GOVTECH

Cyberspazio conteso: attori, conflitti e vulnerabilità

A cura di *Alessandra Russo*

11 MAGGIO 2026

Questo studio analizza il cyberspazio come un dominio strutturalmente conflittuale e sempre più frammentato, in cui la moltiplicazione degli attori — statali e non statali — e l'asimmetria intrinseca favoriscono operazioni a basso costo e ad alto impatto. Il lavoro evidenzia come le campagne cibernetiche contemporanee non si limitino a singoli attacchi, ma si configurino come attività prolungate di spionaggio, sabotaggio e influenza, integrate nelle dinamiche della competizione geopolitica e della guerra ibrida.

Geopolitical Brief n. 58/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 conteso: attori, conflitti e vulnerabilità

Alessandra Russo

Introduzione

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

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

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

Diversificazione di attori e minacce nel cyberspazio

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

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

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

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

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

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

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

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

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

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

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

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

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

[10] ENISA, Threat Landscape 2025.

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

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

Asimmetria e vulnerabilità

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vulnerabilità sistemiche e implicazioni per l'Italia

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Riferimenti bibliografici

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ministero degli Affari Esteri e della Cooperazione Internazionale. (2026). *Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica – Ministero degli Affari Esteri e della Cooperazione Internazionale*. https://www.esteri.it/it/ministero/struttura/dgct/

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

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

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

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

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

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

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

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

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

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

BIOGRAFIA DELL'AUTRICE

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

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