

Geopolitica e cybersecurity: analisi degli ultimi accadimenti nel panorama internazionale 2025



Il panorama geopolitico del 2025 ha evidenziato un'interconnessione senza precedenti tra tensioni internazionali e minacce cibernetiche, configurando un nuovo paradigma di conflittualità ibrida. L'analisi degli eventi recenti dimostra come gli attacchi informatici nation-state abbiano raggiunto livelli di sofisticatezza e coordinamento mai osservati in precedenza, con implicazioni critiche per infrastrutture strategiche, catene di approvvigionamento e sicurezza nazionale. Il presente studio esamina la convergenza tra geopolitica e cybersecurity attraverso l'analisi dei trend emergenti, degli incidenti più significativi e delle strategie di mitigazione adottate dalle organizzazioni leader nel settore.

Geopolitica e cybersecurity: il nuovo paradigma di conflittualità ibrida

La cybersecurity contemporanea ha subito una metamorfosi sostanziale, evolvendosi da disciplina tecnica specialistica a dominio strategico di rilevanza geopolitica primaria. Il World Economic Forum's Global Cybersecurity Outlook 2025 identifica questa trasformazione come il risultato di tre fattori convergenti: l'escalation delle tensioni geopolitiche globali, l'adozione accelerata di tecnologie emergenti e l'incremento della dipendenza da supply chain interconnesse e complesse.

La complessità del cyberspace attuale riflette un ecosistema in cui le tradizionali demarcazioni tra conflitto statale e criminalità informatica si sono progressivamente dissolte, generando un ambiente operativo caratterizzato da incertezza strategica e vulnerabilità sistemiche. Questa nuova realtà richiede una riconfigurazione delle strategie difensive e un approccio olistico alla cyber resilience.

Le principali minacce nation-state nel 2025

Attività cibernetiche sino-americane

L'intelligence statunitense ha documentato un incremento del 150% delle operazioni di cyber-espionage cinesi nel corso del 2024, con particolare focus sui settori finanziario, manifatturiero e dei media. Gli attacchi targeting Taiwan hanno evidenziato un pattern di escalation, con 2,4 milioni di tentativi di intrusione giornalieri nel 2024, rappresentando un raddoppio rispetto al 2023.

Le campagne attribuite ai gruppi APT cinesi, inclusi Volt Typhoon e UAT-5918, hanno dimostrato una preferenza strategica per l'infiltrazione di infrastrutture critiche piuttosto che per operazioni disruptive immediate, suggerendo una pianificazione a lungo termine finalizzata al posizionamento pre-conflitto all'interno di sistemi strategici occidentali.

Operazioni russe multi-vettore

La Federazione Russa ha intensificato le proprie capabilities offensive attraverso l'unità 26165 del GRU (nota come "Fancy Bear"), condotto campagne persistenti contro entità logistiche occidentali e organizzazioni tecnologiche coinvolte nel supporto all'Ucraina. L'NSA ha identificato pattern operativi caratterizzati da tattiche ibride che combinano cyber-attacks, disinformazione e operazioni di influence.

Particolarmente significativo risulta l'hijacking dell'infrastruttura pakistana perpetrato da operatori russi nel 2024, evidenziando una strategia di weaponization delle capacità offensive di threat actors terzi per amplificare la surface attack e complicare l'attribution.

Proliferazione nordcoreana e iraniana

La Corea del Nord ha espanso le proprie operazioni di infiltrazione verso organizzazioni europee della difesa e governative, implementando tecniche di remote worker impersonation per ottenere accessi privilegiati e generare revenue attraverso estorsioni post-breach. Parallelamente, gruppi affiliati iraniani hanno intensificato campagne di cyber-espionage contro entità governative irachene e infrastrutture di telecomunicazione yemenite.

Vulnerabilità delle supply chain e rischi sistemici

Complessità e interdipendenza

Il 54% delle organizzazioni enterprise identifica le vulnerabilità delle supply chain come il principale ostacolo al raggiungimento di livelli adeguati di cyber resilience. L'interconnessione crescente degli ecosistemi digitali ha generato punti di failure sistemici con conseguenze cascading sull'intero network di fornitori e partner.

L'incident ConnectWise del maggio 2025, attribuito a threat actors nation-state attraverso lo sfruttamento della vulnerabilità CVE-2025-3935, ha dimostrato come l'exploitation di un singolo vendor possa compromettere simultaneamente centinaia di organizzazioni clienti, amplificando esponenzialmente l'impatto operativo e reputazionale.

Costi economici e proiezioni

Le supply chain attacks hanno registrato un incremento del 200% nel 2023, con proiezioni che stimano un costo globale annuale di 138 miliardi di dollari entro il 2031, in crescita dai 46 miliardi del 2023. Questa escalation riflette l'evoluzione delle methodologies offensive, che privilegiano l'infiltrazione indiretta attraverso fornitori terzi rispetto agli attacchi diretti ai target finali.

Intelligenza artificiale come catalizzatore di complessità

Adozione asimmetrica e risk assessment

Nonostante il 66% delle organizzazioni riconosca l'impatto trasformativo dell'AI sulla cybersecurity nel 2025, solamente il 37% ha implementato framework adeguati per il security assessment degli strumenti AI pre-deployment. Questa discrepanza evidenzia un gap critico tra adoption rate e security readiness, esponendo le organizzazioni a rischi emergenti non sufficientemente caratterizzati.

Il 47% delle organizzazioni identifica l'uso adversarial dell'AI generativa come preoccupazione primaria, con particolare riferimento all'enhancement delle capabilities di social engineering, phishing sofisticato e automated reconnaissance. Gli LLM attuali presentano vulnerabilità costitutive che non sono adeguatamente address nei framework di sicurezza correnti, creando surface attack potenzialmente devastating.

Geopolitica dell'AI e technological sovereignty

La competizione geopolitica nel dominio AI ha generato technological blocs attorno agli Stati Uniti e alla Cina, compromettendo la cooperazione internazionale e limitando l'accesso cross-border alle innovation più avanzate. La

frammentazione regolatoria risultante impedisce lo sviluppo di standard globali uniformi, creando vulnerabilità sistemiche nelle implementazioni multi-jurisdictional.

Impatti sui settori critici

Infrastrutture energetiche e di telecomunicazione

Gli attacchi alle infrastrutture critiche hanno evidenziato la vulnerabilità sistemica dei settori energetico e delle telecomunicazioni, con particular focus su cavi sottomarini e sistemi satellitari. Gli incidenti nel Mar Baltico hanno sottolineato l'urgenza di proteggere gli asset infrastrutture critiche per il data flow globale e gli scambi economici internazionali.

La digitalizzazione del settore energetico ha amplificato l'exposure a cyberattacks capaci di causare damage significativo alle infrastrutture critiche e disruption della supply energetica, costituendo uno dei top geopolitical risks del 2025.

Settore finanziario e bancario

Il settore finanziario ha registrato aumenti significativi negli attacchi targetizzati, con l'India che emerge come seconda nazione più colpita globalmente nel 2024. Il settore finance e banking ha subito 20 vittime documentate, seguito da government (13), telecomunicazioni (12), healthcare e pharma (10).

L'attack a C-Edge Technologies, joint venture tra State Bank of India e Tata Consultancy Services, ha causato disruption nei sistemi di pagamento di circa 300 banche minori indiane, evidenziando la criticità delle interdipendenze sistemiche nel settore financial services.

Strategie di mitigazione e best practices

Framework di cyber resilience

L'implementazione di strategie di cyber resilience richiede un shift paradigmatico dalle tradizionali misure preventive verso approcci capability-based focalizzati sulla business continuity sotto attacco. Questo include lo sviluppo di minimum viable company (MVC) concepts e la modernizzazione delle infrastrutture legacy per garantire rapid recovery post-incident.

Le organizzazioni leader stanno adottando architetture zero-trust estese agli ecosistemi vendor, implementando segmentazione granulare e continuous trust validation across supply chain relationships. La threat intelligence sharing consortia rappresenta un meccanismo emerging per real-time alerting e prevention di large-scale cyber incidents.

Capacity building e workforce development

Il cyber skills gap ha registrato un incremento dell'8% nel 2024, con carenze moderate-to-critical in due terzi delle organizzazioni. Il settore pubblico presenta le deficienze più acute, con il 49% dei respondents che indica insufficienza della workforce per meeting cybersecurity objectives.

L'84,4% delle organizzazioni pianifica investimenti in training e exercising per il 2025, riflettendo la recognition dell'human element come componente critica della cyber resilience. La collaborazione inter-industry per sharing training resources e best practices rappresenta un approccio emergente per collective capability enhancement.

Regulatory frameworks e compliance

La frammentazione regolatoria costituisce un challenge significativo, con il 70% dei survey respondents che

identifica le regulations come eccessivamente complex o convolute. Il 76% dei CISO indica che la confusion regolatoria impatta significativamente la capacity organizzativa di maintaining compliance.

L'harmonization degli standard internazionali e lo sviluppo di frameworks coerenti rappresentano priorities critical per enabling effective cybersecurity governance across jurisdictions multiple.

Conclusioni e prospettive future

L'analisi degli eventi del 2025 conferma l'emergenza di un nuovo paradigma geopolitico in cui le capabilities cyber costituiscono strumenti primari di proiezione del potere statale e di perseguimento degli interessi nazionali. La convergenza tra tensioni geopolitiche e sophisticated cyber threats ha generato un environment operativo caratterizzato da complexity senza precedenti e vulnerability systemiche.

Le organizzazioni devono adottare approcci proactive per building cyber resilience, implementando strategies che transcendano i traditional security perimeters e incorporino considerations geopolitical nel risk assessment e nella strategic planning. La collaboration ecosystem-wide e l'investment in advanced defensive capabilities rappresentano requirements essential per maintaining competitive advantage in un environment increasingly contested.

La quantum computing readiness e l'adoption di post-quantum cryptographic standards costituiranno elementi differenziating per organizational resilience nel prossimo quinquennio, mentre l'AI democratization richiederà framework governance sofisticati per balancing innovation benefits con security imperatives.

Fonti

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025: Navigating complexity.*

<https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/>

Industrial Cyber. (2025, January 14). *WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats.*

<https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/>

PwC. (2025). *Cybersecurity + geopolitical conflict: What boards and CEOs should know.*

<https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cybersecurity-geopolitical-conflict-board-ceo-response.html>

Center for Strategic and International Studies. (2025). *Significant Cyber Incidents.*

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Cybersecurity and Infrastructure Security Agency. (2025). *Nation-State Threats.*

<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>

S&P Global. (2025). *Top Geopolitical Risks of 2025.*

<https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk>

Critical Start. (2023, December 18). *Geopolitical Factors Shaping the Future of the Cyber Domain.*

<https://www.criticalstart.com/geopolitical-factors-shaping-the-future-of-the-cyber-domain/>

Palo Alto Networks. (2025, June 26). *Threat Brief: Escalation of Cyber Risk Related to Iran*.
<https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/>

The Hacker News. (2025, May). *ConnectWise Hit by Cyberattack; Nation-State Actor Suspected*.
<https://thehackernews.com/2025/05/connectwise-hit-by-cyberattack-nation.html>

Business Today. (2025, January 13). *AI, geopolitics, and workforce gaps: WEF Cybersecurity Report 2025*.
<https://www.businesstoday.in/wef-2025/story/ai-geopolitics-and-workforce-gaps-wef-cybersecurity-report-2025-460436-2025-01-13>

Condividi sui Social Network:
<https://www.ictsecuritymagazine.com/articoli/geopolitica-cybersecurity/>