GOVTECH

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

A cura di *Pierluigi Paganini*

11 MAGGIO 2026

Lo studio analizza il ruolo crescente del cyberspazio e dell'intelligenza artificiale nelle strategie di sicurezza di NATO e UE, evidenziandone la natura di pilastri strutturali negli equilibri di potere contemporanei. Esso mette in luce come, a fronte di obiettivi condivisi, i due attori adottino approcci distinti ma complementari: da un lato, la NATO orientata all'impiego operativo e alla deterrenza nei contesti multidominio; dall'altro, l'UE focalizzata su regolazione, resilienza e tutela del mercato digitale e dei diritti fondamentali.

Geopolitical Brief n. 59/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

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

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

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

il rischio di escalation incontrollata, prevenire incidenti e favorire un minimo di prevedibilità strategica in un contesto internazionale sempre più instabile.

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

[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

interoperabilità e vincoli UE in materia di dati, sicurezza e responsabilità[34].

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

[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/

[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/

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 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

[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/

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 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

[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

trasporti, spaziale e industriale, promuovendo una più stretta integrazione tra capacità di difesa e protezione civile[40].

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.

[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/

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

BIOGRAFIA DELL'AUTORE

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).

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