ZENITA GROUP

VALUTAZIONE ANALITICA

IRAN CYBER OPERATIONS: EFFICACIA, LIMITI E IMPLICAZIONI

Una valutazione sistematica dell'efficacia operativa, dei limiti strutturali e delle implicazioni strategiche delle cyber operations iraniane nel contesto del conflitto regionale mediorientale (2020–2026).

UNA CYBER ACIES

SOMMARIO

Executive Summary

Sintesi valutativa delle cyber operations iraniane nel contesto del conflitto regionale mediorientale 2020–2026

Questo documento analizza l'efficacia militare e strategica delle cyber operations condotte dall'Iran nel contesto del conflitto regionale mediorientale (2020-2026), con attenzione al periodo successivo all'escalation Iran-USA di febbraio 2026 (Operation Epic Fury, 28 feb). A differenza dei tradizionali threat brief situazionali, adotta un framework analitico derivato da metodologie di intelligence militare.

+600
Rivendicazioni 7gg

47
Threat Actors

9
APT statali attivi

+50
Picchi giornalieri di claims

+4%
Connettività in Iran

11
Paesi colpiti

1. OPERAZIONI CYBER OFFENSIVE: IMPATTO LIMITATO SU SCALA STRATEGICA

Le operazioni cyber offensive iraniane hanno prodotto effetti tattici documentati in contesti circoscritti — ICS/SCADA su impianti idrici, GPS spoofing marittimo, disruption di infrastrutture israeliane — ma non hanno mai raggiunto la soglia di impatto strategico necessaria a modificare equilibri militari. Per ogni attacco cyber con effetti documentati, operazioni cinetiche proxy (Hezbollah, Houthi) e missilistiche hanno prodotto effetti di gran lunga superiori.

2. RACCOLTA INTELLIGENCE: IL VERO CENTRO DI GRAVITÀ

La raccolta di intelligence cyber rappresenta la priorità operativa reale dell'Iran. APT33, APT34 e MuddyWater mantengono accessi persistenti in reti governative, difesa e infrastrutture critiche di decine di paesi. Questa capacità — pre-posizionamento silenzioso, esfiltrazione di IP, sorveglianza di dissidenti — rappresenta il rischio maggiore e più duraturo per organizzazioni europee.

3. RACCOLTA INTELLIGENCE: IL VERO CENTRO DI GRAVITÀ

A differenza del modello russo (GRU/Viasat), il coordinamento tra cyber e cinetico iraniano è principalmente opportunistico. I casi documentati mostrano correlazione temporale ma raramente integrazione tattica. La struttura frammentata IRGC/MOIS/proxy ostacola la pianificazione integrata necessaria per operazioni sincronizzate.

4. FATTORI LIMITANTI STRUTTURALI

L'efficacia strategica iraniana è limitata da: capacità offensive inferiori a Russia/Cina; dipendenza da supply chain tecnologica soggetta a sanzioni; difese avanzate dei target primari (Israele, USA, Arabia Saudita); incapacità di sostenere operazioni ad alta intensità nel tempo.

5. IMPLICAZIONI PER ORGANIZZAZIONI EUROPEE

Il settore marittimo, PA, infrastrutture energetiche e difesa europeo sono target documentati. Nella finestra feb-mar 2026: oltre 600 rivendicazioni di attacco in 7 giorni, campagne DDoS e defacement coordinate su PA, media e infrastrutture critiche. Il rischio primario rimane l'esfiltrazione persistente e il pre-posizionamento silenzioso — ma la componente disruptiva è operativamente attiva.

FRAMEWORK METODOLOGICO

Approccio analitico e criteri di valutazione

Questo documento supera la logica binaria successo/fallimento, adottando una **metrica di valore relativo:** l'efficacia di un'operazione cyber è misurata in funzione della sua capacità di generare effetti non ottenibili tramite strumenti cinetici o diplomatici. Adotta invece una valutazione graduata degli effetti, comparando le cyber operations con altri strumenti di potere disponibili all'Iran: forze proxy, capacità cinetiche convenzionali, coercizione economica e diplomatica.

OPERAZIONI CYBER

(Operazioni Distruttive / Disruptive)

Operazioni cyber intese a distruggere, degradare o manipolare dati e sistemi. Comprende: wiper malware, attacchi ICS/SCADA, DDoS su infrastrutture critiche, defacement coordinato. Metrica: effetti fisici misurabili, downtime documentato, perdite economiche quantificabili.

RACCOLTA INTELLIGENCE

(Raccolta, Spionaggio, Influence Ops)

Operazioni finalizzate alla raccolta di informazioni, pre-posizionamento strategico e influence operations a lungo termine. Include: APT persistenti, esfiltrazione di IP, sorveglianza dissidenti. Metrica: accessi documentati, dati esfiltrati, impatto su processi decisionali avversari.

PRINCIPI METODOLOGICI

Effetti reali vs. intenzionali

Si analizzano gli effetti documentati, non le intenzioni attribuite. Un attacco cyber con zero downtime è valutato come tale indipendentemente dalla sofisticazione tecnica.

Analisi top-down + bottom-up

La valutazione tattica di singoli incidenti (bottom-up) è integrata con una valutazione cumulativa degli effetti strategici (top-down).

Comparazione con altri strumenti

Le cyber operations iraniane vengono sistematicamente comparate con le capacità cinetiche, proxy e diplomatiche disponibili, per valutarne il valore relativo — non assoluto.

Trasparenza delle fonti e dei limiti

Tutte le valutazioni sono qualificate in termini di confidenza (ALTA/MEDIA/BASSA). Il "cyber fog of war" è esplicitamente riconosciuto. Le affermazioni sono supportate da fonti pubbliche o da analisi con livello di confidenza esplicitato.

Orientamento operativo

Le conclusioni sono tradotte in implicazioni concrete per organizzazioni europee nei settori a rischio: marittimo, PA, difesa, energia, telecomunicazioni.

OPERAZIONI CYBER OFFENSIVE — EFFICACIA

Analisi per categoria target: contributo operativo delle capacità cyber rispetto agli strumenti cinetici o proxy

Le operazioni cyber offensive iraniane vengono analizzate per categoria di obiettivo con approccio sistematico. Per ciascuna categoria si valuta: l'impatto cyber documentato, l'impatto cinetico/proxy comparabile e il contributo netto delle operazioni cyber. La valutazione sintetica indica il contributo netto reale di ciascuna categoria.

Categoria target	Impatto cyber doc.	Operazioni emblematiche	Contributo netto
Forze Militari Avversarie	Accessi dimostrativi, nessun effetto tattico reale	Nessun caso documentato di disruption sistemi militari in ops attive — solo pre-posizionamento (MOIS/APT33)	BASSO
ICS/SCADA & Infra Idriche	Accessi documentati, effetti minimi	CyberAv3ngers USA/IL (CISA AA23-335A); Oldsmar FL (2021); Jordan NCC silos grano (mar 2026)	BASSO
Comunicazioni & Trasporti	GPS spoofing sistematico operativo	GPS spoofing Golfo Persico/ Mar Rosso (2019-24); pre-posizionamento sistemi marittimi	MODERATO
Settore Energetico	Wiper limitati, proxy fisici superiori	Shamoon 2.0 affiliates Aramco (2017, attr. Russia); proxy Houthi >> cyber in effetti	BASSO
Pubblica Amministrazione	Albania 2022: caso strategico unico	HomeLand Justice, rottura relazioni diplomatiche Albania-Iran. Caso unico NATO.	MODERATO-ALTO
Infrastruttura Cloud 2026	AWS UAE/Bahrain: nuovo precedente	Danni fisici 1 mar 2026; IRGC dichiara data center target militare. Effetti a cascata regionali.	ALTO

CASO STUDIO — ALBANIA 2022 (HomeLand Justice / MERCURY+DEV-1084)

- **Luglio–settembre 2022:** attori iraniani (MERCURY+DEV-1084) compromettono reti governative albanesi per 14 mesi, poi lanciano attacco distruttivo su PA e servizi pubblici.
- **7 settembre 2022:** Albania recide le relazioni diplomatiche con l'Iran — PRIMO CASO MONDIALE di rottura diplomatica conseguente a un cyber attack. Attribuzione formale NCSC UK + CISA/FBI.

CASO STUDIO — AWS UAE/BAHRAIN (1 MARZO 2026) · ALTO

- **AWS conferma danni fisici a facility in UAE (2 siti) e Bahrain (1 sito) — il più forte precedente di impatto militare su infrastruttura hyperscaler USA. Fars News Agency (IRGC):** target esplicito "per supporto a USA".
- **Fonti:** AWS statement 2 mar; CNBC 3-6 mar; Bloomberg 5 mar; Fortune 3 mar 2026.

Vantaggi Teorici Del Dominio Cyber - Grado Di Realizzazione

Analisi sistematica: la cyber offre vantaggi teorici unici — ma l'Iran non li ha realizzati

La cyber offre vantaggi teorici rispetto agli strumenti fisici e proxy: effetti reversibili, deniabilità, portata geografica, limitazione del danno collaterale, effetti sistemici. Questa sezione valuta sistematicamente se l'Iran ha realizzato questi vantaggi nelle operazioni documentate. La risposta è consistentemente negativa su tutti gli assi.

Vantaggio teorico	Stato	Valutazione
Effetti reversibili (no danno permanente)	NON REALIZZATO	Le operazioni più ambiziose (Shamoon, Dustman) hanno prodotto distruzione permanente di dati. Solo il GPS spoofing è stato veramente reversibile.
Deniabilità operativa	PARZIALMENTE REALIZZATO	Attribution rapida da MSTIC/CISA/GCHQ ha ridotto la finestra a settimane. La deniabilità non si traduce in immunità da sanzioni.
Portata geografica globale	REALIZZATO (solo intel)	Documentato in 78+ paesi (APT34/MSTIC 2024) — ma per raccolta intelligence, non operazioni offensive.
Limitazione danno collaterale	NON REALIZZATO	Proxy Houthi/Hezbollah hanno causato danni fisici massivi e deliberati. Nessuna evidenza di "cyber restraint" coordinato.
Efficienza economica	PARZIALMENTE REALIZZATO	Zero-days e toolchain avanzate hanno costi elevati + dipendenza da supply chain sotto sanzioni.
Effetti sistemici a cascata	NON REALIZZATO	Iran non ha mai replicato NotPetya russo (2017). Nessun "wormable malware" attribuito con questa capacità.

Mappa Attori — Classificazione Per Tipologia

Struttura a 4 livelli: APT statali / Proxy IRGC / Hacktivisti coordinati / Attori russi

La mappa degli attori iraniani e del teatro allargato è strutturata per tipologia operativa e non per semplice attribuzione: questa distinzione è critica per calibrare le difese. Gli APT statali rappresentano la minaccia più sofisticata e persistente; i proxy e gli hacktivisti generano volume e rumore. Fonti: CISA, MSTIC, NCSC, ENISA, ESET, Unit 42, Mandiant, CrowdStrike, analisi Maticmind 2026.

TIER 1 — APT STATALI (IRGC / MOIS) — Minaccia ad alta sofisticazione, obiettivi strategici				
Attore / sigla	**Struttura**	**Capacità primaria**	**Operazioni emblematiche**	**Target it/eu**
APT33 Peach Sandstorm	**IRGC-linked**	Wiper malware attacchi ICS/SCADA spear phishing	Shamoon 2.0 (2017, Aramco) Dustman (2019, Kuwait) ZeroCleare (2019, ME) Albania 2022 (MOIS/ Homeland Justice)	Energia/oil&gas EU OT gas/ICS (ALTO)
APT34 OilRig	**MOIS (Intel)**	DNS tunneling RAT persistenti spear phishing PA	DNSpionage (2019) Helix Kitten campaign OilRig 2022-23 Intrusioni PA Gov ME	PA europea (ALTO) Difesa/aerospazio NATO contratti
CyberAv3ngers	**IRGC Cyber Div.**	Attacchi OT/ICS PLC/ SCADA water utilities	Impianti idrici USA/IL (2023) CISA Advisory AA23-335A Jordan NCSC: OT bloccato (mar 2026)	Impianti idrici EU OT ind. (ALTO) Food/energy
MuddyWater Mango Sand.	**MOIS (ops)**	RAT custom RustyWater (Rust) Dindoor/ Fakeset backdoor	BugSleep (2024) · Earth Vetala Fakeset (feb 2026) Op. Olalampo 2026, area MENA	PA europea (ALTO) Telco EU Difesa/ supply ch.
APT35 Charming Kitten	**IRGC-linked**	Spear phishing mobile (RedAlert APK) sorveglianza	Endless Mayfly diusinformation campaign/media impersonation· Targeting di dissidenti in Germania 2023	Accademici/giorn. Dissidenti, EU think tank, istituti
Agrius / Pink Sandstorm	**MOIS (attrib. disputata)**	Wiper/ransomware faux extortion Israele supply chain	Fantasy wiper (2022) Apostle/IPsec Helper Backdoor	Israele (CRITICO) Forniture difesa Supply chain IT
Fox Kitten UNC757	**IRGC(access broker)**	Exploit VPN/edge access broker perimeter device	Fortinet/Pulse Secure exploit Edge device scanning Initial access broker IRGC	PA/infrastr. EU Reti VPN enterprise. Edge device exp.
Tortoiseshell Imperial Kitten	**IRGC mercenari dig.**	Watering hole fake recruiting spionaggio IT	LinkedIn/Indeed ops 2023 Israele + diaspora target Defense sector intrusion	Difesa/aerospazio Diaspora iraniana, Maritime, Shipping, Logistics

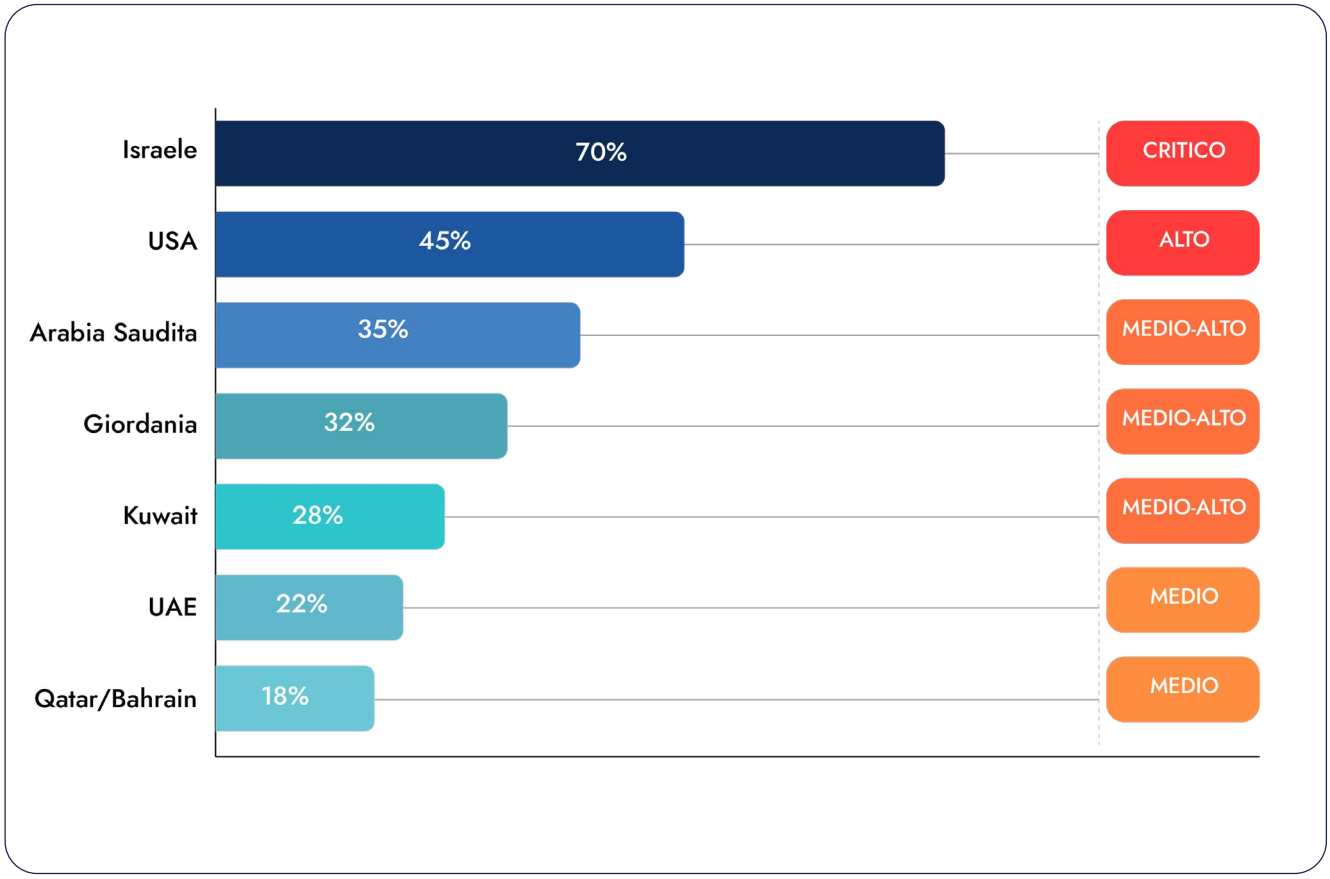
TIER 2 — PROXY IRGC / SEMI-STATALI — Plausible deniability, operazioni tattiche				
Attore / sigla	**Struttura**	**Capacità primaria**	**Operazioni emblematiche**	**Target it/eu**
Emennet Pasargad Cotton Sandstorm	**IRGC Electronic Warfare**	WezRAT infostealer hack-and-leak influence ops	Charlie Hebdo hacking, WezRAT vs IL Cyber Directorate USA election 2020/24	EU election narrat. Opinion leader EU Media (BASSA)
Handala Hack Team	**MOIS-linked (attrib. parziale)**	Data leak defacement pressione psicologica	Clalit IL, provider healthcare (feb 2026), doxxing di funzionari della difesa israeliani	Energia/infrastr.MO Rischio EU supply
Moses Staff Abraham's Ax (COBALT SAPLING)	**IRGC proxy/ personas**	Leak dati falso ransomware pressione psicologica	Gov israeliano/giordano, Arabia Saudita Aziende difesa MO Supply chain EU (2023)	Aziende IT EU (MED) Studio legali dif. Forniture NATO

TIER 3 — HACKTIVISTI COORDINATI (Electronic Operations Room) - Volume, rumore, deterrenza mediatica				
Attore / sigla	**Struttura**	**Capacità primaria**	**Operazioni emblematiche**	**Target it/eu**
Cyber Islamic Res. 313 Team / DieNet	**Electronic Op. Room**	DDoS coordinato leak & dox canali Telegram	Campagne DDoS EU/ IL/Kuwait 2023-26 Leak PA israeliana RipperSec, Moroccan BCA	Media EU (MEDIO) Siti PA (ALTO) Opinion leader
Cyber Toufan Holy Souls	**IRGC proxy/ hackt.**	DDoS leak data disinformazione	DDoS target EU/IL 2023-24 Canali Telegram propaganda DDoS banche e media	Media EU (MEDIO) Siti governo PA

TIER 4 — ATTORI RUSSI (Teatro allargato) - Convergenza tattica, non coordinamento strategico documentatomediatica				
Attore / sigla	**Struttura**	**Capacità primaria**	**Operazioni emblematiche**	**Target it/eu**
Cyber Islamic Res. 313 Team / DieNet	**Electronic Op. Room**	DDoS coordinato leak & dox canali Telegram	Campagne DDoS EU/ IL/Kuwait 2023-26 Leak PA israeliana RipperSec, Moroccan BCA	Media EU (MEDIO) Siti PA (ALTO) Opinion leader
Cyber Toufan Holy Souls	**IRGC proxy/ hackt.**	DDoS leak data disinformazione	DDoS target EU/IL 2023-24 Canali Telegram propaganda DDoS banche e media	Media EU (MEDIO) Siti governo PA

INTENSITÀ RELATIVA TARGET PER PAESE (STIMA UCA)

Intensità di targeting osservata — Operation Epic Fury, feb-mar 2026 — Assessment UCA



Fonte: Unit 42, CloudSEK, Flashpoint, AttackIQ — analisi aggregata attack claims feb-mar 2026. Assessment UCA, confidenza MEDIA.

IMPLICAZIONI PER SETTORI ITALIANI ED EUROPEI

Profilo di rischio settoriale e raccomandazioni operative per il contesto europeo

Il Canadian Centre for Cyber Security (Five Eyes) ha valutato come **"very likely"** l'uso di operazioni cyber iraniane come strumento di ritorsione nel contesto dell'attuale crisi geopolitica. Il Canada è classificato come **target secondario,** in ragione del supporto politico espresso verso USA e Israele.

Una dinamica analoga potrebbe interessare altri paesi NATO ed europei con posizioni pubbliche allineate.

SETTORE MARITTIMO

RISCHIO ALTO

Vettore Primario

Cyber reconnaissance su sistemi satcom, Port Community Systems (PCS) e Terminal Operating Systems (TOS), con potenziale pre-posizionamento su sistemi di cargo management e port authority. GPS spoofing sistematico nel Mar Rosso/Golfo Persico documentato 2019-2024.

Mar '26: 1.100+ anomalie AIS in 7gg, con "Denial Zones" (oscuramento) e "Injected Zones" (coordinate false) per confondere i sistemi di navigazione/puntamento.

Rischio Sottostimato

- Sistemi satellitari commerciali poco protetti;
- digitalizzazione portuale rapida;
- rilevanza strategica supply chain EU;
- interdipendenza con operazioni Houthi nel Mar Rosso.

Raccomandazioni

1. Segregare navigazione, satcom e cargo systems con zone/conduits IEC 62443.
2. MFA phishing-resistant + VPN always-on su accessi shore.
3. OT-IDS dedicato per anomalie GNSS/GPS/ECDIS.
4. Drill trimestrali per spoofing, jamming e degrado operativo.

INFRASTRUTTURE ENERGETICHE E CLOUD

RISCHIO MOLTO ALTO

Vettore Primario

Pre-posizionamento documentato in sistemi ICS/SCADA USA e Israele (CISA AA23-335A). Data center cloud regionali (es. infrastrutture hyperscaler nel Golfo) sono sempre più percepiti come asset strategici e potenziali target in scenari di escalation. Il rischio principale riguarda interruzioni operative o effetti indiretti sulla supply chain digitale. Danni fisici confermati.

Rischio Sottostimato

Data center cloud sono ora esplicitamente nel mirino IRGC. Supply chain cloud condivisa tra organizzazioni europee e target primari, con potenziale effetto a cascata su pagamenti, logistica e servizi pubblici.

Raccomandazioni

1. Completare asset inventory OT (Purdue Model + tool automatica).
2. Isolare OT da internet: zone/conduits IEC 62443 + data diode.
3. VA trimestrale su PLC esposti (priorità CISA AA23-335A).
4. Mappare dipendenze cloud di terze parti; architettura multi-provider.

PUBBLICA AMMINISTRAZIONE E DIFESA

RISCHIO ALTO

Vettore Primario

APT34/OilRig e APT42 (Charming Kitten) conducono campagne di spear-phishing e credential harvesting contro target governativi europei. Obiettivo: intelligence su politiche regionali, posizioni negoziali, contratti difesa e piani infrastrutturali.

Rischio Sottostimato

Molte PA europee restano su infrastrutture legacy e on-premises: profilo di rischio simile ai governi ME colpiti. L'accesso persistente APT su reti governative è la minaccia primaria.

Raccomandazioni

1. Cloud migration per dati critici su infrastrutture cloud sovrane UE.
2. MFA phishing-resistant su tutti gli accessi esterni e account privilegiati.
3. TI sharing con CSIRT nazionali su IoC APT34/MuddyWater.
4. Hunt forward proattivo con EDR/XDR e query TTP iraniani.

SETTORE DIFESA E INDUSTRIA

RISCHIO MOLTO ALTO

Vettore Primario

MuddyWater (MOIS) conduce operazioni sistematiche contro supply chain della difesa EU. Target documentati: contractor NATO, aziende aerospaziali, produttori di droni. Obiettivo: acquisizione IP sensibile.

Rischio Sottostimato

L'Europa, come produttrice di sistemi d'arma e tecnologie duali, è target primario per acquisizione di IP sensibile. Il rischio non è il sabotaggio ma l'esfiltrazione silenziosa di anni di R&D.

Raccomandazioni

1. Supply-chain risk assessment su fornitori Tier 1-3 con clausole CRA-compliant.
2. Certificazione Cyber Resilience Act + SBOM obbligatorio.
3. Segmentazione OT/IT e Zero Trust in ambienti produttivi (IEC 62443).
4. TI sharing con ASD ISAC / ACN-PSNC.

HACKTIVISMO/ DDoS/ PRESSIONE PSICOLOGICA

RISCHIO MEDIO ALTO

Vettore Primario

APT34/OilRig e APT42 (Charming Kitten) conducono campagne di spear-phishing e credential harvesting contro target governativi europei. Obiettivo: intelligence su politiche regionali, posizioni negoziali, contratti difesa e piani infrastrutturali.

Rischio Sottostimato

Molte PA europee restano su infrastrutture legacy e on-premises: profilo di rischio simile ai governi ME colpiti. L'accesso persistente APT su reti governative è la minaccia primaria.

Raccomandazioni

1. Cloud migration per dati critici su infrastrutture cloud sovrane UE.
2. MFA phishing-resistant su tutti gli accessi esterni e account privilegiati.
3. TI sharing con CSIRT nazionali su IoC APT34/MuddyWater.
4. Hunt forward proattivo con EDR/XDR e query TTP iraniani.

FATTORI LIMITANTI STRUTTURALI

Analisi dei fattori inibitori — overdetermination del fallimento: invertire uno o due fattori non avrebbe prodotto impatti diversi

Fattore limitante	Categoria	Importanza
Dipendenza da supply chain tecnologica soggetta a sanzioni: hardware, software commerciale, cloud.	Capacità tecnica	ALTA
Difese avanzate dei target primari (Israele, USA): investimenti pluriennali + intel sharing NATO.	Target resilienza	ALTA
Architettura digitale resiliente dei target EU: cloud adoption, segmentazione OT/IT, risposta post-NotPetya.	Target resilienza	ALTA
Frammentazione strutturale IRGC/MOIS/proxy: coordinamento limitato, senza dottrina unificata.	Struttura interna	ALTA
Assenza di dottrina offensive integrata con operazioni cinetiche: coordinamento principalmente opportunistico.	Dottrina operativa	MODERATA
Tendenza a operazioni ad alto profilo mediatico vs. effetti militari concreti: priorità alla narrazione.	Priorità strategica	MODERATA
Isolamento internazionale: Iran non beneficia di supporto tecnico comparabile a USA/UK verso Ucraina.	Ecosistema alleanze	MODERATA
Capacità di rigenerazione limitata dopo ops ad alta intensità: toolchain e infrastrutture bruciate.	Sostenibilità	MODERATA
Attribution rapida e pubblica: Iran è attore altamente monitorato — anonimizzazione difficile.	Attribution	MODERATA
Sanzioni limitano accesso a zero-day market e infrastrutture di anonimizzazione qualità.	Capacità tecnica	BASSA
Target primari hanno preparato contromisure specifiche su anni di esperienza contro Iran.	Target resilienza	BASSA
Interferenza reciproca tra attori: proxy con minor disciplina espongono capacità core.	Struttura interna	BASSA

DOTTRINA IRANIANA: JANG E ASHUB

Il ruolo della cyber nella strategia di conflitto permanente a bassa intensità

Nota metodologica: Il concetto di **"Jang-e-Ashub"** (guerra e caos) è utilizzato in questo report come **framework interpretativo**, non come una dottrina ufficialmente codificata dall'Iran. Il termine è ampiamente impiegato nella letteratura accademica e di sicurezza (tra cui analisi di Michael Eisenstadt, Mehdi Khalaji e studi della RAND) per descrivere l'approccio strategico iraniano. In questa prospettiva, **il cyber non rappresenta un dominio autonomo,** ma uno dei livelli di uno s**pettro di conflitto persistente e scalabile,** modulato in funzione della pressione geopolitica da esercitare.

ESCALATION CONTROLLATA

Deterrenza attiva senza trigger militare

All'interno di questo schema, la cyber viene utilizzata dall'Iran come strumento di **segnalazione strategica.** Operazioni come attacchi wiper contro target israeliani o sauditi servono a dimostrare capacità di risposta senza ricorrere a una proiezione militare diretta.

La logica operativa è **scalabile**: dalle campagne **DDoS** ad attacchi **wiper,** fino a potenziali operazioni su **ICS/OT**, con un livello di intensità calibrato sulle reazioni dell'avversario. In questo spettro, **la cyber rappresenta un livello intermedio di escalation**: più visibile e attribuibile delle attività dei proxy, ma meno destabilizzante di un'azione militare convenzionale.

GUERRA PSICOLOGICA AMPLIFICATA

La percezione della minaccia come arma strategica

Gruppi come **Emennet Pasargad e Handala** conducono campagne di influence operations in cui il cyber hanfunge da amplificatore comunicativo. Le operazioni di hack-and-leak non mirano tanto al valore dei dati sottratti, quanto alla **narrazione strategica** che ne deriva. Social media, canali Telegram coordinati e disinformazione amplificano l'impatto dell'operazione, in linea con la dottrina iraniana Jang e Ashub, che integra dominio informativo e cyber per influenzare la percezione pubblica e politica.

PRE-POSIZIONAMENTO STRATEGICO

Accessi dormienti come leva di coercizione

Attori come **CyberAv3ngers** e **Agrius** sono stati associati a compromissioni di sistemi **OT/ICS** negli Stati Uniti e in Israele (CISA AA23-335A). In molti casi l'obiettivo non sembra essere l'attacco immediato, ma il pre-positioning: accessi persistenti e dormienti che costituiscono una capacità di coercizione latente. Nel contesto europeo il rischio di dinamiche analoghe è considerato elevato per similitudine di esposizione tecnologica, sebbene non esistano evidenze pubbliche comparabili a quelle documentate negli Stati Uniti.

RACCOMANDAZIONI OPERATIVE

Azioni prioritarie calibrate sul profilo di minaccia documentato — ancorate a TTP specifici feb-mar 2026

Le raccomandazioni seguenti sono calibrate sul profilo di minaccia documentato in questo report, implementabili con risorse operative ordinarie, senza bloccare la continuità operativa. Ogni punto è ancorato a un TTP o attore specifico documentato nella finestra feb-mar 2026.

IDENTITÀ E ACCESSI PRIVILEGIATI

- **MFA adattivo su tutti gli accessi privilegiati e remote access — priorità:** account dominio, cloud admin, sistemi OT-adjacent. [TTP: MuddyWater/Dindoor, feb 2026]
- **Revisione service account e credenziali hard-coded:** MuddyWater usa credential stale per lateral movement silenzioso.
- **Modello Just-In-Time per amministratori:** nessun privilegio permanente, ogni sessione autorizzata on-demand e loggata.
- **Inventario strumenti RMM (AnyDesk, TeamViewer)**: ogni tool non gestito è potenziale vettore di persistenza (TTP MuddyWater).

SEGMENTAZIONE E SUPERFICI D'ATTACCO

- **Microsegmentazione progressiva:** separare OT/ICS dalla rete IT con policy esplicite. [TTP: Fox Kitten/UNC757]
- **Patching prioritario su VPN concentrator, firewall edge e appliance RA:** Fox Kitten opera quasi esclusivamente su Fortinet, Pulse Secure.
- **Verifica configurazione WAF su tutti i portali pubblici critici:** campagne DDoS hanno incluso bypass CDN documentati.
- **Monitoring DNS query log per beaconing e tunnel DNS:** APT34/OilRig usa DNS hijacking come tecnica primaria di esfiltrazione.

DETECTION E RISPOSTA

- **Copertura SOC H24 o escalation notturna strutturata sui sistemi critici:** profilo temporale attori iraniani = attività fuori orario EU.
- **Regole detection su PowerShell loader,** abuso RMM e spear phishing con lure geopolitici (sanzioni Iran, NATO).

- **Feed TI contestuale:** lead time medio 12-24h tra claim Telegram e attacco verificato. Monitorare canali Cyber Islamic Resistance, DieNet, 313 Team.
- **Runbook per gestione claim pubblici:** strategia iraniana esagera gli impatti per forzare reazione mediatica.

FORMAZIONE E AWARENESS

- **Alert interno su spear phishing geopolitico verso profili LinkedIn esposti**: APT35/Charming Kitten impersona figure in difesa, energia, accademia.
- **Formare il personale sul vettore mobile: RedAlert APK (Unit 42, mar 2026)** replica app istituzionali di emergenza per installare spyware.
- **WezRAT (Cotton Sandstorm) impersona lo Israeli National Cyber Directorate:** verificare sempre i canali ufficiali prima di installare tool.
- **Partecipare ai CSIRT network EU e ai canali CISA/ENISA:** IoC sharing APT34/MuddyWater è il moltiplicatore difensivo più efficace a costo zero.

CONCLUSIONI ANALITICHE

Sintesi valutativa — cinque findings dall'analisi sistematica

Le cyber operations iraniane presentano una dicotomia fondamentale tra narrazione e realtà operativa: sono tra le più visibili e mediaticamente amplificate nel panorama della minaccia globale, ma il loro impatto strategico concreto è sistematicamente inferiore alle proiezioni tradizionali.

01 OPERAZIONI CYBER OFFENSIVE: impatto sistematicamente sopravvalutato

Le operazioni cyber offensive iraniane non hanno finora raggiunto la soglia di impatto strategico necessaria a modificare equilibri militari. Ogni analisi che le posiziona come arma decisiva in un conflitto regionale è probabilmente distorta da bias di sovrastima del cyber rispetto agli strumenti proxy e cinetico-missilistici.

02 RACCOLTA INTELLIGENCE: il vero centro di gravità

La raccolta di informazioni strategiche tramite operazioni cyber è il vero vettore strategico. Le organizzazioni europee dovrebbero riorientare gli investimenti difensivi verso rilevamento di APT persistenti, threat hunting proattivo e protezione della proprietà intellettuale — non solo verso prevenzione di attacchi distruttivi.

03 IL MODELLO DIFENSIVO UCRAINO È TRASFERIBILE

Cloud migration, endpoint protection AI-based, threat intelligence condivisa tra pubblico e privato: è il paradigma di riferimento. Le sue lezioni sono trasferibili direttamente al contesto europeo con gli adattamenti necessari per il quadro normativo NIS2 e normative nazionali.

04 FINESTRA DI RISCHIO: prossimi 30-45 giorni — scenario

L'escalation in corso (marzo 2026) crea condizioni favorevoli ad attività cyber opportunistiche, raccolta intelligence e signaling. I danni AWS in UAE/Bahrain (1 mar 2026) evidenziano che i data center rientrano ormai tra gli asset digitali esposti al conflitto ibrido. Assessment UCA: probabilità elevata di attività cyber reattiva su EU nel breve periodo.

05 FRAMMENTAZIONE ATTORI: limite e fattore di incertezza

La frammentazione IRGC/MOIS/proxy è limite operativo e fattore di incertezza per i difensori. Comportamenti anomali dei proxy possono precedere o mascherare operazioni più sofisticate degli APT statali. Monitorare i proxy come early warning dei team principali.

OUTLOOK
PROIEZIONE RISCHIO 30-45 GIORNI

Orizzonte: Aprile 2026 — scenari probabilistici calibrati su intensità escalation, finestre operative e pattern storici

Le proiezioni seguenti sono scenari probabilistici, non previsioni deterministiche. La probabilità assegnata è calibrata su: intensità dell'escalation attuale, finestre operative documentate e pattern storico delle cyber operations iraniane.

Scenario (30-45 Giorni)	Prob.	Razionale / Indicatori
Intensificazione spear phishing su PA e difesa EU (Lure: sanzioni Iran, dossier nucleare, NATO)	ALTA	Indicatori OSINT coerenti con cluster compatibili APT34/MuddyWater. Assessment UCA, confidenza MEDIA.
Campagna influence ops su narrative conflitto Iran-USA (Target: opinione pubblica EU)	ALTA	Meccanismo automatico. Proxy già attivi su Telegram e social media. Documentato nel pattern Feb-Mar 2026.
DDoS coordinato su target EU e NATO (Cyber Toufan, Holy Souls, NoName057-affiliati)	ALTA	Gruppi proxy già operativi. Distribuzione narrative false in parallelo. Impatto tecnico limitato, psicologico elevato.
Wiper/ransomware su target israeliano o UAE come ritorsione	MEDIA	Agrius ha capacità dimostrate. Pattern storico: follow-on cyber entro 7-14 giorni da eventi cinetici significativi.
Pre-posizionamento OT/SCADA in reti EU (Attivazione improbabile senza escalation cinetica)	MEDIA-BASSA	Rischio monitoraggio proattivo raccomandato. Evidenze USA presenti (CISA AA23-335A), EU per analogia.
Operazione cyber su infrastruttura cloud UE (Rischio indiretto via supply chain)	BASSA-MEDIA	Il precedente AWS UAE/Bahrain eleva il rischio teorico. Target primari restano USA/Israele/ME.

ASSESSMENT UCA — LIVELLO DI ALLERTA: ALTO per i prossimi 30-45 giorni

» **Priorità operativa: threat hunting su IoC MuddyWater/APT34; verifica pre-posizionamento su accessi legacy e supply chain digitale. Monitorare canali Telegram proxy iraniani come early warning.**

CHI SIAMO

ZENITA GROUP

Zenita Group nasce dall'incontro di realtà imprenditoriali italiane leader nei rispettivi mercati, con l'obiettivo di creare un polo di eccellenza nei settori di Digital Engineering, Defense, Intelligence & Security e Smart Platforms in Italia e di esportare tecnologie innovative anche all'estero.

Ciascuna azienda del Gruppo opera in ambiti strategici differenti e complementari, favorendo lo sviluppo di una visione all'avanguardia, che valorizza le competenze distintive di ogni realtà.

Dalla progettazione e gestione di infrastrutture digitali critiche alla digitalizzazione dei processi per la PA, dalle piattaforme cloud a sistemi di supporto per la difesa e la sicurezza nazionale, Zenita Group integra competenze specialistiche e capacità industriali per accompagnare la trasformazione digitale in Italia e all'estero, garantendo resilienza e sicurezza a istituzioni, imprese e cittadini.

MATICMIND - ZENITA GROUP

Maticmind, parte di Zenita Group, è uno dei principali system integrator italiani nel settore ICT, con quasi vent'anni di esperienza nell'innovazione digitale e nella sicurezza delle infrastrutture critiche. La società supporta organizzazioni pubbliche e private – tra cui telco, grandi gruppi bancari e istituzioni nazionali – nella progettazione, integrazione e gestione di soluzioni tecnologiche complesse, garantendo continuità operativa e affidabilità.

L'offerta di Maticmind copre sette aree strategiche: Networking, Data Center, Cloud, Cyber Security, Digital Workplace, Enterprise Applications e IoT & Automation. Queste sono supportate da un portafoglio di servizi professionali e gestiti, pensati per accompagnare i clienti dalla consulenza strategica all'ingegneria delle soluzioni, dall'implementazione al supporto post-vendita, fino alla gestione operativa quotidiana.

Maticmind consente ai propri clienti di affrontare con fiducia la trasformazione digitale, riducendo i rischi, ottimizzando le performance e proteggendo i dati critici in un contesto digitale sempre più complesso e minaccioso.

Cinque centri di competenza, un'unica forza cyber

1

Centro strategico per l'analisi e gestione del rischio cyber: governance, compliance, modelli di maturità, supply chain security posture.

- Offensive Security
- Consulting Services (CisoasaService, PM,..)
- Governance, Risk e Compliance
- Social Engineering Simulation
- Risk Assessment
- Maturity Model checkup
- Supply Chain Security Posture
- Cyber Academy

2

Continuità operativa e sicurezza in tempo reale assicurata da presidio operativo che integra SOC H24, con le capacità tecniche del TAC e il controllo infrastrutturale del NOC. Garantisce un monitoraggio continuo, una risposta tempestiva agli incidenti e un supporto tecnico evoluto.

- **SOC (Security Operation Center)**
  - SOC H24
  - Cyber Threat Intelligence
  - Malware Analysis
- **SOS (SECURITY OPERATION SERVICES)**
  - Crisis Management
  - IncidentResponse & Digital Forensic Analysis
- **TAC (Technical Assistance Center)**
  - Gestione di ticket e supporto tecnico avanzato
  - Assistenza su soluzioni proprietarie e terze parti
  - Troubleshooting di sicurezza e infrastruttura
  - Supporto su incidenti tecnici e configurazioni complesse
- **NOC (Network Operation Center)**
  - Monitoraggio infrastrutturale H24
  - Supervisione performance di rete, cloud e sistemi
  - Gestione allarmi e segnalazioni
  - Coordinamento tecnico con il SOC in caso di anomalie

3

Esecuzione ed implementazione di progetti complessi di sicurezza: infrastrutture, cloud, OT/IoT, application security e integrazione di soluzioni cyber.

- Infrastructure & Network Security Management
- Cyber Resiliency e Data Protection
- Microsoft, Fortinet & CISCO Competence Center
- Cloud Security By Design
- Application Security SSDLC
- OT & IoT Security Management
- Security System Integration and Monitoring

4

Gestione e integrazione di soluzioni proprietarie e tecnologie di terze parti: piattaforme EDR, firewall, IAM, SIEM, DLP.

- Piattaforma Twin4Cyber
- Cyber Range
- WiseView - Risk Management Platform
- SIEM/SOAR
- EDR/XDR/NDR
- Identity & Access Management (IAM/PAM)
- NGFW
- Data Loss Prevention

5

Progetti speciali e sperimentazione: architetture avanzate, droni, AI, cyber-physical systems, prototipi e soluzioni non convenzionali.

- Architetture avanzate multi-layer e ibride
- Sistemi di comando e controllo per droni e UAV
- Integrazione AI in contesti cyber e sicurezza industriale
- Progetti su ambienti cyber-physical / smart infrastructure
- Soluzioni sperimentali
- Cyber testbed per ambienti OT e industriali
- Soluzioni cyber per difesa e protezione civile
- Soluzioni sperimentali edge & fog computing.

NOTE LEGALI E CLASSIFICAZIONE

CLASSIFICAZIONE: USO RISTRETTO — CONFIDENZIALE

Il presente documento è classificato USO RISTRETTO ai sensi delle policy interne di Maticmind – Zenita Group.

La distribuzione è limitata ai soggetti espressamente autorizzati. Ogni riproduzione o divulgazione non autorizzata è vietata.

LIMITAZIONI ANALITICHE

Le valutazioni sono basate su fonti open source, advisory pubblici di CISA, MSTIC, Mandiant, ENISA e analisi propria di Maticmind alla data di pubblicazione (07 marzo 2026). L'attribuzione di operazioni cyber a specifici attori statali è espressa con gradi di confidenza (ALTA/MEDIA/BASSA) in conformità con metodologie standard di threat intelligence. Le proiezioni di rischio a 30-45 giorni sono scenari probabilistici, non previsioni deterministiche.

TUTELA DEI DATI PERSONALI

Il documento non contiene dati personali di individui identificabili. Il trattamento dei dati è effettuato in conformità al Regolamento UE 2016/679 (GDPR) e al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

PROPRIETÀ INTELLETTUALE

Il contenuto analitico, la struttura metodologica, i framework valutativi e la presentazione del presente documento sono proprietà intellettuale di Maticmind. In caso di citazione autorizzata, indicare alla fonte: "Una Cyber Acies — Threat Intelligence Division, UCA-TI-2026-003, Marzo 2026".

ZENITA
GROUP

UNA CYBER ACIES

WWW.ZENITAGROUP.COM