"Cyber intelligence e international security nel 2026”

Gestire il cyber crime per rompere il silenzio normativo e diplomatico sulle operazioni digitali degli Stati. Un analisi strategica sulle operazioni cyber degli Stati, la zona grigia del diritto internazionale e le implicazioni per la sicurezza globale alla luce anche del conflitto USA-Iran.

di
Federica Maria Rita Livelli e Antonio Albanese

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding...”

Traduzione
“*Cyberspazio. Un'allucinazione consensuale vissuta quotidianamente da miliardi di operatori legittimi, in ogni nazione, da bambini a cui vengono insegnati concetti matematici... Una rappresentazione grafica di dati estratti dalle banche di ogni computer del sistema umano. Complessità impensabile. Linee di luce si estendevano nel non-spazio della mente, ammassamenti e costellazioni di dati. Come luci di città, che si allontanano..."*

William Gibson, Neuromancer

Sommario

Executive Summary....3
1. Il conflitto Usa-Iran 2026: il cyber come quinto dominio operativo....3
1.1 Anatomia di un conflitto ibrido....3
1.2 La zona grigia della legittimità: attacchi cyber come atti di guerra?....4
1.3 Implicazioni strategiche: nuovi paradigmi della deterrenza....5
2. Il vacuum normativo internazionale: silenzio legale e diplomatico....5
2.2 La diplomazia del silenzio: perché gli Stati non parlano....6
2.3 Tentativi di governance: Budapest, GGE e i loro limiti....6
3. Modelli di attribuzione e intelligence sharing: le best practice....6
3.1 L'attribuzione come strumento diplomatico....7
3.2 Il framework EU INTCEN e la condivisione strutturata....7
3.3 Il modello estone: legal framework per la risposta statale....7
3.4 Intelligence-led policing: il caso Emotet e la convergenza civile-militare....8
4. Il panorama delle minacce nel 2026: casi e scenari geopolitici....8
4.1 Principali Casi di Cyber Crime Statale (2024-2026)....8
4.2 Scenari geopolitici 2026: il nuovo ordine cyber internazionale....9
5. Framework operativo: ciclo di validazione e cyber intelligence integrata....10
5.1 Il ciclo di intelligence: dall'OSINT alla decisione politica....10
5.2 Best practice per il 2026: priorità operative....11
6. Raccomandazioni strategiche: rompere il silenzio legale e diplomatico....12
6.1 Comunità internazionale e governi....12
6.3 Il ruolo del fattore umano nella cyber intelligence....13
7. Conclusioni: verso un regime internazionale di cyber governance....13
Fonti e Riferimenti....16

Executive Summary

Il contesto di permacrisi e policrisi geopolitiche e geoeconomiche nel 2026 richiede la capacità di analizzare il panorama cyber intelligence e della sicurezza internazionale, con particolare attenzione alla gestione del cyber crime nelle operazioni digitali degli Stati.

Inoltre, mentre l'Europa si confronta con nuove realtà geopolitiche, la necessità di un approccio globale alla sicurezza non è mai stata così pressante. Le dinamiche mutevoli delle alleanze globali e la crescente complessità delle minacce informatiche, soprattutto con l'integrazione dell'intelligenza artificiale nella guerra ibrida, evidenziano una verità fondamentale: la guerra moderna non si basa solo sulla potenza militare.

Pertanto, l'obiettivo è contribuire al superamento del silenzio legale e diplomatico che avvolge le cyber operazioni statali, aprendo un dibattito strutturato su norme, responsabilità e cooperazione internazionale.

È doveroso evidenziare che il 2026 ha segnato un punto di svolta epocale: il conflitto armato tra USA-Israele e Iran (Operation Epic Fury / Operation Roaring Lion, 28 febbraio 2026) ha definitivamente consacrato il cyberspazio come dominio operativo integrale dei conflitti moderni. Le cyber operazioni hanno preceduto, accompagnato e amplificato gli attacchi cinetici, dimostrando l'inseparabilità tra warfare digitale e convenzionale.

Di fatto, come riportato anche dal Rapporto Clusit – marzo 2026, l'anno appena trascorso, è stato un *annus horribilis* con un ulteriore aumento degli attacchi cyber a fronte delle crisi geopolitiche in atto.

1. Il conflitto Usa-Iran 2026: il cyber come quinto dominio operativo

L'intento del white paper è di fornire la cronistoria di cosa è accaduto dall'inizio del conflitto ad ora per meglio comprendere le dinamiche di cyber intelligence e campo di azione.

1.1 Anatomia di un conflitto ibrido

Il 28 febbraio 2026, gli Stati Uniti e Israele hanno lanciato operazioni militari congiunte contro l'Iran - i.e. *Operation Epic Fury (USA)* e *Operation Roaring Lion (Israele)* - segnando l'apice di una escalation pluriennale. Per la prima volta nella storia dei conflitti moderni, le operazioni cyber hanno preceduto deliberatamente gli strike cinetici con l'obiettivo esplicito di lasciare il nemico "*disrupted, disoriented and confused*", nelle parole del Generale Dan Caine, Capo di Stato Maggiore Congiunto delle Forze Armate USA.

Le cyber operazioni si sono articolate su tre livelli simultanei:

1. disruption dei sistemi di comando, controllo e comunicazione iraniani;
1. information operations per alimentare il dissenso interno e destabilizzare il regime;
2. degradazione delle infrastrutture digitali critiche.

Inoltre, la connettività Internet iraniana è crollata all'1-4% dei livelli normali per oltre 60 ore, in quello che alcune fonti israeliane hanno definito "il più grande cyberattacco della storia".

Cronologia delle operazioni cyber nel conflitto USA-Iran (febbraio - aprile 2026)	
28 febbraio 2026	**Coordinate USA-Israele:** *cyber strike pre-kinetic* su reti C2 iraniane; compromissione app BaadeSaba (preghiera) per disinformazione; *takedown* di canali media di Stato.
28 febbraio –1° marzo 2026	**Blackout internet:** connettività Iran al 1-4%; oltre 60 ore di disruption totale.
1- 2 marzo 2026	**Contrattacco hacktivist:** >60 gruppi pro-Iran attivati; gruppo NoName057(16) russo si unisce alle operazioni; attacchi DDoS su sistemi di pagamento israeliani e siti governativi del Kuwait.
11 marzo 2026	**Attacco Stryker:** Handala Hack (MOIS) colpisce l'azienda medicale USA con malware distruttivo; 50TB di dati esfiltrati; 17 giorni di ripristino operativo.
19 marzo 2026	**Risposta DOJ:** il Dipartimento di Giustizia USA smantella 4 pilastri dell'infrastruttura MOIS-Handala; offerta di $10 milioni per informazioni su attori cyber iraniani.
17 aprile 2026	**Parziale ripristino Internet:** l'Iran inizia a ripristinare internet limitato, solo su National Information Network nazionale.

1.2 La zona grigia della legittimità: attacchi cyber come atti di guerra?

Il conflitto USA-Iran 2026 ha sollevato molti interrogativi sull'applicabilità del diritto internazionale al cyberspazio. Di fatto, le operazioni cyber che hanno preceduto e accompagnato le operazioni cinetiche hanno operato in un vacuum normativo: né il diritto dei conflitti armati, né la Carta delle Nazioni Unite offrono una risposta definitiva su quando un'operazione cyber costituisce "uso della forza".

La compromissione dell'app BaadeSaba — una delle app per la preghiera più diffuse in Iran — per inviare messaggi sovversivi a milioni di utenti rappresenta un esempio emblematico di operazione al confine tra spionaggio, *information warfare* e operazione psicologica. Il diritto internazionale classico non fornisce strumenti per categorizzare, e quindi regolamentare, questa tipologia di azione.

Inoltre, l'interruzione della connettività ad internet per 47 giorni — attribuita a una combinazione di strike fisici su data center e cyber disruption — configura un potenziale attacco alle infrastrutture civili, vietato dal diritto umanitario internazionale.

Tuttavia, l'impossibilità di distinguere tra infrastrutture militari e civili nel cyberspazio rende l'applicazione di tali norme estremamente complessa.

Operazioni USA-Israele	Risposta Iran / Pro-Iran
Pre-positioning cyber pre-kinetic	Attivazione rete hacktivist globale
Distruzione C2 iraniani	Malware distruttivo su target USA (Stryker)
Compromissione app civili (BaadeSaba)	DDoS infrastrutture finanziarie regionali

Takeover media di Stato (IRNA - Islamic Republic News Agency)	Data exfiltration e leak operazioni
Accesso telecamere di sicurezza Teheran	Targeting OT/ICS (Rockwell Automation)
Campagne IA anti-regime su social media	Campagne phishing anti-israeliane (APK APK malevolo RedAlert)

1.3 Implicazioni strategiche: nuovi paradigmi della deterrenza

Il conflitto USA-Iran 2026 ha evidenziato come l'Iran — che "manca di opzioni di risposta convenzionali simmetriche" (CSIS - Center for Strategic and International Studies, 2026) — abbia fatto ricorso massivamente al cyberspazio e alle reti di proxy come strumento di deterrenza e ritorsione asimmetrica. Tale dinamica non è nuova, ma raggiunge nel 2026 una scala e sofisticazione senza precedenti.

Il ricorso ai proxy hacktivist — da Handala Hack (MOIS) a gruppi autonomi distribuiti globalmente — introduce una complessità strutturale nella deterrenza cyber: quando le operazioni cyber "Superano l'ambito delle operazioni militari stesse" (CSIS, 2026), i meccanismi classici di escalation e de-escalation perdono efficacia. La “negabilità plausibile”, storicamente un vantaggio strategico, si converte in un fattore di instabilità sistemica.

Un ulteriore elemento di complessità è rappresentato dalla convergenza tra gruppi statali e criminali: il gruppo *CL-STA-1128 (Cyber Av3ngers)*, identificato da Palo Alto Networks Unit 42 nel marzo 2026, ha dimostrato capacità OT (Operational Technology) /ICS (Industrial Control Systems) su sistemi Rockwell Automation, segnalando un innalzamento qualitativo delle minacce iraniane alle infrastrutture industriali occidentali.

2. Il vacuum normativo internazionale: silenzio legale e diplomatico

Per quanto riguarda l’architettura giuridica attuale, è doveroso evidenziarne i limiti.

Di fatto, il diritto internazionale esistente non è stato progettato per il cyberspazio. Tre corpi normativi risultano parzialmente applicabili - i.e. il diritto dei conflitti armati (DIU), il diritto delle relazioni internazionali pacifiche (Carta ONU) e il diritto internazionale penale - ma nessuno copre adeguatamente le operazioni cyber statali nella loro specificità.

Il *Tallinn Manual* (2.0, 2017) rappresenta il tentativo accademico più sistematico di applicare il diritto internazionale esistente al cyberspazio, ma rimane un documento non vincolante, elaborato da esperti indipendenti, con scarso recepimento nella prassi degli Stati.

Inoltre, le divergenze interpretative tra grandi potenze — USA, Russia, Cina — rendono impossibile un consensus su norme minime di comportamento.

Di seguito una tabella contenente le principali lacune del diritto internazionale nel cyberspazio.

Le quattro lacune principali del diritto internazionale nel cyberspazio	
1	**Attribuzione:** assenza di meccanismi internazionali vincolanti per l'attribuzione delle operazioni cyber agli Stati responsabili; la "plausible deniability" strutturale rende elusiva la responsabilità

2	**Soglia dell'uso della forza:** mancanza di definizione condivisa di quando un'operazione cyber costituisce "uso della forza" (Art. 2(4) Carta ONU) o "attacco armato" (Art. 51), che giustifica la legittima difesa
3	**Protezione infrastrutture civili:** le distinzioni del DIU tra obiettivi militari e civili sono di difficile applicazione a infrastrutture duali (internet, sistemi energetici, reti finanziarie)
4	**Spionaggio cyber:** il diritto internazionale non regola tradizionalmente lo spionaggio — neanche quello cyber — creando una zona grigia in cui operazioni SIGINT e offensive si sovrappongono

2.2 La diplomazia del silenzio: perché gli Stati non parlano

È doveroso evidenziare che il "silenzio diplomatico" sulle cyber operazioni statali non è accidentale, bensì strutturale. Gli Stati evitano di codificare norme vincolanti nel cyberspazio per ragioni strategiche convergenti, indipendentemente dalla collocazione geopolitica.

Le grandi potenze – i.e. USA, Russia, Cina e Israele - hanno investito massicciamente in capacità cyber offensive e non intendono limitarle attraverso accordi internazionali. D'altro canto, i paesi in via di sviluppo temono che le norme internazionali vengano usate dalle potenze consolidate per mantenere l'egemonia digitale; mentre, altri player - quali Iran, Corea del Nord, gruppi non statali - utilizzano il vacuum normativo come vantaggio competitivo asimmetrico.

Il conflitto USA-Iran 2026 ha mostrato, ulteriormente, quanto questo silenzio sia pericoloso: senza norme condivise, la *miscommunication* e la *misperception* possono trasformare operazioni cyber di intelligence in atti interpretati come *casus belli*.

Inoltre, la "contaminazione" degli strumenti — dai *wiper* ai *ransomware*, dai *DDoS* alla manipolazione di app civili — rende sempre più difficile distinguere tra *crime, warfare* e spionaggio.

2.3 Tentativi di governance: Budapest, GGE e i loro limiti

La *Convenzione di Budapest sul Cybercrime* (*Budapest Convention on Cybercrime* 2001) rimane il principale strumento internazionale di cooperazione contro il cyber crime, con 68 Stati parte.

Tuttavia, Russia e Cina non l'hanno ratificata e il suo ambito di applicazione esclude esplicitamente le operazioni degli Stati. Il successivo *Protocollo Aggiuntivo* (*Additional Protocol to the Convention on Cybercrime* - 2022), pur migliorando la cooperazione procedurale, non affronta le operazioni statali.

Inoltre, i *Gruppi di Esperti Governativi delle Nazioni Unite* (*United Nations Groups of Governmental Experts (GGE)* - 2010-2021) hanno prodotto rapporti consensuali che riconoscono l'applicabilità del diritto internazionale al cyberspazio e identificano undici norme non vincolanti di comportamento responsabile.

È doveroso informare che, nonostante il processo *OEWG (Open-Ended Working Group)* prosegua, permangono le divisioni tra blocchi occidentale e Russia-Cina limitano i progressi, impedendo di stabilire, ad oggi, un meccanismo di verifica o enforcement.

3. Modelli di attribuzione e intelligence sharing: le best practice

Di seguito una panoramica dei vari modelli di attribuzione e dell'intelligence sharing, unitamente alle relative best practice.

3.1 L'attribuzione come strumento diplomatico

L'attribuzione pubblica delle operazioni cyber è diventata uno strumento politico-diplomatico fondamentale per "rompere il silenzio", trasformando operazioni nella zona grigia in eventi con nome, responsabilità e conseguenze. Il caso *NotPetya* (2017) ha stabilito il precedente, ovvero: una dichiarazione congiunta, coordinata da Stati Uniti, Regno Unito, Nuova Zelanda, Australia e Canada, ha attribuito pubblicamente l'attacco alla Russia, costituendo la prima forma sistematica di deterrenza per normazione.

Segue un esempi di framework di attribuzione multi-livello riferito al modello NotPetya-SolarWinds

Framework di attribuzione multi-livello: il modello NotPetya-SolarWinds	
FASE 1	**Correlazione tecnica:** analisi forense malware, TTP (Tactics, Techniques, Procedures), infrastrutture C2; utilizzo framework MITRE ATT&CK per fingerprinting del threat actor
FASE 2	**Analisi geopolitica:** contestualizzazione degli obiettivi nel quadro delle relazioni internazionali; pattern storici di comportamento del presunto attore statale
FASE 3	**Validazione HUMINT:** conferma attraverso fonti umane dell'origine statale; cruciale per distinzione tra operazione diretta, proxy e false flag
FASE 4	**Intelligence sharing:** condivisione multi-laterale con alleati attraverso canali classificati (Five Eyes, EU INTCEN, NATO CCDCOE) per costruire consenso pre-annuncio
FASE 5	**Dichiarazione pubblica coordinata:** annuncio simultaneo da più capitali per massimizzare impatto diplomatico e minimizzare capacità di smentita

3.2 Il framework EU INTCEN e la condivisione strutturata

Il programma *EU INTCEN* (*European Union Intelligence and Situation Centre*) rappresenta il modello più avanzato di *cyber intelligence sharing* tra democrazie. Attraverso piattaforme standardizzate - quali MISP (*Malware Information Sharing Platform*) e protocolli *STIX (Structured Threat Information eXpression) / TAXII* (*Trusted Automated eXchange of Intelligence Information*) - gli Stati membri condividono IoC (*Indicators of Compromise*) preservando la protezione delle fonti HUMINT attraverso processi di anonimizzazione strategica.

Il modello si articola su livelli di classificazione graduali, permettendo la declassificazione progressiva delle informazioni per massimizzare la protezione collettiva, senza compromettere le fonti sensibili. Inoltre, il ciclo di feedback tra agenzie riceventi e mittenti garantisce l'arricchimento contestuale continuo dell'intelligence condivisa.

Il conflitto USA-Iran ha evidenziato, di fatto, la necessità di estendere questo modello dato che la velocità con cui i 60+ gruppi hacktivist si sono attivati — molti operando da fuori dell'Iran, attraverso Starlink e altri servizi VSAT — ha richiesto un coordinamento intelligence in tempo reale che i meccanismi esistenti faticano a sostenere.

3.3 Il modello estone: legal framework per la risposta statale

Gli attacchi DDoS massivi contro l'Estonia nel 2007 - i.e. il primo caso documentato di cyber aggressione contro uno Stato sovrano - hanno prodotto la risposta più avanzata in termini di framework legale-operativo.
In particolare, l'Estonia ha sviluppato un modello che integra:

- dimensione militare (*Cyber Defense Unit* con mandato chiaro sulle soglie di intervento)
- dimensione civile (partnership pubblico-privato formalizzata)

- dimensione internazionale (*NATO Cooperative Cyber Defence Centre of Excellence -CCDCOE)* come hub per la standardizzazione delle dottrine di risposta.

L'elemento chiave del modello estone è la definizione legale chiara di quando un'azione informatica supera la soglia di "uso della forza" secondo l'Articolo 2(4) della Carta ONU. Tale chiarezza normativa domestica — anche in assenza di un consenso internazionale — permette all'Estonia di rispondere in modo proporzionato e legalmente fondato a operazioni che altri Stati sarebbero costretti a ignorare o “scalare” in modo non calibrato.

3.4 Intelligence-led policing: il caso Emotet e la convergenza civile-militare

L'operazione congiunta Europol per lo smantellamento della *botnet Emotet* (2021) rimane il caso studio più significativo di convergenza tra cyber intelligence, forze dell'ordine e cooperazione internazionale.

Di fatto, la sincronizzazione di 8 giurisdizioni per l'esecuzione simultanea del *takedown* - con neutralizzazione dell'infrastruttura e sostituzione del payload - ha dimostrato la fattibilità operativa della cooperazione *cross-border*.

Ovvero, l’operazione – a livello di lesson learned – ha dimostrato come anche contro cyber crime apparentemente non statale, l'approccio *intelligence-driven* multi-disciplinare è essenziale, poiché gruppi criminali possono essere proxy di Stati.

Inoltre, il confine tra *organized cybercrime* e *state-sponsored operation* è strutturalmente porosa - come confermato dai rapporti tra Hydra (Russia - Hydra Market è stato il più grande e longevo marketplace in lingua russa sul dark web fino alla sua chiusura nell'aprile 2022), Lazarus Group (Corea del Nord.

Il Lazarus Group è un collettivo di hacker sponsorizzato dallo stato nordcoreano, noto anche come APT38, che conduce attività di spionaggio informatico a livello globale e furti finanziari per finanziare il regime. Operativo almeno dal 2009, è noto per l'attacco informatico alla Sony Pictures del 2014, la rapina alla Banca del Bangladesh del 2016 - 81 milioni di dollari - e l'attacco ransomware WannaCry del 2017), e, nel 2026, da Handala Hack (Iran - Il gruppo funge da copertura per Void Manticore - nota anche come Storm-0842 o Banished Kitten, un'unità affiliata al Ministero dell'Intelligence e della Sicurezza iraniano. MOIS.È il gruppo che ha recentemente penetrato l’account e le mail del direttore FBI Kash Patel nel marzo 2026).

4. Il panorama delle minacce nel 2026: casi e scenari geopolitici

Di seguito una panoramica delle minacce e dei principali casi di cyber crime degli ultimi anni e lesson learned e best practice.

4.1 Principali Casi di Cyber Crime Statale (2024-2026)

Campagna Cyber Russa contro l'Ucraina (2024): +70% - Gli attacchi informatici russi contro l'Ucraina sono aumentati di quasi il 70% nel 2024, con 4.315 incidenti documentati che hanno preso di mira infrastrutture critiche, servizi governativi, il settore energetico e le entità legate alla difesa.
La campagna dimostra l'integrazione sistemica tra cyber warfare e conflitto cinetico convenzionale, con operazioni cyber utilizzate per degradare le capacità difensive e di comunicazione prima degli attacchi fisici.

Cyber spionaggio cinese (2024): +150% e +300% nel Manifatturiero - Le operazioni di cyber spionaggio cinese hanno registrato una crescita senza precedenti nel 2024. Il settore dei semiconduttori è identificato come particolarmente vulnerabile, in relazione alla competizione con TSMC e alle restrizioni alle esportazioni americane.
Google identifica la Cina come la minaccia di spionaggio industriale più sofisticata e capillare al mondo, con focus su proprietà intellettuale nei settori strategici: AI, quantum computing, tecnologie militari avanzate.

Attacco al U.S. Treasury Department (dicembre 2024) - Hacker cinesi hanno violato un fornitore terzo del Dipartimento del Tesoro degli Stati Uniti, ottenendo accesso a oltre 3.000 file non classificati. Il caso enfatizza la problematica delle vulnerabilità della supply chain: l'aggressore non ha attaccato frontalmente il governo USA, ma ha sfruttato un anello debole della catena di fornitura. La best practice di risposta richiede validazione multi-livello dei fornitori, architetture Zero Trust per limitare il movimento laterale, e piattaforme XTI per il monitoraggio continuo della supply chain.

Furto ByBit: $1,5 Miliardi in Ethereum (febbraio 2025) - Hacker nordcoreani hanno rubato 1,5 miliardi di dollari in Ethereum dall'Exchange con sede a Dubai ByBit, stabilendo il record mondiale per furto di criptovalute attribuito a uno Stato-nazione.
Il caso illustra la strategia di Pyongyang di utilizzare il cyber crime finanziario come fonte di reddito per il programma nucleare, ovvero, un modello unico nel panorama internazionale che dissolve la distinzione tra criminalità e politica di Stato.

4.2 Scenari geopolitici 2026: il nuovo ordine cyber internazionale

Di seguito i vari scenari geopolitici che stanno caratterizzano il 2026.

Guerra ibrida Russia-NATO - Escalation digitale
Il conflitto russo-ucraino continua a essere il laboratorio più avanzato di guerra ibrida. Pur non essendo coinvolta direttamente, la NATO ha iniziato a rispondere alle operazioni della "zona grigia" russa con azioni *cyber offensive* più aggressive, segnando un cambiamento dottrinale significativo.
Inoltre, l'escalation di attacchi alle infrastrutture energetiche, ai sistemi di trasporto e alle reti di comunicazione europee, combinata con operazioni di disinformazione contro processi elettorali, configura un livello di aggressione che sfida le categorie tradizionali del diritto internazionale.

Competizione USA-Cina - La guerra dei chip
La competizione tecnologica USA-Cina si manifesta con crescente intensità nel cyberspazio. Lo spionaggio industriale contro i produttori di semiconduttori – i.e. TSMC, Intel, Samsung - è sistematico e documentato. Inoltre, le restrizioni all'esportazione di tecnologie EUV e AI imposte da Washington accelerano la risposta cyber di Pechino, che cerca di acquisire - attraverso operazioni clandestine - ciò che non può ottenere per via commerciale, oltre che sviluppare propri chip IA.

Iran - Cyber come deterrenza asimmetrica - Il conflitto in atto ha rivelato la piena maturità delle capacità cyber iraniane. Ovvero, l'Iran ha dimostrato di saper combinare operazioni statali dirette con reti di *proxy hacktivist* distribuite globalmente, operanti autonomamente anche durante il blackout internet domestico attraverso servizi VSAT e Starlink.
Inoltre, il targeting di sistemi OT/ICS (Rockwell Automation, sistemi SCADA energetici) evidenzia una evoluzione qualitativa verso capacità distruttive sulle infrastrutture critiche occidentali.

Corea del Nord - Il modello del cyber crime statale
Il gruppo Lazarus e le operazioni affiliate continuano a rappresentare il caso più estremo di "fusione" tra Stato e cyber crime. Con il furto ByBit, Pyongyang ha dimostrato capacità di eseguire operazioni finanziarie offensive da miliardi di dollari, finanziando direttamente il programma di armamenti.
Inoltre, l'infiltrazione in aziende tech globali tramite operativi sotto false identità — identificata da Microsoft nel 2025 — introduce un vettore di rischio supply chain di difficile contrasto.

5. Framework operativo: ciclo di validazione e cyber intelligence integrata

Segue una roadmap di attuazione del framework operativo di cyber intelligence integrata.

5.1 Il ciclo di intelligence: dall'OSINT alla decisione politica

La gestione efficace delle minacce cyber di stampo statale richiede un framework operativo che integri OSINT, HUMINT e analisi tecnica in un ciclo strutturato di raccolta, validazione e disseminazione.

È doveroso evidenziare che il caso SolarWinds (2020) rimane un riferimento metodologico fondamentale, considerando che l'elemento umano fu determinante per identificare la campagna come spionaggio statale russo — e non cyber crime ordinario — e per valutare la portata strategica oltre i dati tecnici.

Di seguito uno schema del ciclo di cyber intelligence in 6 fasi

IL CICLO DI CYBER INTELLIGENCE	
FASE 1	**RACCOLTA AUTOMATIZZATA** - OSINT, Network Monitoring, Honeypots, Dark Web Feed, Threat Intelligence commerciale
FASE 2	**ANALISI TECNICA AI/ML** - Pattern recognition, anomaly detection, correlazione IoC, clustering TTPs (Tactics, Techniques, and Procedures).
FASE 3	**VALIDAZIONE UMANA CRITICA** - Analisti senior verificano falsi positivi, contestualizzano geopoliticamente, valutano motivazioni dell'attore.
FASE 4	**ARRICCHIMENTO HUMINT** - Conferma e approfondimento attraverso fonti umane; verifica cross-source; valutazione affidabilità.
FASE 5	**SINTESI E ATTRIBUZIONE** - Documento intelligence actionable; livello di fiducia sull'attribuzione; opzioni di risposta.
FASE 6	**DECISIONE POLITICA** - Risposta diplomatica, legale, tecnica o militare; coordinamento alleati; comunicazione pubblica

NOTA
La Fase 3 - Validazione Umana Critica è il punto nevralgico dell'intero ciclo, considerando che nessun sistema AI/ML, per quanto avanzato, può sostituire il giudizio contestuale di un analista senior nel distinguere tra un attacco stato-sponsorizzato e un'operazione cybercriminale opportunistica, o nel valutare le implicazioni geopolitiche di un'attribuzione pubblica.

Nel contesto del conflitto USA-Iran 2026, la velocità con cui operazioni proxy attivate da attori geopoliticamente eterogenei (pro-Iran, pro-Russia, hacktivist autonomi) si sono sovrapposti, ha reso la validazione umana ancora più critica sempre più un asset strategico.

5.2 Best practice per il 2026: priorità operative

Di seguito alcune delle best practice e priorità da considerare a fronte dello scenario geopolitico contingente.

Architettura Zero Trust - L'implementazione di Zero Trust — "*never trust, always verify*" — è diventata la priorità assoluta per organizzazioni ed enti governativi. Da quanto si evince dai vari report del settore della cybersecurity, il 96% delle organizzazioni globali favorisce questo approccio, mentre l'81% è in fase di implementazione. I principi fondamentali includono: verifica continua delle identità, privilegio minimo (JIT access), micro-segmentazione della rete, e *continuous monitoring* di tutte le sessioni e connessioni.

SOC automatizzati dall'AI - Nel 2026, l'AI passa da deployment sperimentali a componenti completamente integrate nei *Security Operations Center (SOC)*. L'AI non è più limitata al rilevamento di anomalie, ma abbraccia l'intero ciclo dell'incidente, ovvero: *threat identification, prioritization, containment* e *remediation* automatizzati.
Inoltre, i sistemi SOAR (*Security Orchestration, Automation and Response*) potenziati dall'AI liberano gli analisti umani per le analisi maggiormente complesse di contesto geopolitico, i.e. l'area dove il fattore umano rimane insostituibile.

Post-Quantum Cryptography (PQC) - Il quantum computing raggiunge nel 2026 un punto di svolta che impone la migrazione urgente verso *Crittografia Post-Quantum (PQC)*. Pertanto, si consiglia - quanto prima - alle organizzazioni di: inventariare tutti i sistemi che utilizzano crittografia asimmetrica vulnerabile; implementare "*crypto-agility*" per permettere il rapido switch di algoritmi; partecipare ai programmi di standardizzazione NIST.

Di fatto, è doveroso evidenziare che gli attori statali - in particolare Russia e Cina – stanno accumulando dati cifrati oggi in previsione di decriptarli quando il quantum computing sarà maturo (i.e. strategia "*harvest now, decrypt later*").

La resilienza come strategia core - Il paradigma si sta spostando dalla prevenzione totale - ormai riconosciuta come impossibile - alla resilienza come strategia operativa fondamentale. Ne consegue che le organizzazioni devono assumere che la compromissione sia inevitabile e pianificare in base a questa assunzione, definendo: *Business Continuity Planning* con scenari cyber-attack specifici, *Recovery Time Objective (RTO)* e *Recovery Point Objective (RPO)* realistici; *tabletop exercise* trimestrali con scenari geopolitici attuali.

6. Raccomandazioni strategiche: rompere il silenzio legale e diplomatico

Di seguito alcune raccomandazioni strategiche per rompere il silenzio legale e diplomatico.

6.1 Comunità internazionale e governi

È doveroso evidenziare che superare il silenzio diplomatico sulle cyber operazioni statali richiede un approccio su più livelli, che combini obblighi legali vincolanti, meccanismi istituzionali nuovi e incentivi diplomatici strutturati. Le seguenti raccomandazioni scaturiscono dall'analisi dei casi studiati e dalle dinamiche del conflitto USA-Iran 2026.

Raccomandazioni prioritarie per governi e organizzazioni internazionali	
Tribunale Internazionale Cyber	Istituzione di una giurisdizione specifica per il cyber crime statale, con competenza sull'attribuzione certificata delle operazioni, analoga al Tribunale Penale Internazionale ma con meccanismi adattati alla specificità del dominio digitale
Estensione delle Convenzioni di Ginevra al cyberspazio:	Protocollo aggiuntivo che definisca le cyber armi, individui le infrastrutture civili protette (ospedali, sistemi idrici, reti elettriche), e stabilisca soglie di intervento proporzionale
Transparency reporting obbligatorio:	Obbligo per gli Stati di dichiarare le proprie capacità cyber offensive — sul modello dei trattati di controllo degli armamenti — come prerequisito per la costruzione della fiducia internazionale
Sanzioni multilaterali coordinate	Meccanismi automatici di sanzioni multilaterali per violazioni accertate da organismi internazionali certificati, riducendo la dipendenza dal consenso politico contingente
Hotline cyber tra Paesi	Canali di comunicazione diretta per la de-escalation delle crisi cyber, analoghi alle hotline nucleari della Guerra Fredda, con protocolli di notifica per operazioni ad alto rischio di mispercezione
European Union Vulnerability Database[9]	Promuovere ulteriormente il Catalogo europeo delle vulnerabilità attivamente sfruttate, armonizzato con il CISA KEV americano, per una prioritizzazione basata su evidenza delle patch e una risposta coordinata

Organizzazioni che operano nell'ambito delle Infrastrutture Critiche - Le organizzazioni che operano nei settori critici — i.e. energia, finanza, healthcare, difesa, space, ecc. — fronteggiano minacce che combinano capacità statali con obiettivi criminali. Pertanto, dovrebbero considerare le seguenti raccomandazioni integrate che tengono conto del panorama geopolitico del 2026.

Settore Energia e Infrastrutture Critiche	Settore Finanziario
Segmentazione OT/IT rigorosa con air gap fisici	**Preparazione per attacchi** a sistemi SWIFT e pagamenti
Threat intelligence feed specifici per APT energy-targeting	**Crypto-asset security** contro *state-sponsored heist*
Esercitazioni di black-start (riavvio completo)	**Sanctions compliance automation** contro *money laundering*
Collaborazione con CISA/ENISA per early warning	**Collaborazione con FinCEN** per intelligence su flussi anomali
Protezione sistemi SCADA da attori iraniani e russi	**Incident response plan** per furto di asset digitali

Healthcare e Pharma	Aerospazio e Difesa
Protezione research data su vaccini e terapie	**Continuous threat hunting** vs. *Assume persistent breach:*
Resilience planning con *patient safety* come priorità	***ITAR (International Traffic in Arms Regulations) /EAR (Export Administration Regulations)*** compliance automation
Segmentazione *medical devices* da reti IT generali	**Collaborazione** con *defense intelligence* per attribuzione
Intelligence su targeting da stati ostili (bio-tech)	**Quantum-safe encryption (QSE)** per comunicazioni classificate
Backup immutabili e Recovery Point Objective < 4h	**Supply chain verification** per componenti critici

6.3 Il ruolo del fattore umano nella cyber intelligence

L'avanzamento delle tecnologie AI rischia di oscurare una verità fondamentale, ovvero: il fattore umano rimane l'elemento centrale e insostituibile della cyber intelligence. Non si tratta solo di analisti che validano dati tecnici, ma di professionisti capaci di leggere il contesto geopolitico, comprendere le motivazioni degli attori, e tradurre l'intelligence tecnica in successive decisioni politiche calibrate effettuate dalle autorità preposte.

La manipolazione psicologica - i.e. ingegneria sociale, deepfake, campagne di disinformazione creati dall'AI — dimostra come l'essere umano rimanga l'infrastruttura critica più vulnerabile. Nel conflitto USA-Iran 2026, la compromissione dell'app BaadeSaba e le campagne di disinformazione AI-enabled contro il regime iraniano, di fatto, hanno operato sulla dimensione psicologica e cognitiva, non tecnica, del conflitto.

Pertanto, la convergenza tra *Cyber Intelligence*, *OSINT* e *HUMINT* richiede un approccio radicalmente integrato, considerando che l'automazione gestisce volume e velocità, mentre l'elemento umano garantisce qualità, contesto e responsabilità. Solo attraverso questo equilibrio è possibile evitare errori di valutazione dalle conseguenze geopolitiche significative, quali la mis-identificazione di un'operazione di spionaggio come atto di guerra, o viceversa.

7. Conclusioni: verso un regime internazionale di cyber governance

Il 2026 rappresenta un anno di svolta epocale per la cyber security internazionale. Il conflitto USA-Iran ha dimostrato ulteriormente che il cyberspazio è il quinto dominio della guerra, inseparabile da

terra, mare, aria e spazio. Di fatto, la convergenza tra cyber crime, cyber warfare e cyber intelligence - già teorizzata - è sempre più una realtà operativa documentata.
Ne consegue che il silenzio legale e diplomatico sulle operazioni cyber degli Stati non è più sostenibile. Non perché venga richiesto da considerazioni etiche astratte, bensì perché è diventato una fonte di instabilità sistemica: la mancanza di norme condivise aumenta il rischio di mispercezione, escalation non intenzionale e proliferazione incontrollata di capacità offensive.

Di fatto, se il caso Stuxnet del 2010 ha aperto un vero e proprio vaso di Pandora, il conflitto USA-Iran 2026 ha evidenziato definitivamente la necessità di una cyber governance.

È doveroso evidenziare che, pur essendo la strada verso un regime internazionale di governance cyber sia lunga e difficile, essa non è impossibile, soprattutto ricordando come il modello dei trattati di controllo degli armamenti della Guerra Fredda - costruito pazientemente tra avversari ideologici profondi - offra una lezione di metodo: la cooperazione su norme minime di comportamento non richiede fiducia reciproca, ma solo il riconoscimento condiviso che l'instabilità totale è peggiore delle limitazioni negoziate.

Inoltre, in questo contento di perma-crisi e poli-crisi, le organizzazioni devono garantire sempre più la resilienza e investire nell'elemento umano della cyber intelligence, oltre a partecipare attivamente alla costruzione di un ecosistema di cooperazione internazionale.
Il cyberspazio non può rimanere il "Far West" della sicurezza internazionale: la posta in gioco – i.e. infrastrutture critiche, sistemi finanziari e vite umane - è troppo alta.

Pertanto, per superare il silenzio legale e diplomatico, si tratterà di:

- **Avviare negoziati per un ulteriore protocollo aggiuntivo** alle Convenzioni di Ginevra sul cyberspazio, con definizione vincolante di *cyber weapon* e protezioni per le infrastrutture civili
- **Istituire un Gruppo di Esperti Internazionali** per la certificazione dell'attribuzione cyber, a supporto delle dichiarazioni pubbliche coordinate degli Stati alleati
- **Costruire un sistema di hotline cyber bilaterali** tra le principali potenze (USA-Russia, USA-Cina, NATO-Russia) per la de-escalation delle crisi digitali
- **Adottare standard internazionali minimi di transparency reporting** sulle capacità cyber offensive, inserendo la questione nell'agenda G7 e G20
- **Accelerare la migrazione globale verso crittografia post-quantum** prima che il quantum computing renda obsoleti gli attuali sistemi di protezione delle comunicazioni classificate
- **Investire massicciamente nella formazione di analisti di cyber intelligence** con competenze integrate: tecniche, geopolitiche e giuridiche internazionali

Concludendo, la velocità con cui gli eventi cyber si propagano impone sistemi di intelligence capaci di anticipare, interpretare e rispondere a minacce senza confini e a forme inedite di conflitto digitale.

Datum, in latino, indicava «ciò che è dato» — un punto di partenza, non un punto di arrivo. Oggi il dato è l'elemento fondamentale da cui prende avvio ogni processo conoscitivo: raccolto, condiviso, elaborato per generare informazione utile all'azione.

Inoltre, la validazione attraverso fonti multiple non è un'opzione metodologica, ma una condizione di sopravvivenza operativa. Altrettanto cruciale è l'integrazione tempestiva di queste informazioni nei processi decisionali - dalla gestione delle crisi alla protezione degli ecosistemi critici - senza dimenticare che nessuna tecnologia può sostituire la responsabilità politica di rompere il silenzio e costruire una governance cyber condivisa, fondata su una diplomazia digitale finalmente all'altezza della posta in gioco.

Il contrasto alle nuove forme di conflitto richiede, pertanto, una metamorfosi profonda: un framework legale condiviso e una cyber diplomazia non solo come strumento tattico di raccolta informativa ma anche come architettura di intelligence informativa.

Fonti e Riferimenti

Il presente White Paper si basa su fonti primarie di ricerca open-source, documenti governativi e rapporti di intelligence privata aggiornati ad aprile 2026. Di seguito le principali fonti di riferimento.

Fonti primarie istituzionali:

- CISA (Cybersecurity and Infrastructure Security Agency) - Nation-State Cyber Actors (cisa.gov)
- Center for Strategic and International Studies — Significant Cyber Incidents Database 2024-2026 (csis.org)
- Canadian Centre for Cyber Security — Cyber Threat Bulletin: Iranian Cyber Threat Response, (Febbraio 2026)
- Palo Alto Networks Unit 42 — Threat Brief: Escalation of Cyber Risk Related to Iran (aggiornato ad Aprile 2026)
- U.S. Department of Justice — Justice Department Disrupts Iranian Cyber-Enabled Psychological Operations (Marzo 2026)
- CSIS — How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran? (Marzo 2026)

Rapporti di threat intelligence:

- Microsoft Security Intelligence — 2025 Review: Nation-State Cyber Operations
- Google Threat Intelligence Group / Mandiant — Annual M-Trends Report 2025
- Flare.io — Monitoring Cyberattacks Directly Linked to the US-Israel-Iran Military Conflict
- SentinelOne — Cybersecurity Trends and Nation-State Actors 2025-2026
- Accenture — State of Cybersecurity 2025
- CrowdStrike — Global Threat Report 2025

Framework e documentazione tecnica:

- MITRE ATT&CK Framework — Enterprise Matrix v15
- NIST — Post-Quantum Cryptography Standards (FIPS 203, 204, 205)
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017)
- EU NIS2 Directive — Directive (EU) 2022/2555
- World Economic Forum — Global Cybersecurity Outlook 2026

Fonti italiane ed europee:

- CybersecItalia — Cyberspazio: l'agenda UE per prevenire il terrorismo
- CybersecItalia — Oltre il perimetro tecnologico: fattore umano, manipolazione psicologica e difesa human-centric
- AgendaDigitale — Geopolitica dell'AI: il nuovo power play globale in un mondo senza arbitri
- ISMS.online — The line between nation-states and cybercrime is blurring: that's bad news for CISOs
- Bytelegali — Pierguido Iezzi: la vera infrastruttura critica oggi è l'essere umano