

GLOBAL OSINT DOSSIER — 2026

What Actually Matters

Strategic Overview

2026 is defined by convergence: AI and cyber operations dominate, great power competition is continuous, and non-state actors now possess state-like capabilities. Infrastructure is the primary battlefield.

AI as a Geopolitical Force Multiplier

AI is embedded in intelligence workflows and enables autonomous cyber capabilities. It lowers barriers to entry and redistributes power to smaller actors.

Cyber Conflict

Cyber operations are persistent and target critical infrastructure. Malware is pre-positioned for future conflict, making cyberspace an active war domain.

Great Power Competition

China, Russia, and the United States are engaged in multi-domain competition across economic, military, and technological fronts.

Transnational Crime

Criminal networks are merging with cyber capabilities and financial systems, creating hybrid threats that destabilize nations.

Information Warfare

Disinformation and AI-generated narratives are shaping public perception and undermining trust in institutions.

Infrastructure Risk

Energy, telecom, and supply chains are increasingly fragile due to interdependence and cyber vulnerabilities.

Cross-Domain Synthesis

AI, cyber, and crime are converging. Infrastructure fragility and decentralized power are defining risks.

Top Risks

1. AI-driven cyber escalation 2. US-China tech decoupling 3. Infrastructure collapse 4. Criminal-state hybrid networks 5. Information warfare escalation

Recommendations

Shift to resilience, integrate intelligence systems, harden infrastructure, monitor non-state actors, and control information environments.