INTELLIGENCE BRIEFING
NATIONAL SECURITY RISK MONITOR

SETTIMANA: 24 - 30 NOVEMBRE 2025

Analisi tattica degli scenari geopolitici, minacce cyber e impatti sulla sicurezza industriale.

WWW.SQUADSMPD.COM

SITUATION REPORT

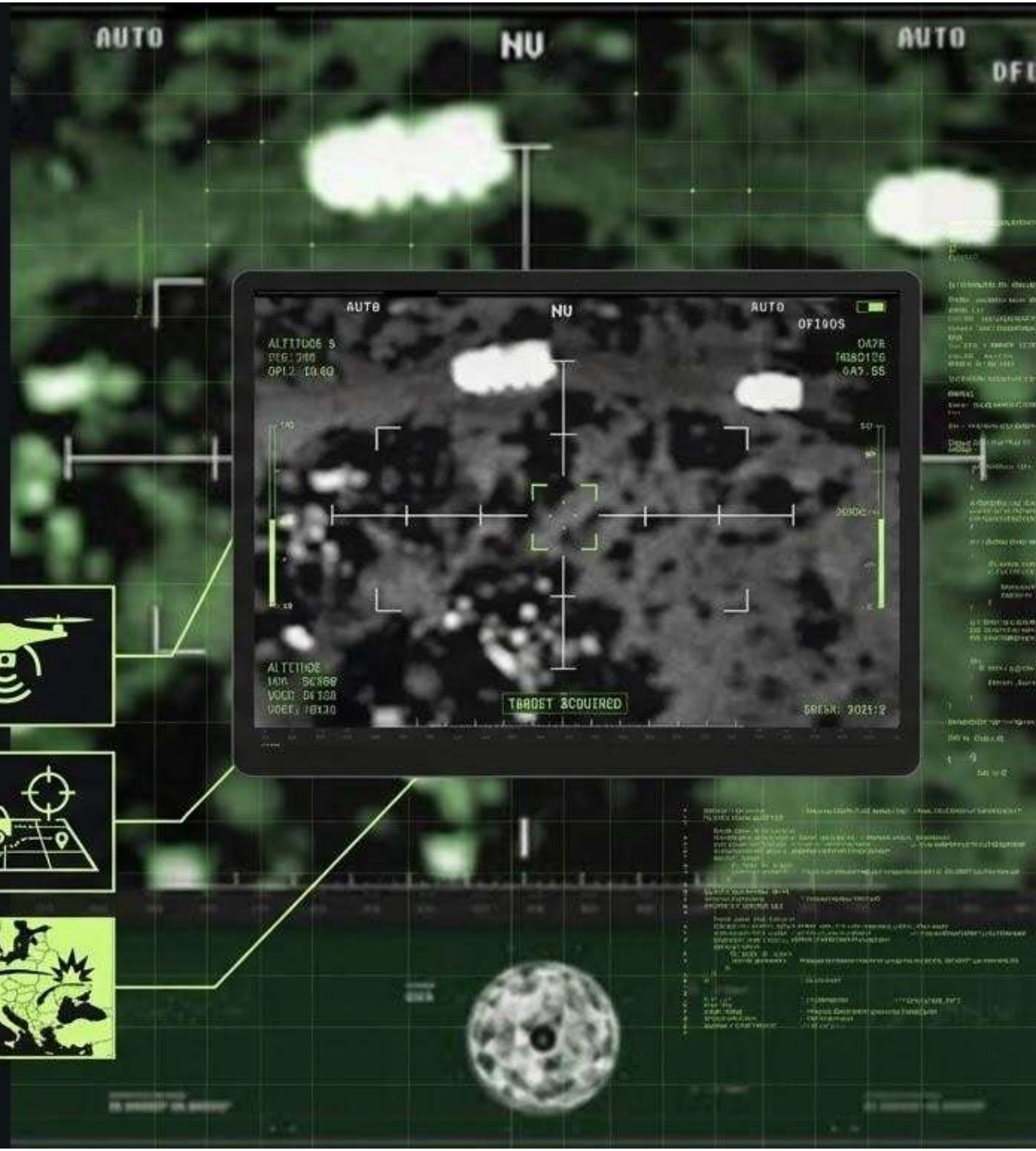
LIVELLO DI RISCHIO: ALTO

La settimana segna una **convergenza critica** tra **conflitti cinetici** ad alta intensità e guerra ibrida.
Le tensioni non sono più compartimenti stagni: l'escalation militare influenza direttamente la sicurezza energetica e la resilienza delle infrastrutture IT.

FRONTE EST: SHIFT TATTICO

Il settore di **Pokrovsk** è il nuovo epicentro. Le intelligence europee confermano un cambio radicale nella dottrina di difesa ucraina.

- **Supremazia dei Droni:** La richiesta di munizioni d'artiglieria è superata dalla domanda di sistemi FPV.
- **Guerra di Logistica:** I target non sono più solo al fronte, ma nelle retrovie produttive.
- **Rischio Europa:** Elevata probabilità di sabotaggi fisici contro le linee di rifornimento occidentali.



MEDIO ORIENTE: ESCALATION QUALITATIVA

RAID IN PROFONDITÀ

Non più scaramucce di confine. L'IDF ha esteso il raggio d'azione con oltre 14 raid aerei su **Baalbek e Tiro**, colpendo la catena di comando strategica.

THREAT ASSESSMENT

L'indebolimento della struttura convenzionale aumenta paradossalmente il rischio di **terrorismo asimmetrico** contro obiettivi occidentali (Soft Targets) al di fuori del teatro operativo.

INDO-PACIFICO: PREPARAZIONE AL 2027

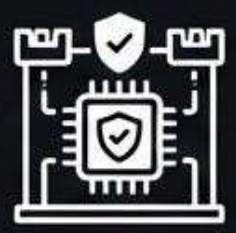
Taiwan annuncia un investimento storico in risposta ai segnali di intelligence su una possibile finestra di invasione nel 2027.

$40B

EXTRA BUDGET DIFESA

› Impatto Supply Chain

Le aziende tech devono accelerare i piani di decoupling.



› Resilienza

Focus su stoccaggio strategico di componenti critici.

CYBER WARFARE: Q4 2025 DATA

70%

Degli attacchi nell'ultima settimana hanno mirato a Infrastrutture Critiche (Energia, Manifatturiero).

$10M+

Costo medio per Data Breach. Un record storico che riflette la sofisticazione degli attacchi Ransomware.

AI DRIVEN

L'IA è il nuovo standard per il phishing. I Deepfake audio vengono usati per autorizzazioni fraudolente.

LA MINACCIA INVISIBILE: SOCIAL ENGINEERING 2.0

Gruppi state-sponsored (es. Storm-2603) stanno utilizzando l'IA per infiltrare le aziende occidentali.

La tecnica emergente consiste nel piazzare **falsi dipendenti IT** o usare deepfake durante i colloqui per ottenere accessi privilegiati dall'interno.

⚠ Settori a rischio: Manifatturiero (26%) ed Energetico (10%).

CLIMATE SECURITY & ECONOMIA

I disastri naturali non sono più solo eventi ambientali, ma vettori di instabilità economica e vuoti di potere.

CALIFORNIA

Danni >$20 mld. Impatto diretto su infrastrutture abitative e agricole.

VIETNAM

Alluvioni bloccano hub manifatturieri critici per l'elettronica.

RACCOMANDAZIONI OPERATIVE

TRAVEL SECURITY

Limitare viaggi non essenziali in Medio Oriente e zone di confine Est Europa. Attivare protocolli di estrazione rapida.

CYBER RESILIENCE

Implementare verifiche **"Out-of-Band"** (canale secondario) per ogni richiesta finanziaria urgente per contrastare i Deepfake.

SUPPLY CHAIN

Audit immediato dei fornitori di elettronica esposti all'area Taiwan. Aumentare lo stock di materie prime energetiche.

Q&A

BestPractices del:

dott. BORGESE Francesco

"La sicurezza non è l'assenza di pericolo,
ma la presenza di misure di mitigazione."

WWW.SQUADSMPD.COM