POLICY PAPERS

Fondazione CSF

SEMPRE MENO IBRIDE, SEMPRE MENO MINACCE

LA "GUERRA POLITICA" ALL'EUROPA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: DALLA ZONA GRIGIA AL NUOVO MEDIO EVO TECNOLOGICO

ARTURO VARVELLI

NOVEMBRE 2026
NUOVA SERIE N. 018

NEXUS
ITALIAN HUB ON HYBRID THREATS

Il presente paper viene presentato nell'ambito del progetto *NEXUS – Italian Hub on Hybrid Threats*, promosso dalla Fondazione CSF in collaborazione con European Council on Foreign Relations (ECFR) e HighGround, al fine di monitorare le minacce ibride che interessano l'Italia e lo sviluppo di risposte in chiave europea. Il progetto nasce con l'obiettivo di articolare un'analisi strutturata e integrata del fenomeno, contribuendo a rafforzare la capacità di risposta del Sistema-Paese; esso si fonda su un approccio *crossdomain* e sulla collaborazione tra attori pubblici, mondo della ricerca e settore privato. Le attività di NEXUS si concentrano su aree chiave quali la manipolazione dell'informazione, le minacce *cyber* e tecnologiche, la sicurezza economica e la resilienza delle infrastrutture critiche.

Autore



Arturo Varvelli

European Council on Foreign Relations (ECFR)
Head of Office and Senior Policy Fellow - Rome

Abstract

Nel discorso sullo stato dell'Unione del 16 settembre 2026, la Presidente della Commissione europea Ursula von der Leyen ha usato una formula destinata a restare: le minacce ibride che l'Europa affronta sono «sempre meno ibride e sempre meno minacce». La frase contiene due affermazioni distinte. Dire che sono sempre meno ibride significa che hanno perso la loro ambiguità: sabotaggi, incendi dolosi, ordigni, incursioni di droni nello spazio aereo dell'Alleanza. Dire che sono sempre meno minacce significa che non descrivono più un rischio potenziale, ma atti che si compiono quotidianamente contro infrastrutture, istituzioni e processi democratici europei.

Da qui conviene partire. Per due decenni il concetto di minaccia ibrida ha offerto una chiave di lettura utile, ma ha anche prodotto un effetto collaterale: ha abituato i governi a collocare questi atti in una zona grigia tra pace e guerra, nella quale le regole ordinarie sembrano sospese e nessuno è davvero tenuto a reagire. L'eccezione mutuata dagli studi strategici di "guerra ibrida" e talvolta utilizzata indiscriminatamente al posto di "minaccia" ha contribuito al contempo a rendere "accettabile" che si parli di guerra e che quella zona grigia creata sia oggi più funzionale a chi la subisce, perché vi trova un alibi per l'inazione. [...]

Parole chiave: Guerra politica, Minaccia Ibrida, Minacce sotto-soglia, Disinformazione, Intelligenza artificiale, Sovranità tecnologica, Deterrenza

Nel discorso sullo stato dell'Unione del 16 settembre 2026, la Presidente della Commissione europea Ursula von der Leyen ha usato una formula destinata a restare: le minacce ibride che l'Europa affronta sono «sempre meno ibride e sempre meno minacce» (Commissione europea 2026). La frase contiene due affermazioni distinte. Dire che sono sempre meno ibride significa che hanno perso la loro ambiguità: sabotaggi, incendi dolosi, ordigni, incursioni di droni nello spazio aereo dell'Alleanza. Dire che sono sempre meno minacce significa che non descrivono più un rischio potenziale, ma atti che si compiono quotidianamente contro infrastrutture, istituzioni e processi democratici europei.

Da qui conviene partire. Per due decenni il concetto di minaccia ibrida ha offerto una chiave di lettura utile, ma ha anche prodotto un effetto collaterale: ha abituato i governi a collocare questi atti in una zona grigia tra pace e guerra, nella quale le regole ordinarie sembrano sospese e nessuno è davvero tenuto a reagire. L'eccezione mutuata dagli studi strategici di *guerra ibrida* e talvolta utilizzata indiscriminatamente al posto di *minaccia* ha contribuito al contempo a rendere *accettabile* che si parli di guerra e che quella zona grigia creata sia oggi più funzionale a chi la subisce, perché vi trova un alibi per l'inazione.

La minaccia sotto-soglia / La soglia che si sposta

Il primo nodo è la definizione del limite. Quando un'operazione si traduce nel sabotaggio di un cavo sottomarino, in un ordigno su un'infrastruttura energetica o in un drone che viola lo spazio aereo di un Paese NATO o Ue, non si è più nel campo dell'ambiguità ma in quello del conflitto aperto. La mancata rivendicazione o l'impiego di intermediari non mutano la natura dell'atto: incidono soltanto sulla capacità di attribuirlo e sulla disponibilità politica a trarne le conseguenze. L'ambiguità, in altre parole, non è un residuo accidentale ma uno strumento deliberato.

I dati disponibili più solidi (con attribuzioni più chiare ed evidenti), seppure non possano essere attuali, descrivono in ogni caso una traiettoria di escalation. Secondo l'International Institute for Strategic Studies (IISS) (Edwards, Seidenstein 2025), i sabotaggi russi confermati contro infrastrutture critiche europee sono aumentati del 246% tra il 2023 e il 2024. Il dato più recente, tuttavia, segnala soprattutto un cambiamento qualitativo: tra settembre 2025 e gennaio 2026 sono state registrate trenta violazioni sospette dello spazio aereo NATO da parte di droni o velivoli verosimilmente russi, a fronte delle ventitré censite nei tre anni e mezzo precedenti (Cederbaum 2026). Nella sola

Germania, nel 2025, le autorità hanno registrato 320 sospetti tentativi (Rekawek, Lanches 2026) di sabotaggio, con un tasso di attribuzione che resta basso. L'escalation, dunque, non riguarda solo il numero degli episodi: consiste nello spostamento verso soglie più alte e più visibili, che misurano di volta in volta la reazione dell'avversario.

Il calcolo di Mosca è leggibile. La Russia confida che le democrazie occidentali restino al di sotto della soglia di una risposta forte e visibile, e fa leva sul timore dei governi di doversi dichiarare «in guerra». Come osserva il Center for Strategic and International Studies, i leader occidentali sono riluttanti a prospettare risposte più incisive per paura di un'escalation incontrollata, e una parte del dibattito continua a sostenere che l'Occidente non sia in guerra con la Russia (Jones Seth G. 2025). Ogni soglia superata senza conseguenze diventa così il punto di partenza della successiva, e il danno tollerato cresce di conseguenza.

Il problema è anche strutturale. L'Europa non dispone ancora di una deterrenza ibrida credibile, né di soglie condivise oltre le quali imporre costi significativi al di sotto dell'Articolo 5 (Beznosiuk 2026; NATO 2026). La responsabilità primaria della risposta continua a gravare sul singolo Stato colpito, il che sposta l'onere dell'attribuzione e della reazione proprio sugli attori più esposti. La proposta, avanzata nello stesso discorso sullo stato dell'Unione, di un protocollo europeo di sicurezza modellato sull'Articolo 4 della NATO, da attivare su richiesta di uno Stato colpito da un incidente che non equivale a un attacco armato ma minaccia la sicurezza nazionale, va letta come un primo tentativo di colmare questo vuoto (Piccioli 2026).

Russia: un bersaglio politico

Mosca resta evidentemente la prima minaccia. La campagna russa di sabotaggio e sovversione in Europa, guidata dall'intelligence militare (GRU), affianca la guerra convenzionale in Ucraina e la retorica nucleare (Jones 2025b).
Le ragioni della sua intensificazione sono in parte materiali: a fronte di perdite stimate nell'ordine di 1,2 milioni di uomini nel conflitto in Ucraina, gli strumenti sotto-soglia offrono a Mosca effetti politici (Beznosiuk 2026; Olech, Wojciechowska 2026) a costi contenuti e con un elevato grado di negabilità. Vi si aggiunge un obiettivo strategico ulteriore: rallentare il riarmo europeo senza ricorrere a un'escalation militare diretta.
Il danno fisico, tuttavia, è il mezzo e non il

fine. Il vero bersaglio è la tenuta democratica, la credibilità delle istituzioni, la coesione sociale. Von der Leyen lo aveva già descritto nell'ottobre 2025 come una campagna «coerente e crescente» volta a inquietare i cittadini, mettere alla prova la determinazione europea, dividere l'Unione e indebolire il sostegno all'Ucraina (USA Congress 2026). L'IISS rileva che l'effetto cumulativo degli attacchi contro obiettivi fisici, digitali e informativi è stato proprio quello di minare la resilienza occidentale e accentuare le fratture interne alle società europee (Edwards, Seidenstein 2025).

E in questa prospettiva che Jonathan Guiffard e Kevin Limonier (2026) hanno proposto, sulle pagine del *Grand Continent*, di sostituire la nozione di *guerra ibrida* con quella di *guerra politica*.

La differenza non è terminologica: gli avversari dell'Europa non si limiterebbero a destabilizzare Stati e amministrazioni, ma mirerebbero a sovvertire i sistemi politici e i valori su cui si fondano. Secondo gli autori, Mosca ha rilanciato questa forma di conflitto a partire dal 2011-2012, quando le proteste di piazza contro il terzo mandato di Putin furono percepite dal Cremlino come una minaccia esistenziale, e da allora sostiene con continuità movimenti sovranisti di diverso orientamento.

Cina: la minaccia strutturale

Se l'obiettivo russo è indebolire e dividere, quello cinese è di natura diversa: plasmare un ordine e costruire dipendenze di lungo periodo. La dottrina delle «Tre guerre» (dell'opinione pubblica psicologica e legale) è parte integrante della strategia militare di Pechino (Gershaneck, Chan 2025). Il suo metodo informativo merita attenzione, perché segna uno scarto rispetto alla propaganda tradizionale: l'obiettivo non è necessariamente persuadere, ma saturare lo spazio digitale con contenuti statali amplificati da reti automatizzate e da algoritmi, fino a rendere indistinguibile il segnale dal rumore. L'intelligenza artificiale rafforza questa capacità. Uno studio dell'Hybrid CoE (Hanhijärvi 2026) documenta come l'avanzato ecosistema IA cinese consenta ad attori legati allo Stato di produrre contenuti su misura, monitorare su larga scala e raggiungere pubblici stranieri selezionati. A questa dimensione si affiancano il ricorso al *lawfare* e a entità formalmente civili nel dominio marittimo, con implicazioni dirette per la sicurezza di cavi e infrastrutture sottomarine, e un'offensiva diplomatica sulla governance globale dell'IA, condotta in una fase in cui norme e standard sono ancora in via di definizione (Song-Pehamberger, Klein 2026; Wong, Fedasiuk 2026). La minaccia cinese, in sintesi, si manifesta meno come attacco

e più come infrastruttura, standard e dipendenza.

Stati Uniti: un alleato e un'incognita

Gli Stati Uniti restano un alleato dell'Italia e dell'Europa, e non possono essere collocati sullo stesso piano di Russia e Cina. Sarebbe tuttavia un errore ignorare le divergenze di interesse che attraversano oggi il rapporto transatlantico e che hanno effetti concreti sulla sicurezza informativa europea.
Un episodio recente lo illustra. All'inizio di ottobre 2026 l'Unione europea, il Canada e la Lituania si sono ritirati da una conferenza sulla disinformazione in seguito a pressioni statunitensi: secondo quanto riportato da *Politico* (Gkrits., Toosi and Detsch 2026), il Dipartimento di Stato aveva chiesto alle proprie ambasciate di esprimere le preoccupazioni di Washington e di «valutare» se i governi coinvolti condividessero la qualificazione degli Stati Uniti come attore di manipolazione dell'informazione. Si tratta di una pressione di natura diplomatica, del tutto diversa da quella russa o cinese, ma il suo effetto sull'autonomia europea di analisi e di contrasto non è trascurabile.
Vi è poi un livello strutturale. Una quota rilevante dell'infrastruttura digitale europea, dal cloud alle piattaforme, dai modelli ai satelliti, è di matrice statunitense, ma non è una novità.

La Brookings Institution, uno dei maggiori think tank mondiali (e americani) segnala il rischio che questa dipendenza esponga l'Europa a interruzioni o modifiche improvvise determinate dalle dinamiche politiche interne americane (Tanner, Wyckoff 2025). La conclusione non è un'accusa: mantenere l'alleanza non equivale a delegare la propria autonomia di giudizio e di decisione, ma il rischio in un'epoca di polarizzazione politica esiste.

L'intelligenza artificiale come moltiplicatore

L'IA non genera minacce inedite: agisce come moltiplicatore lungo quattro dimensioni. Riduce i costi di operazioni che un tempo richiedevano apparati, competenze linguistiche e tempi lunghi. Ne amplia la *scala*, consentendo messaggi differenziati per pubblici specifici. Ne accelera la *velocità*, comprimendo a pochi minuti il ciclo tra un evento e la sua rappresentazione manipolata, con la conseguenza che la verifica arriva strutturalmente in ritardo. E complica l'*attribuzione*, rendendo più difficile, oltre che individuare l'autore, anche giustificare politicamente una risposta. Già Thiele (2020) su Hybrid CoE, indicava l'IA come fattore abilitante chiave della guerra ibrida.

Questi effetti si concentrano su tre fronti: la manipolazione dell'informazione, i *deepfake* e le operazioni di influenza, per i

quali NATO e UE sono chiamate ad aggiornare dottrine e capacità di rilevamento (Mazzucchi 2022), e il dominio cyber, dove crescono insieme la capacità distruttiva e le interdipendenze tra infrastrutture (Hybrid CoE Expert Pool Meeting on Cyber 2021; Sulmeyer 2026). Il caso degli attacchi ucraini contro i data center di Yandex, tra l'8 e l'11 ottobre 2026, offre un esempio istruttivo, anche se in senso opposto a quello che è circolato. Gli attacchi hanno prodotto un calo reale del traffico automatizzato proveniente dalla rete Yandex, ma la narrazione secondo cui avrebbero silenziato i bot filo-russi e populisti attivi in Europa non ha trovato riscontro: il dato misurava soprattutto traffico tecnico, l'attività automatizzata complessiva di origine russa è rimasta stabile e il grafico virale sull'attività attorno all'AfD è stato smentito dalle verifiche indipendenti (Vakulina 2026; Gilbert 2026; Irvine-Brown, Sardarizadeh, Durbiny 2026). L'episodio mostra con quanta facilità un dato tecnico grezzo possa trasformarsi in una narrazione politica, a prescindere dalle intenzioni di chi la diffonde.

Una gerarchia medievale tecnologica: regni, vassalli e servi

Se l'IA è il principale strumento di produzione delle narrazioni, il controllo dell'IA diventa una questione di sovranità. Stati Uniti e Cina stanno separando i ecosistemi tecnologici: fino al 2024 era ancora possibile combinare componenti di entrambi, oggi lo spazio di scelta si è ristretto (Lang N. et al. 2026). I vantaggi comparati sono asimmetrici, con la leadership americana nei semiconduttori avanzati, nei data center e nei modelli di frontiera, e quella cinese nell'adattamento applicativo, nella manifattura hardwaree nei modelli *open-weight* (Omorogieva 2026). I blocchi si stanno di fatto già formalizzando: l'iniziativa statunitense *Pax Silica* è passata da 11 a 24 firmatari, mentre la *WAICO* promossa da Pechino è nata nel luglio 2026 con 29 membri fondatori. Dall'agosto 2026, inoltre, Washington ha iniziato a chiedere ai partner di «scegliere da che parte stare» (Collins and Mehta 2026).

Ne emerge una gerarchia in formazione. Al vertice si collocano i *Paesi proprietari* o i *regni*, che controllano l'intera filiera e definiscono regole e standard. Al livello intermedio si trovano le *potenze medie, i vassalli*, dotate di leve specifiche, di capacità *dual use* e di alleanze, talvolta di *chokepoint* che secondo Bego (2026) potrebbero rendere la competizione meno rigidamente bipolare. Alla base si collocano gli *altri paesi, subordinati o servi* – per restare nella metafora medievale – che utilizzano tecnologie altrui e ne subiscono regole, flussi di dati e possibili interruzioni. Chi non controlla l'infrastruttura tecnologica non controlla neppure l'ecosistema informativo dei propri cittadini, e risulta perciò esposto in modo strutturale alle narrazioni altrui.

Nel XXI secolo la sovranità può essere perduta senza alcuna invasione, semplicemente affidando ad altri l'infrastruttura attraverso cui si forma raggiungerà i leader sui modelli di frontiera (Benner, Hensing 2026). Non è tuttavia preclusa la conquista di margini significativi di autonomia attraverso la cooperazione tra potenze medie. L'ipotesi di un *terzo stack* (Tanner, Wyckoff 2025), l'integrazione da 20 miliardi di dollari tra la canadese *Cohere* e la tedesca *Aleph Alpha* (Lang *et al.* 2026) e la proposta di *Cloud and AI Development Act*, che qualifica come rischio l'eccessiva dipendenza da fornitori cloud extraeuropei (Marks 2026), o i relativi ma rapidi miglioramenti della AI francese *Mistral*, indicano che questa strada è già in parte percorribile.

Dalla reazione all'iniziativa

Tre conclusioni emergono da questo quadro.

- La prima è che la minaccia ha più fonti, con caratteristiche diverse: la Russia persegue l'indebolimento e la divisione dell'Europa; la Cina punta a plasmare un ordine e a creare dipendenze; con gli Stati Uniti esistono divergenze reali, da gestire con lucidità e senza rotture, ma con la consapevolezza di una forte dipendenza. Assimilare questi attori sarebbe un errore analitico; concentrarsi su uno solo, un errore strategico.
- La seconda è che l'Europa non può limitarsi a una postura reattiva. Le democrazie non sono sempre state passive nella competizione delle idee: Radio Londra, i volantini lanciati oltre le linee nemiche e, durante la Guerra fredda, Radio Free Europe e Radio Liberty ne sono la testimonianza. Gli strumenti europei attuali, dal quadro FIMI ai piani contro la disinformazione, restano in larga misura difensivi (Csernatoni and Wanless 2026). Una capacità di iniziativa potrebbe articolarsi su tre piani: una deterrenza credibile, fondata su soglie chiare e costi certi; capacità cyber attive sotto la soglia del conflitto, come richiesto dallo stesso Parlamento europeo (2026); e una narrativa europea propria, rivolta anche ai pubblici russo, cinese e del Sud globale. Questa iniziativa incontra però un limite invalicabile: deve restare trasparente e veritiera. Adottare i metodi dell'avversario significherebbe dissipare l'unico vantaggio strutturale delle democrazie, la credibilità.
- La terza conclusione è che sovranità tecnologica e sovranità democratica coincidono sempre di più. Senza leve proprie sulle infrastrutture di calcolo e di comunicazione, l'Europa rischia di passare dalla condizione di attore a quella di vassallo. La posta in gioco non è soltanto chi vincerà la corsa all'intelligenza artificiale, ma se l'Europa saprà difendersi senza rinunciare a ciò che la rende una democrazia.

References

Bego K. (2026), How a surge in defence and dual-use technology investment could reconfigure the global AI race, Chatham House, DOI: 10.55317/9781784136819

Benner T. , Hensing J. (2026), Europe Will Never Be an AI Superpower, Foreign Policy, https://foreignpolicy.com/2026/06/29/europe-ai-superpower-eurostack-anthopic-mistral-openai/ (Ultimo accesso 30/10/2026)

Beznosiuk M. (2026), How Russia's Hybrid Warfare Will Escalate in 2026 and What Europe Must Do, GLOBSEC, https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do (Ultimo accesso 30/10/2026)

Cederbaum C. (2026), Russia Escalating Hybrid Attacks Across Europe, Recorded Future. https://www.recordedfuture.com/blog/russia-new-generation-warfare (Ultimo accesso 30/10/2026)

Collins C. and Mehta A. (2026), The State of AI Global Governance and Its Implications for the U.S.-China Summit, Center for Strategic and International Studies, https://www.csis.org/analysis/state-ai-global-governance-and-its-implications-us-china-summit (Ultimo accesso 30/10/2026)

Commissione europea (2026), Discorso sullo stato dell'Unione, Bruxelles: Commissione Europea.
https://commission.europa.eu/strategy-and-policy/state-union_it (Ultimo accesso 30/10/2026)

Csernatoni R. and Wanless A. (2026), Assessing Information Ecosystems: How Governments Can Get Ahead of Hybrid Threats, Carnegie Europe, https://carnegieendowment.org/europe/research/2026/07/assessing-information-ecosystems-how-governments-can-get-ahead-of-hybrid-threats (Ultimo accesso 30/10/2026)

Edwards C., Seidenstein N. (2025), The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure, London: The International Institute for Strategic Studies. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/ (Ultimo accesso 30/10/2026)

Gershaneck K.K., Chan E. (2025), Political Warfare against Intervention Forces, Air University, https://www.airuniversity.af.edu/JIPA/Display/Article/4167178/political-warfare-against-intervention-forces/ (Ultimo accesso 30/10/2026)

Gilbert M. (2026), Fact check: Viral graph suggests drop in alleged Russian bot activity, DW Fact check, https://www.dw.com/en/fact-check-misleading-graph-about-alleged-russian-bot-activity/a-79651769 (Ultimo accesso 30/10/2026)

Gkritsi E., Toosi N. and Detsch J. (2026), EU, Canada and Lithuania pull out of disinformation conference after US pressure, Politico, https://www.politico.com/news/2026/10/07/disinformation-conference-europe-us-pressure-01111134 (Ultimo accesso 30/10/2026)

Guiffard J., Limonier K. (2026), L'ere de la guerre politique, Le Grand Continent, https://legrandcontinent.eu/fr/2026/10/06/lere-de-la-guerre-politique/ (Ultimo accesso 30/10/2026)

Hanhijärvi H. (2026), Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian approaches, Hybrid CoE, https://www.hybridcoe.fi/publications/artificial-intelligence-and-foreign-information-manipulation-chinese-and-russian-approaches/ (Ultimo accesso 30/10/2026)

Hybrid CoE Expert Pool Meeting on Cyber (2021), The future of cyberspace and hybrid threats, Trend Report 6, Hybrid CoE, https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-6-the-future-of-cyberspace-and-hybrid-threats/ (Ultimo accesso 30/10/2026)

Irvine-Brown R., Sardarizadeh S. and Durbin A.(2026), Is Zelensky right to say data centre strikes have taken down Russian bots?, BBC Verify, https://www.bbc.com/news/articles/c9y7l0pm8jkko (Ultimo accesso 30/10/2026)

Jones Seth G. (2025), Russia's Shadow War Against the West, Center for Strategic and International Studies, https://www.csis.org/analysis/russias-shadow-war-against-west (Ultimo accesso 30/10/2026)

Jones Seth G. (2025b), Deterrence on NATO's Eastern Flank, Center for Strategic and International Studies,https://www.csis.org/analysis/deterrence-natos-eastern-flank (Ultimo accesso 30/10/2026)

Lang N. et al. (2026), The Great Divide: How the US and China Are Splitting the AI World, Boston Consulting Group, https://www.bcg.com/publications/2026/us-and-china-ai-strategy-causing-global-ai-divide (Ultimo accesso 30/10/2026)

Marks J. (2026), America’s Middle Power AI Export Challenge, Stimson Center, https://www.stimson.org/2026/americas-middle-power-ai-export-challenge/ (Ultimo accesso 30/10/2026)

Mazzucchi N. (2022), AI-based technologies in hybrid conflict, Paper 14, Hybrid CoE, https://www.hybridcoe.fi/publications/hybrid-coe-paper-14-ai-based-technologies-in-hybrid-conflict-the-future-of-influence-operations/ (Ultimo accesso 30/10/2026)

NATO (2026), Countering hybrid threats, NATO, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Ultimo accesso 30/10/2026)

Olech A. , Wojciechowska A. (2026), How Europe must respond to Russian hybrid attacks, Defence24, https://defence24.com/defence-policy/how-europe-must-respond-to-russian-hybrid-attacks (Ultimo accesso 30/10/2026)

Omorogieva E. (2026), Tech Stack Diplomacy: Policy Implications of the U.S. AI Export Strategy, New Lines Institute, https://newlinesinstitute.org/tech-econ-sov-sec/tech-stack-diplomacy-policy/(Ultimo accesso 30/10/2026)

Parlamento europeo (2026), Hybrid warfare and the protection of the EU's territorial integrity and critical security and defence infrastructure, Parlamento europeo, https://oeil.europarl.europa.eu/oeil/en/document-summary?id=1915263 (Ultimo accesso 30/10/2026)

Piccioli L. (2026), L'Europa cerca uno scudo contro la guerra ibrida, Formiche, https://formiche.net/2026/09/leuropa-cerca-uno-scudo-contro-la-guerra-ibrida-ecco-il-piano-di-von-der-leyen/ (Ultimo accesso 30/10/2026)

Rekawek K., Lanches J.(2026), Update of Russia's Crime-Terror Nexus, GLOBSEC, https://www.globsec.org/publication/update-russia-crime-terror-nexus-hybrid-warfare-europe (Ultimo accesso 30/10/2026)

Song-Pehamberger D., Klein S. (2026), China's maritime hybrid warfare, Hybrid CoE, Paper 31, https://www.hybridcoe.fi/publications/hybrid-coe-paper-31-chinas-maritime-hybrid-warfare-how-beijing-uses-lawfare-and-civilian-entities-to-amplify-military-power/ (Ultimo accesso 30/10/2026)

Sulmeyer M. (2026), Artificial Intelligence and the Risk of Strategic Cyberattack, RAND Corporation, https://www.rand.org/pubs/perspectives/PEA4901-1.html (Ultimo accesso 30/10/2026)

Tanner B. , Wyckoff A.W. (2025), Making the case for a third AI technology stack, Brookings Institution, https://www.brookings.edu/articles/making-the-case-for-a-third-ai-technology-stack/ (Ultimo accesso 30/10/2026)

Thiele R. (2020), Artificial Intelligence : A Key Enabler of Hybrid Warfare, Working Paper 6, Hybrid CoE, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-6-artificial-intelligence-a-key-enabler-of-hybrid-warfare/ (Ultimo accesso 30/10/2026)

USA Congress (2026), Russian Hybrid Warfare Activities in Europe: Considerations for Congress, https://www.congress.gov/crs-product/R49134 (Ultimo accesso 30/10/2026)

Vakulina S. (2026),Attacchi ucraini ai data center Yandex: crolla l'attività dei bot russi?, Euronews, https://it.euronews.com/2026/10/12/attacchi-ucraini-ai-data-center-yandex-crolla-lattivita-dei-bot-russi (Ultimo accesso 30/10/2026)

Wong A., Fedasiuk R. (2026), China's AI Governance Offensive Threatens US Tech Leadership, American Enterprise Institute, https://www.aei.org/commentary/chinas-ai-governance-offensive-threatens-u-s-tech-leadership/ (Ultimo accesso 30/10/2026)

POLICY PAPERS

Fondazione CSF

Fondazione CSF
Piazza Arbarello, 8 - 10122 Torino- Italia
Via dei Montecatini, 17 - 00186 Roma - Italia
Rue de la Loi 155 - 1040 Bruxelles - Belgio
www.fondazionecsf.it