



Anti-Data Center & AI Opposition Elevating Civil Unrest

August 2026

This report is confidential and is intended solely for the information and use of the client to whom it is addressed. AT-RISK International, LLC does not guarantee the accuracy or completeness of outside agency records.

ANTI-DATA CENTER & AI OPPOSITION ELEVATING CIVIL UNREST

Global Risk Intelligence (GRI) analysts continue to observe intensifying anti-data center sentiment across the United States (U.S.), coinciding with growing concern among security professionals and federal authorities, including the Federal Bureau of Investigation, indicating that AI data centers are emerging as high-value targets in critical infrastructure. While successful physical attacks remain uncommon, organized protest activity, cyber threats, and the potential for sabotage targeting power and telecommunications infrastructure are contributing to an increasingly complex risk environment for data center operators, supporting utilities, technology companies, contractors, and public officials associated with data center development and expansion.

Recently, on 18 July, organizers coordinated 142 protests across 42 states, marking the first nationwide day of action against AI data center expansion, with protests occurring in rural communities and major metropolitan areas. According to a recent Reuters report, only 14% of Americans support the construction of a data center in their community, while approximately 70% oppose such developments. The growing apprehension around AI data centers is further addressed by cybersecurity experts, who warn that these facilities are increasingly targeted by both cyber and physical threats due to their critical role in national infrastructure. In response to these concerns, federal authorities are intensifying their engagement with operators to address a range of threats, including cyber intrusions, insider threats, sabotage, and potential disruptions to infrastructure.

A publicly available aggregated map identifies approximately 12,259 data centers worldwide, including roughly 4,767 in the U.S., 537 in Texas, 296 in California, and 276 in Georgia; the United Kingdom ranks second globally with 568. In the U.S., growing opposition to data center development has increasingly shaped both community activism and state policy. States including Texas, Virginia, and Pennsylvania have experienced heightened protest activity and public debate, while Maine, New York, Michigan, Georgia, Maryland, Oklahoma, South Carolina, South Dakota, Vermont, and Virginia have introduced related legislation. Virginia remains a particular focal point due to its status as a major data center hub and history of community resistance and legal challenges. Most recently, in July 2026, a Blackstone-owned data center project years in development was canceled following sustained local opposition and litigation.

GRI analysts have noted a significant rise in online discussions advocating for the sabotage or destruction of AI data centers. The Soufan Center, an independent non-profit, notes that physical sabotage has become one of the most discussed threats in online anti-AI communities, alongside threats targeting technology executives and policymakers. Anti-data-center activism has primarily involved peaceful protests, zoning issues, and political advocacy, but there's potential for escalation. While explicit threats are not as common, there's a rise in hostile rhetoric, including mentions of vandalism and violence toward data center infrastructure and personnel. As opposition grows nationally, key moments like project announcements and public hearings may increase the likelihood of disruptive actions.

Operational Considerations:

- Expand monitoring to identify emerging online rhetoric and protest activity targeting data centers or related events.
- Develop intelligence tracking permitting disputes, community opposition, litigation, and public meetings that may serve as indicators of escalating protest activity.
- Expand executive protection assessments for leaders associated with AI infrastructure to evaluate exposure.
- Strengthen information sharing with corporate security, cyber teams, law enforcement, and infrastructure partners.

DATA CENTER THREAT LANDSCAPE



NOTABLE SECURITY DEVELOPMENTS (2022–2026)

- DEC 2022** **Moore County Substation Attack (North Carolina)**
Attackers disabled electrical substations, leaving ~40,000 without power. Frequently cited as a benchmark for critical infrastructure vulnerability.
- MAR 2026** **AWS Data Centers Damaged During Iran Conflict**
Iranian drone strikes damaged AWS facilities in the UAE and affected infrastructure near a Bahrain facility. First confirmed military disruption affecting a major U.S. hyperscale cloud provider.
- APR 2026** **Increased Federal Security Engagement**
FBI and industry expanded outreach to operators as AI infrastructure gained greater recognition as critical infrastructure.
- JUL 2026** **Nationwide Anti-Data Center Protests**
Coordinated demonstrations occurred across dozens of states. Activity remained largely peaceful but reflected growing national organization against AI infrastructure projects.

KEY TREND: The environment is defined less by frequent attacks on facilities and more by growing strategic importance, infrastructure dependencies, and organized opposition.

GROWING PUBLIC OPPOSITION

- Nationwide Protests**
Demonstrations in 40+ states
July 18, 2026
- Community Concerns**
Noise, traffic, water usage, tax incentives, and zoning
- Environmental Impact**
High energy demand and cooling water consumption
- Political & Legal Challenges**
Permitting delays, lawsuits, and policy scrutiny
- Reputational Risk**
Perceived lack of transparency and corporate accountability

Public opposition is increasing and can escalate quickly around new projects or expansions.

WHY IT MATTERS

AI & Machine Learning

Cloud Computing

Defense & Intelligence

Financial Systems

Healthcare

Telecommunications



AT-RISK International is a global protection agency specializing in security services for individuals and organizations. Our team of experts creates and maintains secure environments by providing threat analysis, protection, investigations, consulting, intelligence and security training services. Since 2003, our mission has been to discretely mitigate security threats before they occur. Through advanced research, analysis and preparations, we protect companies and individuals throughout the Americas, Europe, the Middle East, the Caribbean and Asia Pacific.