Case Studies for Recent Damage to U.S. Critical Infrastructure

Information as of 08 June 2026

While cyber-attacks are an exceptional means of transmuting lines of communication into lines of attack over vast distances, we are seeing physical augmentation to cyber and exploitation between siloed sectors. While each of these, often separately, are assessed with an organization RMF, the conjunction of intent using different avenues of attack within specific timeframes and environmental conditions compounds risks to historically unprecedented levels.

Physical Sabotage. A May 2026 Improvised Explosive Device (IED) emplacement below the waterline at a Louisiana water treatment plant proved that physical targeting of soft-target utility sectors remains a persistent, potentially devastating, low-tech threat. This placement was intentional and strategic; it was either done by an insider threat or by an outsider possessing specific intent using effective planning. This is when Louisiana, in mid-May 2026, had 28.5% of the state in "severe drought" conditions with a total of 69% of the state in some level of drought condition.

- **Takeaway:** Extremists, proxies, and criminals are taking advantage of the rapid change within policies and regulations. Iran has stated that she is activating her proxy fighters. Extremist organizations like DAEISH/ISIS continue publishing directions on how to cripple western infrastructure through publications like "Inspire". And even insider-threats are increasing with financial strain, external pressures, and job instability. Risk likelihood for Physical Sabotage is increasing, and the potential impacts are also elevating to potentially catastrophic levels.
- **Likely Scope of Impact:** *The convergence of state-sponsored proxy mobilization, widely disseminated open-source sabotage manuals, and economically strained insiders creates a compounding, multi-front threat vector for critical infrastructure*. As regulatory frameworks adapt to the evolving landscape, adversaries are actively exploiting transitional blind spots to lower the barrier to entry for physical attacks. State actors increasingly rely on gray-zone proxies to inflict strategic, catastrophic disruptions while maintaining plausible deniability, a tactic paralleled by extremist organizations, such as ISIS and Al-Qaeda (via publications like *Inspire*), which actively crowd-source the physical destruction of Western utilities. Concurrently, escalating financial and external pressures on personnel transform the traditional insider from a generic security vulnerability into a highly susceptible recruitment

target for hostile actors. *The operational environment requires defending against not just isolated intrusions; but, anticipating catastrophic physical sabotage that leverages a lethal combination of external ideological coercion and internal operational compromise.*

Targeted Wipe Attacks. Pro-Iranian hackers claimed responsibility for a comprehensive digital wipe attack against global medical technology giant Stryker in March 2026. This attack paralyzed production pipelines, demonstrating that state-aligned actors are actively executing destructive payloads against critical infrastructure to cripple broader supply chains. This was an escalation from the previous trend of ransomware.

- **Takeaway:** Wipes are less likely a motivator of financial criminal intent and more likely indicative of proxy actors or state-sponsored digital terrorism. Hybrid warfare takes advantage of the previous "probing" and "testing," mainly vulnerabilities, responses, and backdoors that are now used for more impactful damage to CI in lieu of physical attacks. Risks for ransomware remain stable in their likelihood due to criminals still taking advantage; however, risks for catastrophic wipes or destruction are increasing in probability.
- **Likely Scope of Impact:** The escalation from financially motivated encryption to state-sponsored data annihilation fundamentally alters the recovery paradigm for critical infrastructure. Unlike ransomware, where operational restoration remains theoretically negotiable via decryption keys, wiper malware is engineered for irreversible systemic degradation. *When adversaries transition from reconnaissance to execution, they activate dormant backdoors to deploy destructive payloads impacting digital data loss.* This attack vector frequently and effectively "bricks" specialized Operational Technology and Industrial Control Systems. This forces physical hardware replacement and the manual reconstitution of core utilities, extending service outages from days to potentially months. *By utilizing destructive cyber capabilities as a primary theater for digital terrorism, proxy actors can inflict catastrophic economic and societal paralysis that mirrors the strategic impact of a kinetic strike, all while operating under a veil of plausible deniability.*

Indirect Impacts. Whether it was sabotage or a simple software glitch, the January 2026 Verizon outage, which transpired during acquisition of Frontier Communications and immediately prior to organizational growth, significantly impacted USA communications, emergency response, and security that even drove a Congressional inquiry. This loss of communications is not a stand-alone event and has been seen elsewhere with other communications entities as overt cyberattacks: in 2025, Cellcom confirmed a cyberattack caused a week-long outage in Michigan and Wisconsin.

- **Takeaway:** When Verizon experienced system degradation due to a software glitch, similar to what happened when Crowd Strike's degraded operations in 2024; the impacts extended beyond Verizon's consumer base. Other carriers leveraging Verizon's networks via contracts or other support agreements, and payment systems dependent on cellular networks faced debilitating impacts from Verizon's "glitch". Crippling cyberattacks on communication infrastructure is no longer a low or medium risk but a high payoff target with catastrophic effects.
- **Likely Scope of Impact:** The interconnected architecture of modern critical infrastructure dictates that operational isolation is an illusion; a degradation within a primary telecommunications provider catalyzes immediate cascading failures across interdependent sectors. Beyond retail consumer friction, the loss of cellular connectivity severs the vital data-link layer required for emergency responder coordination, municipal logistics, and real-time financial clearing operations. *The reality that a routine software anomaly or third-party vendor patch can unintentionally induce such widespread operational paralysis serves as a highly visible proof-of-concept for malicious actors*. Consequently, these network choke points provide an asymmetric vector for adversaries aiming to bypass traditional kinetic thresholds, enabling targeted cyber-coercion campaigns designed to yield strategic, multi-sector disruption.

Critical Manufacturing and the Defense Industrial Base (DIB).

To defeat an industrial opponent, industry itself must be defeated. Factory bombings, such as executed in previous conflicts, is more expensive and challenging than simply mitigating production. Foreign adversaries intentionally target manufacturing directly and indirectly: military conflicts with actors capable of proxy and cyber-attacks, the likelihood of risk increases for both the DIB and those sectors on which the DIB depends. Manufacturing is one of the most targeted sectors for malicious software and cyberattacks: in 2025, they experienced a 71% surge in active threats. The DIB supply chain is especially vulnerable to unclear or unknown third-party dependencies and to foreign-influenced risk exposure.

- **Takeaway:** The Critical Manufacturing Sector has dependencies and interdependencies in the following sectors: Transportation Systems, Energy, Chemical, Energy, and Water. To impact the DIB, any of these other sectors are prime targets. Any entity within those noted sectors are projected to have increased likelihood of catastrophic risks from foreign actors notably increase. Any sectors within closer geographic proximity to DIB hubs should consider a high likelihood of catastrophic attacks during this time of geopolitical turmoil and conflict.

- **Likely Scope of Impact:** The *geographic clustering of critical manufacturing alongside its foundational lifelines; like energy grids, water treatment facilities, and transportation corridors creates a densely concentrated, target-rich environment for state-sponsored adversaries*. Rather than directly assaulting hardened Defense Industrial Base (DIB) enclaves, threat actors operationalize hybrid cyber-coercion by degrading these adjacent, often less-secure civilian vectors, triggering a cascading paralysis of military supply chains. In the current landscape of aggressive geopolitical balancing, these critical interdependencies provide an asymmetric advantage, allowing foreign actors to cripple national security output while operating below the threshold of kinetic conflict. Consequently, *sheer geographic proximity to DIB hubs elevates the risk profile of structurally unrelated municipal and private entities, transforming them from peripheral collateral into primary strategic targets.*