Batteries As Cyber Asset, Batteries as Cyber Liability

Harry Krejsa
Carnegie Mellon Institute for Strategy & Technology

We now know the People's Republic of China (PRC) is actively embedding disruptive cyber capabilities on America's critical infrastructure, seeking to sow chaos during a potential conflict and slow our ability to mobilize in response. This infiltration is possible precisely because our current electrical grid represents the worst of both security paradigms—neither fully isolated nor properly designed for connectivity. Decades of ad hoc digitization have created a patchwork where internet-accessible software awkwardly interfaces with operational technologies never built to withstand sophisticated cyber intrusions. We face a stark reality: returning to a fully air-gapped electrical ecosystem is technologically and economically infeasible, while maintaining our current hybrid approach leaves us perpetually vulnerable to actors like Beijing and Moscow who have demonstrated both capability and intent to exploit these seams in our infrastructure.

Booming growth in electricity demand, alongside historic investments in modern and clean energy technologies, represents a golden opportunity to break free from this security paradox by embracing a fully digitally-native infrastructure. Rather than fighting against the inevitability of connectivity, we must lean into it—building systems that anticipate intrusion attempts and adapt continuously to emerging threats. Battery storage systems have emerged as the critical technology enabling this transition, with their deployment accelerating far beyond what analysts predicted just a few years ago. As the transmission buildout many expected would accompany our grid expansion faces permitting obstacles and construction delays, batteries are increasingly filling critical gaps—absorbing surplus energy when production exceeds demand and dispatching it when most needed. More importantly, batteries represent our clearest path toward a coherent security architecture that replaces brittle legacy systems with inherently updatable, resilient technologies natively designed for a connected world. Electricity storage is inherently more efficient than combustion engines, more scalable across applications as diverse as miniature drones to electric vehicles to gigawatt-scale facilities, and provides critical sources of resilience for military installations and civilian infrastructure alike. Indeed, a battery-equipped solar array can maintain essential functions even when cut off from traditional fuel supply lines—a significant advantage during either a natural disaster or military contingency.

Yet these systems represent a double-edged sword for national security. On one hand, battery technologies are "digitally native"—designed from the ground up with software and connectivity at their core—and can incorporate modern security features that legacy operational technology (OT) systems retrofitted with digital controls could never achieve. These same characteristics, however, can create new vulnerabilities if implemented without rigorous security controls, trading security improvements instead for a vast enlargement of potential cyber threat surfaces. Further, unlike traditional energy dependencies, where an oil embargo would immediately disrupt operations, battery supply chain vulnerabilities present differently; systems would continue functioning if supply chains were severed tomorrow, but the long-term strategic implications of foreign dependency remain profound. The overwhelming majority of battery

materials—from critical minerals to the microelectronics managing individual energy cells—run through the PRC. The battery revolution thus presents America with a pivotal choice: harness their potential to create a self-healing, resilient grid capable of withstanding cyber infiltration, or risk constructing an expanded attack surface that simply replicates—or even worsens—our infrastructure's existing weaknesses.

Battery Storage as Security Asset

When properly integrated, battery systems can transform our electrical grid from a vulnerable target into a resilient, defensive asset. Unlike conventional fossil-fuel infrastructure where digital controls were awkwardly grafted onto analog systems never designed for connectivity, battery storage technologies are capable of "security by design" principles. Their sophisticated battery management systems have the contemporary computing necessary to leverage modern cryptographic standards, continuous firmware updating capabilities, and multi-layered authentication protocols from inception. This architectural advantage begins at the foundational level; where legacy industrial control systems require retrofitting to achieve even basic security postures, battery systems can incorporate and be networked into zero-trust frameworks, encrypted communications, and hardware security modules. The implication for critical infrastructure is profound: we have an opportunity to replace technologies with decades of accumulated "technical debt" with systems inherently more defensible against state-sponsored threats.

The distributed nature of battery deployments offers an additional resilience dimension traditionally unavailable to centralized power generation. In our current grid architecture, a single successful cyber intrusion—like that which darkened Ukraine in 2015—can cascade across interconnected systems and create regional blackouts affecting millions. The 2003 Northeastern United States blackout demonstrates this vulnerability: a minor power surge in Ohio ultimately left tens of millions of people across numerous states and Canada without electricity. Battery-enabled distributed resources fundamentally alter this equation by enabling network segmentation in the physical world. During attacks or disruptions, compromised sections can be more easily isolated while battery systems maintain critical services in "islanded" microgrids operating independently from the broader network. This capability transforms our grid from a rigid, brittle system too easily toppled by targeted attacks into an adaptively resilient network that can autonomously seal off compromised sections, reroute power flows, and maintain essential functions—potentially even without human intervention.

Advanced sensing and analytics capabilities embedded within battery systems can further enhance our defensive posture through unprecedented situational awareness. While legacy operational technologies provide limited visibility into anomalous behaviors, battery storage facilities continuously monitor thousands of parameters—from individual cell temperatures to voltage fluctuations—creating rich data streams invaluable for threat detection. Machine learning algorithms can establish baseline performance signatures and instantly flag deviations potentially indicating intrusion attempts, with updating mechanisms far more agile than traditional industrial control systems. Most importantly, batteries operate within a supervisory ecosystem designed for regular software updates, enabling rapid security patching when

vulnerabilities emerge—a stark contrast to legacy infrastructure where essential components often remain in service for decades with known security flaws that cannot be remediated. When paired with AI-driven anomaly detection systems, this comprehensive monitoring capability could enable not just reactive defense but predictive identification of emerging attack vectors, enabling a future where operators can implement countermeasures before malicious actors can achieve their objectives.

Battery Storage as Security Liability

If implemented poorly, battery storage systems can fall far short of the potential described above, and could even introduce new vulnerabilities to our critical infrastructure. While traditional power plants operate with high variations in their external connectivity, modern battery installations are fundamentally digital ecosystems—constantly collecting, analyzing, and transmitting data across multiple network layers. A utility-scale battery facility can have large numbers of sophisticated sensors communicating with centralized management systems, third-party analytics platforms, and grid operators. If not implemented thoughtfully, this proliferation of connection points can exponentially expand potential attack surfaces. The Internet of Things (IoT) devices integral to battery operation introduce particularly challenging security considerations; unlike enterprise IT environments with standardized security frameworks, these specialized systems often operate with proprietary protocols, limited computing resources, and irregular update cycles. Firmware update mechanisms—essential for maintaining security postures—paradoxically introduce their own risks, as compromise of distribution channels could potentially serve as vectors for malware deployment across entire hardware networks. Virtual power plants (VPPs), which aggregate thousands of distributed energy resources through purely software-defined control systems, represent particularly impactful attack vectors; a compromised VPP could potentially manipulate voltage levels across wide areas or coordinate battery discharges in ways that destabilize broader grid operations.

These technical vulnerabilities are exacerbated by significant institutional and regulatory blind spots that leave much of our evolving energy ecosystem unprotected. Only 10-20 percent of the entire U.S. electricity system falls under federal cybersecurity oversight—a troubling gap as distributed energy resources proliferate throughout the grid. The Federal Energy Regulatory Commission (FERC), via the North American Electric Reliability Corporation (NERC), helps set mandatory critical infrastructure protection standards, but their jurisdiction is remarkably limited against the scope of modern cyber threats. This regulatory fragmentation leaves the grid's distribution system—the precise layer expected to see the largest proliferation of battery deployments—largely exempt from mandatory security requirements. The challenge is complicated further by cultural divides between stakeholders; traditional energy companies bring decades of security experience but often struggle to adapt to modern software-defined paradigms, while newer market entrants frequently lack the security sophistication their systemic influence demands. Household and commercial battery installations fall below regulatory thresholds entirely, despite collectively contributing significant power to the grid. The Government Accountability Office has warned for years that this patchwork approach creates dangerous seams in our infrastructure's digital defenses—seams that sophisticated adversaries are actively seeking to exploit.

Supply chain dependencies introduce additional vulnerabilities that cannot be easily addressed through software patching or network monitoring alone. China's dominance across battery manufacturing extends from raw mineral processing to the sophisticated microelectronics controlling energy flows within these systems. The Bipartisan Infrastructure Law and the Inflation Reduction Act began incentivizing supply chain diversification, but Beijing's advantage in the sector remains immense, necessitating a rigorous risk prioritization framework to triage these efforts. That prioritization framework could rank modern energy technologies by their digital enablement and systemic influence—with Virtual Power Plants (VPPs) perhaps occupying the highest risk tier due to their software centrality and grid-wide impact, battery storage systems occupying a middle tier with moderate digital exposure and localized implications, and basic solar panels at the lower tier with minimally-connected digital footprints and highly constrained systemic influence. By addressing the most digitally-enabled and systemically-consequential technologies first, the United States can focus its limited resources on this complex undertaking where vulnerabilities and consequences intersect most dangerously.

V. Conclusion: The Path Forward

The security implications of America's battery revolution hang in a precarious balance—with the potential to either fortify our grid against mounting threats or magnify its existing vulnerabilities. There is no path backward to a simpler, air-gapped reality; we must move forward through digital transformation. Realizing the security benefits while minimizing risks demands unprecedented coordination between communities that have traditionally operated in separate spheres: clean energy innovators focused on deployment speed and decarbonization targets, and national security professionals concerned with defending critical infrastructure against sophisticated adversaries. This strategic unity of effort must extend from technical standards development to supply chain diversification, from regulatory frameworks to intelligence sharing mechanisms. Rather than viewing cybersecurity requirements as impediments to rapid and modern energy deployment, the United States has an opportunity to make security a competitive differentiator—positioning American battery manufacturers as global leaders in trustworthy and resilient energy technology that commands greater trust and value in international markets.

The decisive factor determining whether battery storage systems enhance or undermine our national security will be implementation choices made today—as we deploy these technologies at an unprecedented scale and pace. With no viable alternative to an increasingly connected grid, we must lean into connectivity rather than resist it. Battery storage can either become the backbone of a self-healing, resilient grid capable of withstanding and rapidly recovering from sophisticated attacks, or it could represent an expansion of attack surfaces vulnerable to exploitation by adversaries who have already demonstrated both capability and intent to target our infrastructure. The transformation of our energy ecosystem is already underway; the next task is to ensure that implementation brings grid fortification alongside grid expansion.