PALANTIR TECHNOLOGIES

The Architecture of Total Information Surveillance

INTELLIGENCE ASSESSMENT

Palantir Technologies:

The Architecture of Total Information Surveillance

Classification:	Declassified – Analytic/Educational Purposes
Subject:	Artificial Intelligence
Region:	Global

Executive Summary

Co-founded in 2003 by Peter Thiel, Alex Karp, Joe Lonsdale, Stephen Cohen, and Nathan Gettings with seed capital from the CIA's In-Q-Tel, Palantir Technologies has evolved from a secretive counter-terrorism data-mining contractor into the world's most pervasive artificial intelligence-driven infrastructure company. As of Q1 2026, Palantir operates across five continents, holds contracts with more than 30 governments, with its software simultaneously touching defense, intelligence, law enforcement, border security, national health services, and commercial enterprises. Its fiscal year 2025 revenue reached $4.5 billion, growing 29% year-on-year, with the US government revenue alone exceeding $1.3 billion.

This intelligence assessment provides a structured analysis of Palantir's full product architecture, global deployment footprint across countries, cities and government departments, the value addition it delivers to clients, and the systemic risks – civil libertarian, geopolitical, technological, and ethical – that its model of "total information awareness" introduces into democratic governance structures worldwide.

CommandEleven's core understanding – Palantir has constructed an unprecedented private-sector nervous system for the modern state, removing the requirement of human interaction in the decision-making process. This same platform architecture save patients, guides Ukrainian drone targeting, tracks undocumented immigrants, and monitors global supply chains, while also being the most advanced surveillance and kill-chain facilitation apparatus ever deployed outside classified government systems.

The value is real. The risk is existential.

Company Background and Platform Architecture

Palantir's founding is inseparable from the post-9/11 national security environment. When Peter Thiel invested $30 million, which was followed by a significantly larger investment from the CIA's In-Q-Tel venture capital arm, it was clear Palantir's core clients would be intelligence agencies with needs commercial software could not satisfy – connecting disparate databases, identifying patterns in "noise," and supporting operations where mistakes cost lives. True to form, early clients included the CIA, NSA, FBI, and Special Operations Command. Palantir did not just build software, it embedded engineers, known as forward deployed engineers (FDEs), directly inside client organizations for months or years, creating interdependencies that would provide the greatest sale strength and a significant systemic risk.

When Palantir went public on the New York Stock Exchange in September 2020, via direct listing, it was valued at approximately $15.8 billion. By early 2026, market capitalization has exceeded $200 billion, reflecting investor conviction that AI-driven government software is one of the century's largest addressable markets.

Palantir's Strategic Model

Understanding Palantir's competitive position requires understanding its core technical innovation. Unlike conventional databases or data leaks, Palantir creates a semantic model of the real model – translating data into Objects (a person, a vehicle, an event, a shipment), Properties (attributes), Links (relationships), and Actions (what can be done). Once an organization's data is modelled inside Palantir, every new dataset enriches the same semantic graph rather than creating silos.

A defense customer might connect a satellite image of a vehicle to a signals intelligence intercept, to a database of known individuals, to a historical movement pattern, to a targeting decision workflow – all in one coherent interface. A healthcare customer connects a patient record to admission history, available beds, surgical schedules, and discharge planning. The model is the lock-in mechanism, which once built, it is extraordinarily costly to migrate away from, because the embedded knowledge cannot be easily exported to a competitor system.

Palantir's Full Product Line

The Palantir product line is spread widely across numerous mission-critical industries, which when viewed from a macro-perspective, giving them insight into the lives of every individual in the nations they operate.

Palantir's monitoring systems are based on seven core applications – Gotham, Foundry, Apollo, Artificial Intelligence Platform (AIP), Maven Smart System (MSS), ImmigrationOS, and Hospitals – which are the foundation for the remaining suite of products in various industries.

Palantir Gotham – The Intelligence and Defense Operating System

Gotham is Palantir's original platform, designed explicitly for government and defense intelligence operations. Palantir's own marketing collateral describes it as a "weapons system" and an "Operating System for Global Decision-Making." Gotham is able to:

- multi-source data from satellite imagery, signals intelligence, human intelligence reports, financial data, and communications metadata
- cross-database entity resolution
- network analysis
- geospatial mapping with temporal playback
- investigation case management

In the 2024-2026 iteration, Gotham has expanded to include:

- AI-enabled kill chain integration, supporting target identification and pairing for kinetic military operations
- autonomous sensor tasking – directing drones and satellites via AI-generated rules or human-in-the-loop commands
- mixed reality command interfaces – transforming any physical space into a digital operations center
- multi-domain operations support across land, sea, air, space, and cyber simultaneously

Gotham's primary customers are the United States Army, Air Force, Navy, Marine Corps, Southern Command (SOCOM), NGA, DIA, Space Command; the UK Ministry of Defence; the Israeli Ministry of Defence; NATO, and all Five Eyes military services.

Palantir Foundry – The Enterprise Data Operating System

Foundry was Palantir's pivot toward the commercial market in 2016. Positioned as the "Operating System for the modern commercial enterprise," it serves large enterprises including manufacturers, health care systems, financial institutions, and government agencies with operational needs.

Foundry features 200+ pre-built connectors into every business intelligence application, an Ontology-powered data modelling layer, a low-code/no-code application builder (Workshop), advanced analytics (Python, R, SQL), and AI/machine language (ML) model deployment pipelines that allow trained models to operate directly on live operational data.

Foundry's primary customers are AirBus, British Petroleum (BP), Ferrari, NHS Federated Data Platform, US Army's Army Vantage, Southern California Edison, HCA Healthcare, Mount Sinai, and Tampa General Hospital.

Palantir Apollo – The Deployment Infrastructure Layer

Apollo is the least publicly discussed, but arguably most strategically important platform. It is a continuous delivery and deployment system managing the updating, monitoring, and security of Gotham and Foundry across every environment – cloud, on-premise, air-gapped classified networks, tactical edge deployments (on ships, forward operating bases (FOBs), and aircraft), and disconnected battlefield systems.

Apollo facilitates push software updates to a classified military network in Germany, an NHS server room, and a commercial cloud in Singapore simultaneously, securely and without local IT management involvement. It also enforces security governance protocols, including access controls, classification labels, audit trails, and compliance monitoring, automatically across all environments.

Palantir AIP – The Artificial Intelligence Platform

Launched in 2023, AIP is the orchestration later for the Large Language Models (LLMs) and other AI systems operating on live operational data. Unlike generic LLMs, AIP enables organizations to deploy LLMs directly against their own proprietary data – the same data modelled in their Foundry and Gotham Ontology.

AIP components include:

- AIP Logic – a workflow builder connecting AI agents to real-world actions
- AIP Now – a marketplace of pre-built AI applications
- AIP Assist – natural language platform navigation
- AIPCon – annual customer showcase

In a military context, AIP provides the natural language and automated reasoning layer on top of Gotham's data integration with the Maven Smart System.

Maven Smart System (MSS) – The Military AI Flagship

Originally launched as Project Maven under a 2017 Department of Defense contract, MSS is now the United States military's primary AI-enabled intelligence and targeting platform.

The Maven Smart System capabilities include:

- AI-enabled battlespace awareness
- global integration – connecting geographically dispersed intelligence into a single picture
- force management
- contested logistics
- joint fires integration – connecting targeting recommendations to weapons systems

MSS sub-components include:

- MSS Global Integration – connecting intelligence and operational data from geographically dispersed forces into a single, unified operational picture for combined joint all-domain command and control
- MSS Force Management – real-time tracking of friendly force locations, status, equipment readiness, and personnel across theatres
- MSS Contested Logistics – AI-powered supply chain management under adversarial condition – routing, demand forecasting, and resupply prioritization
- MSS Joint Fires – integration between targeting data and weapons systems – the module that connects AI-generated targeting recommendations with the weapons systems
- MSS Space Integration – connecting space-based sensor data – satellite imagery, signals, missile early warning) into the ground-level operational picture

ImmigrationOS – The Enforcement Surveillance Product

ImmigrationOS represents Palantir's most controversial expansion. Contracted in April 2025 from $30 million for United States Immigration and Customs Enforcement (ICE), functioning as a comprehensive surveillance and targeting system for immigration enforcement.

ImmigrationOS aggregates data from DHS databases, HHS records (including Medicaid data), social media monitoring, biometric databases, and movement tracking to create profiles of undocumented immigrants. Its ELITE sub-module generates deportation target lists and provides "near real-time visibility" on self-deportees.

The ELITE sub-module generates prioritized target lists for ICE Enforcement and Removal Operations field offices, aggregates data across DHS, HHS, social media, and location databases to produce ranked deportation leads with supporting evidence packages for ICE field agents.

In February 2026, the Department of Homeland Security had signed a $1 billion agreement covering ICE, CBP, TSA, FEMA, CISA, and the Secret Service.

Palantir for Hospitals – The Healthcare Product

Palantir for Hospitals is a branded vertical built on Foundry with capabilities to AI-powered nurse scheduling and staffing, transfer center optimization, discharge management, and surgical theatre scheduling. The platform interfaces with Epic and Cerner hospital systems.

Complete Inventory of Integrated Military Products

Beyond the core Gotham/AIP/MSS triad, Palantir has developed multiple military products that represent discrete capability offerings within the defense ecosystem.

Tactical Intelligence Targeting Access Node (TITAN)

The US Army's next-generation AI-enabled intelligence ground station – a mobile, truck-mounted platform that integrates AI/ML processing of multi-domain sensor data – space, aerial and ground – to identify, track, and generate targeting solutions for time-sensitive targets. Working in coordination with MSS, TITAN is able to compress the targeting cycle from intelligence collection to fire mission by integrating satellite imagery, signals intelligence, and ground sensor data into a single AI-processed targeting solution.

Army Vantage

The Army's data analytics platform, connecting 30,000+ datasets and 180+ systems, creating a 360° view of Army operations, logistics, personnel, and readiness. Army Vantage is capabilities include:

- AI-enabled workflows for maintenance predictive analytics
- personnel readiness forecasting
- financial obligation tracking
- supply chain visibility

Skykit

A fully autonomous, disconnected edge intelligence system – a mobile intelligence center in a box – designed for frontline battlefield use where network connectivity is unavailable or compromised

- confirmed operations with Ukrainian Armed Forces, allowing soldiers to task sensors, analyze imagery, and process intelligence without dependence on base network links
- capable of self-contained AI processing for imagery, analysis, pattern-of-life assessment, and situational awareness at the squad/platoon level

MetaConstellation

An AI-powered satellite constellation management software, which integrates with commercial and government satellite assets to provide persistent surveillance over areas of operations.

- capable of automatically re-tasking satellite imaging assets based on AI-defined collection properties, measure changes over time to detect activity patterns, triggers more focused collection when anomalies are detected
- for the military, it provides the space-based intelligence layer that feeds TITAN and MSS targeting workflows, and is especially relevant for targeting time-sensitive mobile targets where persistent overhead surveillance is required

ShipOS – Naval Shipbuilding Platform

Palantir's Foundry-based platform customized for United State Navy shipbuilding and maintenance operations across public and private shipyards.

- capable of material review board digitalization, maintenance scheduling, supply chain visibility for complex naval platforms, and workforce management

Mission Manager

A secure software ecosystem that enables government agencies and prime contractors to deploy, manage, and monitor third-party vendor applications within classified environments

Sensor Inference Platform (SIP)

An edge AI processing platform that ingests and analyzes sensor data, particularly electro-optical and infrared imagery, in real-time at the point of collection, enabling precision targeting by processing airborne sensor data with AI before transmission to ground stations.

Warp Speed

Palantir's manufacturing operating system for the defense industrial base to accelerate and scale the production system for wartime of munitions, drones, and platforms, streamlining defense manufacturing, supply chain coordination, quality management, and production scheduling.

Gotham Mixed Reality Command

An augmented interface that transforms physical spaces into digital operations centers, by projecting Gotham's operational picture – maps, force positions, sensor feeds, and targeting data – as a 3D overlay in physical space, enabling commanders to walkthrough battlefield data, rather than view it on flat screens.

Complete Inventory of Integrated Law Enforcement Products

Palantir's law enforcement product portfolio has evolved from a single Gotham deployment into a differentiated suite of products and regional variants, deployed across police forces in the United States, United Kingdom, and continental Europe.

Palantir Gotham – Law Enforcement Edition

The core platform adapted for police and intelligence agency use, integrating police records, criminal databases, court records, financial intelligence, communications data, vehicle registrations, and open-source intelligence into a single investigation environment.

Key modules:

- Investigation Management – case-building and evidence tracking
- Network Analysis – mapping criminal associations
- Geospatial Analysis – place-based crime analysis and movement tracking
- Timeline Analysis – reconstructing event sequences
- Document Intelligence – automated document processing and entity extraction

Palantir Gotham Europa

A region-specific variant of Gotham designed for European law enforcement agencies, incorporating GDPR compliance and EU-specific data governance requirements.

Regional deployments include:

- VeRA (Vernetztes Recherche- und Analysewerkzeug / Overlapping Systems Research and Analysis Platform) — Bavaria State Police (Bayerische Landespolizei)
- HessenData — Hesse State Police (Hessisches Landeskriminalamt), Frankfurt
- DAR (Datenanalyse-Recherche / Data Analysis Platform) — North Rhine-Westphalia State Police (LKA NRW), Düsseldorf
- Baden-Württemberg State Police
- Norwegian National Police

NECTAR

Palantir's AI-powered digital evidence analysis tool for complex criminal investigations, able to automatically translate languages of seized devices and communications, image and video analysis, association chart generation, and data volume processing at scale.

IMMIGRATIONOS AND ELITE (DISCUSSED ABOVE)

PALANTIR INTELLIGENCE MANAGEMENT (PIM)

Palantir's law enforcement intelligence community product, which operates as an interface between the police operational intelligence and national intelligence agency data, enabling police to both query and contribute to national intelligence databases.

PALANTIR FOUNDRY (LAW ENFORCEMENT ANALYTICS DEPLOYMENTS)

Foundry (LEAD) is used for strategic analytics, performance management, and resource allocation, rather than frontline investigation support. The London Metropolitan Police uses Foundry (LEAD) to analyze officer sickness patterns, overtime usages, absence records, and performance data implementing algorithms to flag officers at risk of misconduct – "automated suspicion."

Global Deployment – Countries, Cities and Departments

The United States

- United States Army – Pentagon/Fort Belvoir/Global
- United States Air Force – Pentagon/Air Force Bases
- United States Space Force and Space Systems Command in el Segundo, CA
- United States Space Command – Peterson SFB, CO
- United States Special Operations Command – MacDill AFB, Tampa, FL
- United States Marine Corps – Quantico, VA/Global
- United States Navy/NAVSEA
- National Geospatial Intelligence Agency (Springfield, VA)
- Department of Homeland Security – ICE, CBP, TSA, FEMA, CISA, USSS
- ICE/ERO
- USCIS
- CMS/HHS – Baltimore, MD
- HCA Healthcare – Nashville, TN
- Mount Sinai Health System – New York City, NY
- Tampa General Hospital – Tampa, FL
- Cleveland Clinic – Cleveland, OH

The United Kingdom

- Ministry of Defence
- Atomic Weapons Establishment – Aldermaston, Berkshire
- GCHQ – Cheltenham, Gloucestershire
- NHS England
- Metropolitan Police
- Leicestershire Police
- East of England Police – Cambridge
- Coventry City Council
- Cabinet Office – Whitehall, London
- DEFRA – London

UKRAINE – THE AI WAR LABORATORY

Ukraine is the most active live war-zone deployment of Palantir's platforms, described by many as Palantir's AI War Laboratory, where targeting workflows, sensor fusion, and kill chain processes are tested at operational scale.

- Ministry of Digital Transformation – Kyiv – reconstruction planning and refugee resettlement management
- Ministry of Economy – AI-powered demining prioritization – identifying highest-risk areas for clearance teams
- Ukrainian Armed Forces – Gotham-based battlefield intelligence, targeting, satellite imagery analysis, and bomb-proof school site selection
- State Emergency Service – Crisis and disaster response coordination

ISRAEL – STRATEGIC AI DEFENSE PARTNERSHIP

Israel has used Palantir since 2014, expanding its relationship in January 2024 specifically "in support of war-related activities."

- Israeli Defense Ministry – kill-chain data integration and targeting support for Gaza and Lebanon
- Unit 8200 – Data Science and AI Center – Palantir-derived tools for targeting decision support
- IDF Civil-Military Coordination Center – AI used to manage humanitarian aid delivery tracking in Gaza while NGOs were banned
- Lavander – the AI system used for human targeting, analyzing surveillance datasets to identify individuals suspected of being terrorist operatives. At one point, it identified 37,000 targets, based on communication patterns, and membership in specific online groups.
- Where's Daddy? – tracking system that monitors individuals flagged by Lavander, automating track and target phases of the kill chain
- The Gospel (Habsora) – an AI system that identifies objects and infrastructure as potential targets, dramatically accelerating the rate of target generation

Other Significant Deployments

- NATO – Brussels and Allied Commands – Maven Smart Systems
- Germany – Bundeswehr modernization
- France – Total Energies
- Australia – AUSTEO-level defense level deployments under Five Eyes framework
- Japan – Undisclosed JSDF intelligence contracts
- United Arab Emirates – Government analytics contracts
- Colombia – Counter-narcotics intelligence support

Risk Assessment

Understanding the systemic risk of deploying a technology solution with the ability to not only monitor, but initiate a kill chain, against any individual for actions taken or not taken is imperative to understanding the risk being deployed.

In February 2026, Switzerland, during a contract termination, completed the most comprehensive risk assessment of the Palantir systems and the structural risk posed to any democratic state. Three categories of concern apply to any Palantir client.

Data Sovereignty and Vendor Lock-In

- Operational Dependency – Palantir's architecture, Forward Deployed Engineers (PDEs) embedded in client organizations, and Apollo-managed updates create institutional dependencies that make migration prohibitively. For national security clients, operational continuity cannot be interrupted for platform migration. Once a military or intelligence service's targeting workflows, intelligence databases, and analyst training are built around Palantir, the switching cost is existential.

- Foreign Legal Jurisdiction – as a US-incorporated company, Palantir is subject to the 2018 CLOUD Act, requiring US companies to provide government access to data, regardless of where it physically resides. For non-US clients, sensitive national security data – military targeting systems, healthcare records, police databases – is accessible to US government agencies through legal compulsion of Palantir. The UK's Palantir contracts are described as a "catastrophic surrender of data sovereignty."

- Systemic Concentration – Palantir is simultaneously embedded in healthcare, defense, border security, law enforcement, and energy. A catastrophic platform failure – from zero-day vulnerability, state-sponsored cyber-attack, corporate insolvency, or geopolitical rapture – would simultaneously impair multiple national critical systems.

Civil Liberties and the Surveillance State Architecture

Palantir's integrated surveillance capabilities represent the privatization of the surveillance state – a comprehensive social monitoring architecture controlled by a private company, accountable only to shareholders and not democratic governance.

Predictive policing in Gotham-based law enforcement deployments, known as "Minority State policing," has been documented to produce racially disproportionate outcomes through biased training data, feedback loops, and opacity. In simple terms, historical policing data over-represents minority communities, which facilitates AI attention at these same communities leading to more arrests because the algorithms used for targeting are not disclosed, stopping any legal challenges or correction of the algorithms.

ImmigrationOS has added a qualitatively new dimension to the risk model – health data weaponized for law enforcement. In January 2026, it was confirmed that ICE's ELITE tool incorporated Medicaid data as inputs for deportation targeting. The is precisely the kind of function creep privacy advocates have warned against. In May 2025, thirteen former Palantir employees publicly condemned the practice, with nationwide Purge Palantir protests in July 2025

In addition, Amnesty International's August 2025 report documented the use of social media sentiment analysis on international students to identify "terrorism-related content" by ImmigrationOS, identifying between 1,800 and 4,000 international students for visa revocation due to pro-Palestinian activism. Interestingly, the same algorithm is not used to identify real terrorism threats, based on the decades of profiles that have been developed by intelligence agencies via interrogations, incarcerations, and analysis, demonstrating the misuse of a tool to serve political objectives, rather than protect national security objectives.

Kill Chain Accountability and International Humanitarian Law

Palantir's role in AI-enabled military targeting raised fundamental humanitarian law questions, under the core principles of distinction methodology, proportionality, and precautions taken. While Palantir's systems accelerate targeting decisions, claiming to require formal human sign-off, satisfying the human-in-the-loop requirement – when AI processing thousands of targets per day, human review is cursory violating

the same requirement. Investigations have demonstrated AI generated targeting recommendations at a rate impossible for humans to scrutinize effectively. Lavender and Habsora (Gospel), Israeli applications of the Palantir technology in Gaza, generates a target list creating. Israeli Defence Forces (IDF) officials described the process – "we work quickly and there is no time to delve deep into the target. The view is that we are judged according to how many targets we manage to generate," and "a human eye will go over the targets before each attack, but it need not spend a lot of time on them."

While Palantir attempts to wash its hands – we only provide the platform, the client is responsible for the use – its own integration into the kill chain is more direct than weapons manufacturers, who have used the same argument in the past.

The developing danger is that as humans begin to rely on these systems, they become desensitized to the process and lose the ability to consider the risk of civilian harm in a meaning manner, literally creating mass assassination factories where civilian casualties no longer matter.

Who bears legal responsibility for civilian casualties from AI-assisted targeting still remains unresolved by any court or international treaty.

The Ideological Dimension

Peter Thiel – co-founder, board chair, and visionary behind Palantir – is one of the most influential figures in the tech-authoritarian movement – Silicon Valley billionaires who view democracy as an inefficient obstacle and see data-driven, AI-assisted state power as its successor.

Re-read that statement to better understand where the surveillance economy is traveling and how it is going to interact and affect every individual on the planet.

Thiel's political investments include funding J.D. Vance's Senate campaign and Vice-Presidential career. This alignment between Palantir's product evaluation – expanding ICE surveillance, supporting Israel's war in Gaza, and deepening military AI integration – and the Trump administration's agenda is not coincidental, rather is reflects a coherent worldview that the State's coercive capabilities should be technologically maximized and democratically unconstrained.

Strategic Implications and Assessment

CommandEleven's position on organizations like Palantir has been clear from the beginning – State power should never be outsourced to those who are not democratically elected or empowered. Without the umbrella of democracy, the power can be abused similar to an authoritative or dictatorial state. What is significantly worse is when a supposed democracy willingly hands that power to unelected individuals and organizations, more concerned with profit generation than the protection of the State.

Palantir represents the most advanced example of the outsourcing of the State's core coercive and intelligence functions to a private technology company. This categorically different from contracting for military equipment or IT infrastructure. Palantir is embedded in the decision-making process itself, with its engineers sit inside intelligence agencies, software that generates target lists, and platforms that produce outputs on which life and death decisions are made. When the State contracts Palantir, it grants a private company privileged access to the cognitive function of the State.

Palantir's simultaneous deployment across multiple allied government domains creates an intelligence aggregation risk of exceptional severity. A nation-state adversary, capable of compromising Palantir's core infrastructure, would simultaneously access US military targeting, UK national health records, Ukrainian battlefield positions, Israeli defense systems, and NATO alliance planning. No single government system, however sensitive, presents an equivalent aggregated target. Even US Intelligence Community guidelines specifically identify cross-domain information aggregation as a higher order threat than the compromise of any individual classified system.

What makes this real is that Palantir has been repeatedly breached by former employees, hackers and, most recently, by Kim Dotcom in February 2026.

Democratic accountability for state power requires that decision-making processes be visible to and contestable by the public and elected representatives. Palantir's architecture is structurally incompatible with this principle. The algorithmic logic embedded in targeting, policing, and immigration enforcement in proprietary – protected as trade secrets and unavailable for judicial review. When a court seeks

to understand why a deportation target was identified, or why a predictive policing algorithm directed officers to a particular neighborhood, the answer sits inside a private company's intellectual property. The rule of law is being systematically hollowed out.

Final Assessment

This intelligence assessment makes the following findings absolutely clear:

- **Capability** – Palantir's technical capabilities represent a massive leap in human decision support, facilitating improvements in military targeting speed, medical management, and logistical optimization
- **Architecture** – The structural lock-in is effectively irreversible at scale, as clients are not purchasing a platform or software, but surrendering a portion of their institutional cognitive function to Palantir's architecture
- **Risk Concentration** – Simultaneous deployment across defense, health care, law enforcement, and border security create systemic risk concentration. The aggregate risk profile is exponentially greater than the sum of individual risks
- **Accountability Deficit** – The transparency of Palantir's algorithmic decision-support in targeting, policing, and immigration enforcement is structurally incompatible with democratic governance norms and humanitarian principles
- **Geopolitical Exposure** – Non-US governments that have granted Palantir deep access to national security systems face geopolitical exposure unresolvable by contractual safeguards alone. The CLOUD Act combined with the ideological alignment between Palantir's leadership and the current US administration, creates a foreign intelligence exposure never seen or experienced before.

commandeleven

STRATEGIC INSIGHT. TACTICAL ADVANTAGE.

CommandEleven delivers counter-terrorism, intelligence, geopolitical risk analysis, and threat assessments for governments, corporates, and institutions operating in conflict-prone regions including MENA, South Asia, and Central Asia.

https://commandeleven.com