*[6].

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)[7]. 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

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

[7] 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[8]. 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[9]. A partire dall'adozione della Strategia Nazionale di Cybersicurezza 2022-2026[10] — articolata in 82 misure operative finanziate da un fondo dedicato istituito con la Legge di Bilancio 2023[11] — l'ACN ha progressivamente consolidato un profilo che

[8] 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.

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

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

[11] 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,

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[12]. 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[13]. 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[14].

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

[12]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.

[13]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

[14]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[15]. 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[16]. Tale orientamento si fonda sul *Position Paper* sul Diritto Internazionale e il Cyberspazio del 2021[17], 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

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

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

[17] 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[18]. 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*

[18] 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[19]. 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

[19] 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[20]. 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[21]. 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[22]. 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

[20] 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/

[21] 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

[22] 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[23].

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[24]. 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

[23] 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/

[24] 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[25]. 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

[25] 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[26]. 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».

[26]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»[27]. 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[28]. 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

[27]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/

[28]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[29]. 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[30]. 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

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

[30] 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[31]. 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

[31] 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)[32]. 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[33]. 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)[34]. 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

[32]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.

[34] 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 [35] . 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 [36] . 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

[35] 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/

[36] 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[37].

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[38]. 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

[37] 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

[38] 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[39]. 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[40]. 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

[39] 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/

[40] 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 [41]. 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*

[41] 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 [42] — 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

[42] 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 [43]. Una seconda direttrice attiene

[43] 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/;

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*[44]. 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.

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/. Per il caso specifico della Danimarca, si veda: https://um.dk/techamb/en/

[44] 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

BIOGRAFIA DELL'AUTORE

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.*

Geopolitica.info

CENTRO STUDI

Il Centro Studi

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

I Report del Centro Studi

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

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info