Carnegie Mellon University

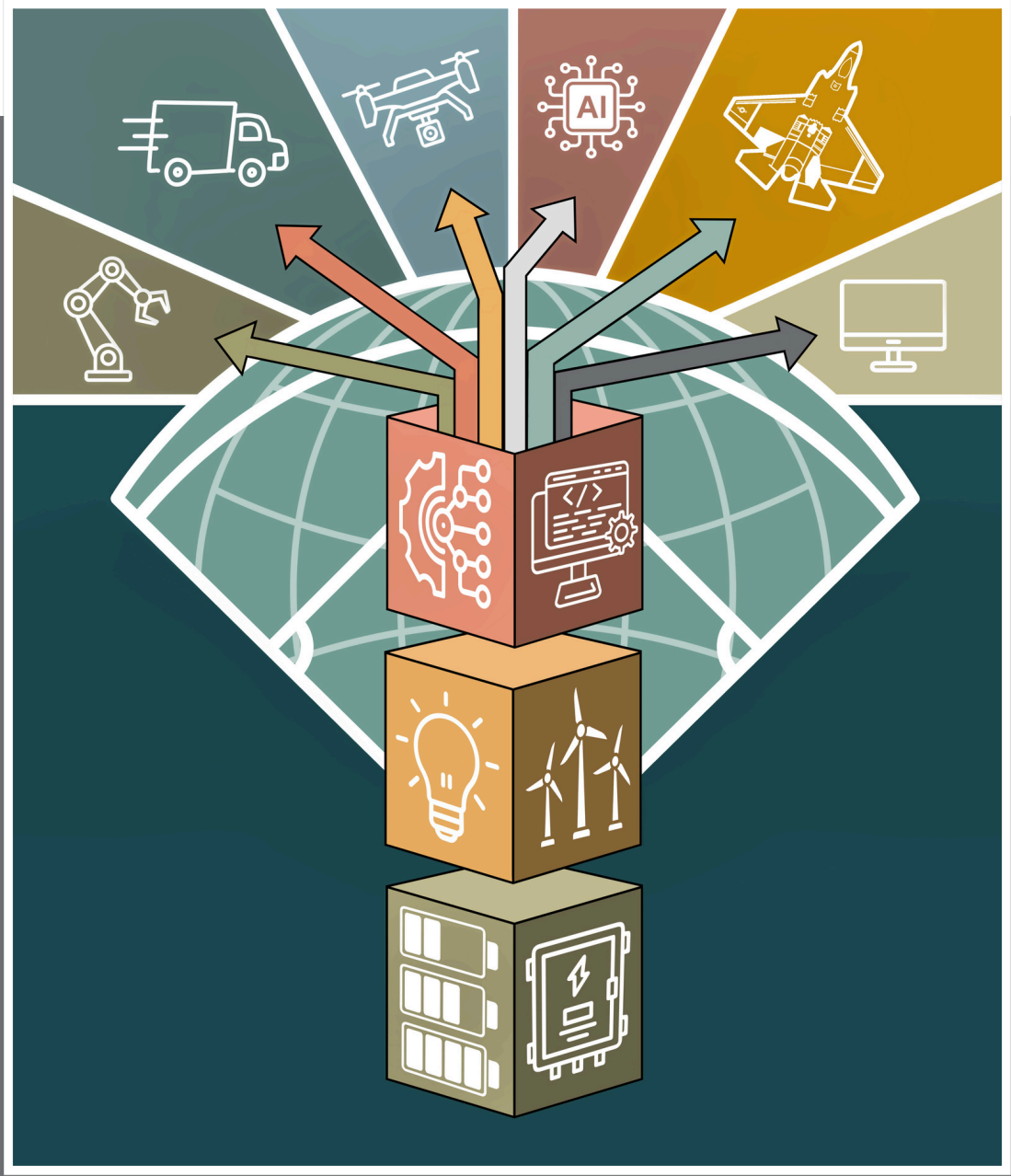
FDD

MAY 2026

WHITE PAPER

ELECTROTECH MONEYBALL

An Industrial Strategy for Ranking Risk and Opportunity in Energy & AI Supply Chains



By Phoebe Benich, Dr. Emma Stewart, and Harry Krejsa

Carnegie Mellon Institute for Strategy & Technology

CCTI Center on Cyber and Technology Innovation

About the Authors

Phoebe Benich is a non-resident fellow at the Carnegie Mellon Institute for Strategy & Technology (CMIST), focusing on US-China technology competition, energy security, and governmental engagement with the startup ecosystem. Phoebe was previously director for strategic risk at the White House's Office of the National Cyber Director (ONCD), where she oversaw Indo-Pacific partnerships and served as the staff lead for developing and implementing modern energy cybersecurity priorities. Prior to ONCD, she was a senior program manager at In-Q-Tel and served on the staff of the U.S. Cyberspace Solarium Commission and Defense Innovation Board, with earlier roles spanning Asia-Pacific national security at the State Department, Booz Allen Hamilton, and the Center for a New American Security.

Dr. Emma Stewart is a non-resident fellow with CMIST, leads Idaho National Lab's Center for Securing Digital Energy Technology, and is a nationally-recognized expert in batteries and grid cyber- and supply chain security. Previously, she served as chief scientist at the National Rural Electric Cooperative Association, where she led research and cyber programs for electric cooperatives nationwide. Dr. Stewart has held leadership positions at both Lawrence Livermore and Lawrence Berkeley National Laboratories, where she pioneered critical work in grid resilience, developed the first micro-synchrophasor network in the US, and managed complex simulation and analysis projects.

Harry Krejsa is the director of studies at CMIST. Harry joined Carnegie Mellon from the White House ONCD, where he led development of the 2023 National Cybersecurity Strategy, established national modern energy security priorities, and represented the U.S. government in technology security consultations with foreign partners and the global private sector. Harry previously worked at the intersection of technology, industrial strategy, and US-China competition for the Department of Defense, the Cyberspace Solarium Commission, and the Center for a New American Security.

Acknowledgements

The authors are indebted to many friends, colleagues, and mentors who contributed immeasurably to the production of this report. Expert feedback from Jack Burnham, John Costello, Mieke Eoyang, Annie Fixler, Sarah Hipel, Andrew Scott, and numerous industry interviews was invaluable. Research assistance from Ryan Podnar was foundational. Support and direction from Dr. Audrey Kurth Cronin of the Carnegie Mellon Institute for Strategy & Technology, Dr. Costa Samaras of the Scott Institute for Energy Innovation, and Mark Montgomery of the Foundation for Defense of Democracies' Center on Cyber & Technology Innovation were key to the authors' success. Project guidance and design provided by Jess Regan, Leah Weingartner and Carolyn Just were critical. Editing by Sandra Tolliver was excellent.

This report was reviewed to ensure that it contains no controlled information; all judgments and conclusions are entirely those of the authors. The authors employed artificial intelligence tools to aid with initial research, drafting and editing, and preliminary visual concepts. All AI-assisted material was rigorously checked, revised, approved, and integrated by the authors.

The views herein are the authors' alone, along with any errors of fact, omission, or interpretation.

This report and its findings are the sole responsibility of the authors.
Cover illustration by Jess Regan. Internal illustrations by Jess Regan and Leah Weingartner.

TABLE OF CONTENTS

FOREWORD

By: **Jim Langevin**, Former US Representative, Rhode Island; Chairman, FDD Center on Cyber and Technology Innovation Advisory Board; **Tom Fanning**, Former Chairman and CEO, Southern Company; Member, FDD Center on Cyber and Technology Innovation Advisory Board

The United States is building the grid that will power the next half-century of American prosperity. The scale of that undertaking—driven by AI, electrification, and the reindustrialization of critical supply chains—is without recent precedent. So is the risk if we get it wrong.

Between us, we have spent decades focused on our nation's cybersecurity problems, working from the sometimes-conflicting perspectives of government and the private sector. One of us ran one of America's largest energy companies and co-chaired the body responsible for coordinating the electric sector's cyber and physical defense against national security threats. The other led congressional efforts to build the legal and institutional architecture—from the National Cyber Director to the Cybersecurity and Infrastructure Security Agency—that the federal government now relies on to secure critical infrastructure.

We served together on the congressionally-mandated Cyberspace Solarium Commission, where we saw firsthand how the seams between government and industry, and between legacy systems and new technology, create the openings that adversaries are most eager to exploit.

That experience is why this paper commands our attention.

"Electrotech Moneyball" confronts a problem that too few policymakers have reckoned with clearly: The sourcing and security decisions being made today—often without adequate strategic scrutiny—will lock in advantages or vulnerabilities for decades. The hardware and software being deployed into our grid at historic speed are not just energy technologies. They are the shared industrial base underpinning defense, AI, autonomous systems, and advanced manufacturing. Thus, the advantages and vulnerabilities locked in today are also not confined to the energy sector.

The paper's central insight is one we believe deserves serious engagement. Not every component carries the same risk, and treating the entire supply chain as a uniform emergency will paralyze the very buildout we need. The authors propose a disciplined framework for distinguishing where real vulnerability concentrates—in the digitally active control layers that increasingly govern how power is generated, routed, and balanced. The security calculus for these components is fundamentally different than for commodity hardware. That distinction matters. Without it, we will either over-restrict inputs we cannot yet replace—stalling deployment of electricity generation and transmission we need to power our modern economy—or we will spread our limited security resources so thin that we will defend nothing well.

In today's digital world, it is clear that the government cannot provide our national security on its own as it has in the past. The private sector owns and operates over 85% of our critical infrastructure. Today and in the future our national security requires a collaboration—not just "cooperation" or "coordination" or "sharing"—in order to protect and sustain the American economy and provide the national security that our citizens deserve. Industry, however, also cannot secure it without clear signals from government about where scrutiny should concentrate. And neither can succeed without a broader national conversation about what we are willing to invest—in domestic manufacturing, in allied partnerships, in the hard work of setting standards before architectures become locked in—to ensure this buildout strengthens rather than undermines American competitiveness.

It is not an exaggeration to say that how our nation addresses this challenge will determine whether we will remain the preeminent global economic power or whether we will be dangerously vulnerable to and dependent upon our most capable adversary, China.

The authors are asking the right questions at the right time, with the analytical rigor the moment demands. The framework they propose—grounded in the idea that we can assess technology based on its systemic importance, risk, impact, and level of digital sophistication—offers policymakers, industry leaders, and civil society a common language for making the hard prioritization choices that no longer can be deferred.

We urge readers across government, the private sector, and the broader national security community to give this paper the serious consideration it deserves. The window for getting this right is closing.

EXECUTIVE SUMMARY

The United States is in the early stages of a generational energy buildout driven by AI demand and accelerated by hundreds of billions of dollars in public and private investment. Central to this buildout is the digitization of the grid itself: the batteries, power electronics, and embedded software that will give America's electrical infrastructure a digital nervous system capable of the flexibility, responsiveness, and adaptive threat management that aging analog systems cannot provide. Deployed well, this digitization will be the foundation for a grid architecture that is more dynamic and more defensible than what it replaces.

Yet even as we race to realize this modernization and expansion, we are dependent on the United States' principal strategic competitor for the tools to build it. The People's Republic of China (PRC) dominates much of what many experts call the "electrotech stack"—the integrated set of hardware and software components central to this buildout that are transforming electricity from a physical flow into something that also can be digitally generated, stored, and directed. That dependence is not only creating a supply vulnerability, but also threatening to undermine the very security advantages that a modernized grid is supposed to deliver.

The United States cannot slow its grid expansion, leave it undefended, or decouple it from PRC supply chains overnight. Smart strategic planning means addressing the most serious vulnerabilities first. Not every component in America's rapidly digitizing grid carries equal risk. Treating the entire electricity ecosystem as if everything is an emergency means that nothing will be defended effectively. And imposing blanket restrictions on all Chinese-made components would throttle the very industrial buildout the United States needs to outpace current PRC manufacturing advantages. Indeed, the most strategically underweighted danger to the US energy ecosystem may not come from Beijing, but from self-inflicted paralysis—whether through overcorrection that delays the technologies this buildout demands, or indecision that continues ceding agency to our competitors.

"The most strategically underweighted danger to the US energy ecosystem may not come from Beijing, but from self-inflicted paralysis—whether through overcorrection that delays the technologies this buildout demands, or indecision that continues ceding agency to our competitors."

This paper proposes a "Moneyball" framework for strategic prioritization of and within the electrotech stack—one grounded in the recognition that, increasingly, these components are not

exclusive to energy systems, but essential to a common industrial foundation with growing leverage across defense, robotics, autonomous systems, and advanced computing. It seeks to determine where to focus first, to achieve the greatest cross-sector strategic return.

The framework assesses each technology across three dimensions:

1. How urgent is its deployment and how imminent is technological lock-in?
2. Which technologies constitute the biggest vehicles for risk—but also the most systemically influential opportunities to mitigate it?
3. How much cross-sector industrial competitive advantage would domestic leadership of that technology confer?

One of the framework's core analytical distinctions—and the primary determinant of a component's systemic risk—is where it falls on a spectrum of "smart" to "dumb" connectivity, and how far that connectivity reaches across the stack. Commodity battery cells and passive solar hardware, for example, do not present the same threat surface as their associated digitally active control layers, such as battery management systems, inverter firmware, fleet orchestration platforms, or cloud-connected software. The latter actively and increasingly determines how power is generated, stored, routed, and balanced across the grid. Systemically consequential risk concentrates in that "smart" layer; so too should policy.

Based on that assessment, the framework sorts components into three tiers of policy priority:

- Tier 1: Tight domestic control for the most consequential technologies;
- Tier 2: Trusted-ally sourcing where allied supply chains can suffice; and
- Tier 3: Managed global procurement with appropriate safeguards for commodity hardware where security exposure is lower.

The most urgent policy action is using this "Moneyball" framework to prioritize security scrutiny for the buildout now underway—applying deployment-phase requirements to the digitally active Tier 1 control layers that can then function as "firebreaks" against risks that would otherwise propagate down the stack. This approach mirrors the zero-trust logic now standard in federal and enterprise cybersecurity, where the architecture assumes compromise, authenticates at every trust boundary, and enhances control rigor with systemic consequence rather than relying on perimeter defense alone. Where security exposure is lower, "dumber" Tier 3 commodity hardware can continue to be sourced globally—even from less-trusted vendors—preserving the cost advantages and deployment speed the buildout demands.

In this paper, we apply this framework to two especially clear test cases: batteries—whose rapid deployment across the grid and growing role in defense, transportation, and advanced manufacturing place them at the intersection of every dimension the framework is designed to surface—and solar panels, which materially contrast in their risk profile and narrower cross-sector impact. While federal leadership would accelerate the benefits of this framework, it is not a prerequisite. State leadership in high-leverage jurisdictions for our current energy expansion, like Virginia and Texas, can set precedents through procurement and interconnection requirements, and private-sector collaboration on secure-by-design baselines will be a critical complement.

The electrotech stack is increasingly the operating system through which our economy's energy, data, and value flow. Its deployment will determine whether America's infrastructure can grow fast enough, flex dynamically enough, and defend itself credibly enough to sustain the generational buildout now underway. Getting the prioritization right means this operating system will be built to ensure American advantage. Getting it wrong—or not building at all—will cede that advantage to the Chinese industrial strategy that is already supplying the parts.

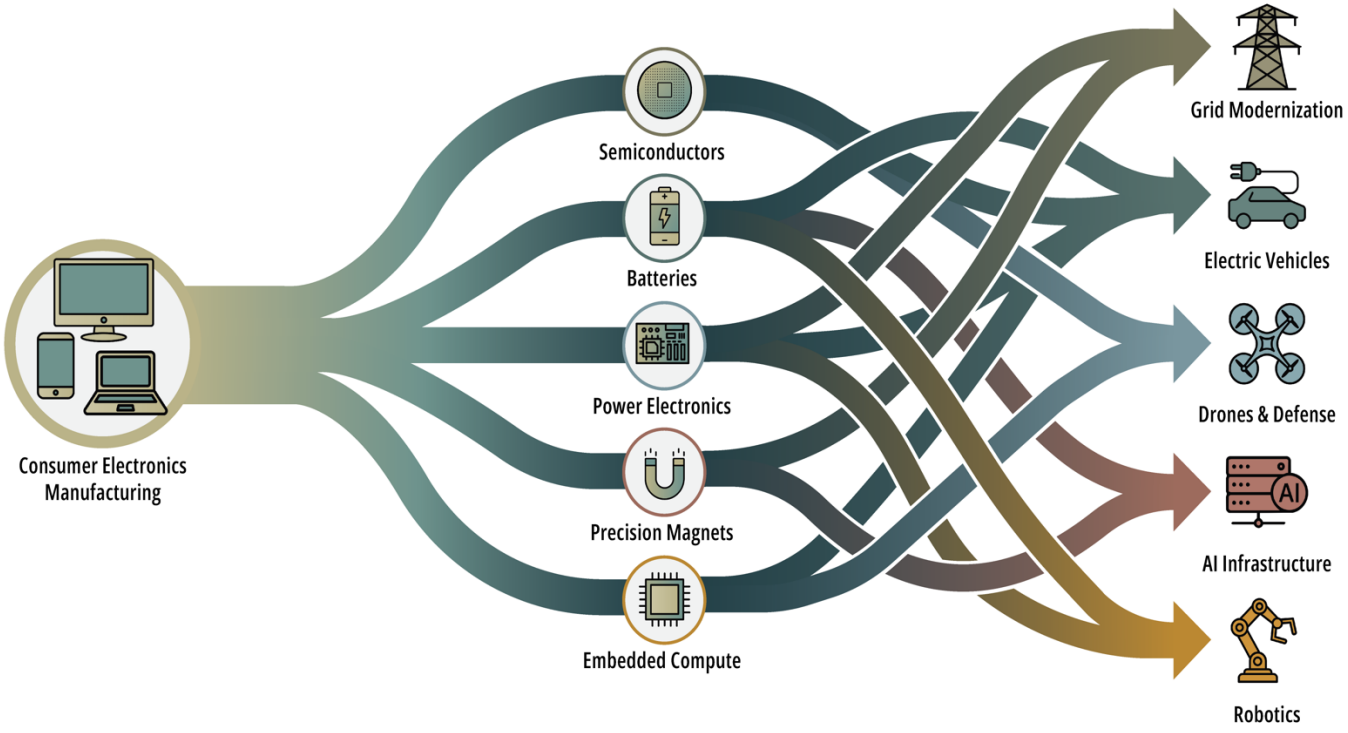


Fig 1: The electrotech stack—sophisticated and digitally-enabled technologies refined through the consumer electronics revolution—increasingly underpins energy, defense, AI, and robotics not as separate supply chains but as an intertwined industrial base. Dominance or vulnerability in one sector will deeply influence the rest.

THE ELECTROTECH OPPORTUNITY

The rapidly digitizing technologies at the center of America's grid modernization—such as batteries, power electronics, semiconductors, and the software that orchestrates them—comprise an integrated "electrotech stack" whose security and sourcing will shape US competitiveness across energy, defense, AI, and advanced manufacturing for decades.[1] This section introduces that stack, explains why it represents both an extraordinary industrial opportunity and a growing strategic vulnerability, and establishes why the sourcing decisions being made now will be difficult to reverse.

The emerging electrotech stack encompasses the hardware and software layers that make modern electrical systems digitally programmable, including those that power everything from AI infrastructure to electric vehicles to drones. This includes the semiconductors that switch and convert power at computational speeds, the batteries and power electronics that store and dispatch it on demand and at a quality required for the new sensitive loads, the precise motors applying constantly-updating electromagnetic torque, and the software that coordinates all of it in real time. Together, these components are transforming electricity from a physical flow into something that can be digitally managed and optimized, offering competitive advantage to economies that can dominate and deploy crucial elements of this stack.

This digitally-native architecture is fundamentally distinct from the more analog industrial control systems (ICS) that came before it. Legacy grid infrastructure—characterized by mechanical switches and hardwired power electronics—either operated without external network interfaces, or with simplistic, bolted-on connectivity oriented more toward remote operation and monitoring rather than machine-speed management and orchestration. The components of the electrotech stack, by contrast, are disproportionately networked, software-defined, and remotely updatable by design. This digital connectivity offers advantages in performance and security alike; a software-defined grid can not only be rebalanced and adapted at speeds and scales that legacy systems never could approach, but can also be monitored, patched, and, when faced with disruption or attack, document operational forensics that will be key to response and recovery.[2]

The very mechanisms that enable this software-defined coordination—network logs, software update channels, telemetry feeds, and cloud connectivity—are simultaneously a source of risk and (if architected with discipline) a means to detect and contain it.[3] Each represents an interface between grid infrastructure and external networks—and therefore a potential vector for unauthorized access, malicious code delivery, or operational disruption. And because the grid itself is becoming digitized, that connectivity (and its concurrent promise and peril) is flowing onto older

assets as well.[4] Nuclear plants, gas turbines, and large hydro facilities are becoming enabled by and dependent on our infrastructure's growing digital layer, regardless of the technology profile of the particular generator. But in each case, the same digital integration that creates vulnerability also creates the means to monitor, patch, and defend against it—provided those capabilities are governed with the discipline the threat demands.

Importantly, the electrotech stack's significance extends well beyond energy. The semiconductor fabrication lines, battery chemistry and cell manufacturing, wireless communication modules, precision sensors, and power management systems that scaled to meet global demand for smartphones and laptops comprise the same industrial base now producing the components being deployed into AI infrastructure, modern grid systems, battery storage facilities, EV drivetrains, drones, and broader defense platforms. This shared industrial heritage—including electrotech's defining capability, the digital management of physical systems—means that advancements or dependencies in one sector can easily influence or propagate across the others.[5]

> ***Electrotech is increasingly not a collection of separate industries with distinct supply chains, but a single industrial base with multi-sector leverage.***

As a result, electrotech is increasingly not a collection of separate industries with distinct supply chains, but a single industrial base with multi-sector leverage. The country that dominates that shared foundation is poised to reap compounding advantages across all of them. Moreover, because of this shared industrial heritage, one country's dominance in the electrotech industrial base can become self-reinforcing: the design and sourcing decisions being made today in support of the AI-driven grid expansion will influence competitive positions across not only energy, but also defense, advanced computing, transportation, and autonomous systems for decades to come.

THE DATA CENTER DRIVER

The scale and velocity of AI-driven energy demand is catalyzing a fundamental rearchitecting of the American grid. In doing so, it is also dramatically expanding both the deployment and the strategic significance of the electrotech stack. As hyperscalers and independent power producers rush to site and power data centers, their demand is accelerating a shift toward techniques like dynamic load management and rapidly deployable technologies such as distributed generation and behind-the-meter (BTM) assets. The traditional governance structures built to ensure grid reliability, security, and equitable access were not designed for this frontier, and they are struggling to adapt at a speed and scale adequate to meet demand. This section examines the historic nature of that demand, demonstrates how the resulting infrastructure buildout is also deploying the electrotech tools that could make the grid more resilient, and identifies the governance gaps that will determine whether that deployment strengthens or undermines grid security.

New Demand Straining Existing Infrastructure and Governance

The AI boom is driving a frantic surge in planning, construction, and connection of data centers, and with it, demand for both the electrotech components and the energy needed to power them. In 2025, the United States had more than 5,400 data centers and nearly 3,000 new sites under construction.[6] The size of individual facilities is escalating rapidly: While no gigawatt-scale data center is yet in operation, a 2025 Department of Energy (DOE) request for information surfaced designs for an AI data park by 2028—a single facility with a 1 GW capacity (roughly the continuous electrical power draw of a mid-sized American city).[7] This construction is driving clear trends for the future of national and international electricity demand. Lawrence Berkeley National Lab forecasts that data centers' share of US electricity could triple from 4.4% in 2023 to 12% by 2028,[8] a pattern mirrored globally, where electricity demand is growing at more than twice the rate of overall energy demand.[9]

As these data centers increase the United States' overall demand for electricity, their operators are facing the harsh reality of our grid's limits. According to the Federal Energy Regulatory Commission (FERC), the United States will add roughly 130 GW of generating capacity by 2028, reaching a net gain of 96 GW after planned retirements.[10] That falls short of projected data center demand alone, which S&P Global estimates could reach 134.4 GW by 2030.[11] Closing that gap between supply and demand will require not just more generation, but a fundamental overhaul of the transmission infrastructure.

But indeed, the infrastructure over which electricity flows is also under strain. Much of America's transmission and distribution infrastructure is decades old and already nearing end of life, having been underinvested in for years.[12] The North American Electric Reliability Corporation (NERC) Large Loads Task Force—a working group convened by the body responsible for the reliability of North America's generation and transmission infrastructure—has found that data center load growth is already narrowing operating margins, heightening risk of forecasting errors, and concentrating supply chain and cybersecurity vulnerabilities.[13] The Department of Energy's Speed to Power initiative has identified reconductoring (i.e., replacing existing transmission cables with higher-capacity and more digitally flexible alternatives) as a key near-term lever to relieve that pressure.[14]

Smarter infrastructure, however, cannot compensate for simple scarcity. The US built only 322 miles of new high-voltage transmission lines in 2024, far short of the 5,000 miles of new capacity per year the Department of Energy estimates the US needs to ensure grid reliability.[15] Shortages are also the norm for transformers, the large electrical devices that convert electricity to the right voltage for transmission and distribution. Transformer lead times have grown from eight to ten weeks before 2020 to well over a year today and are desperately needed to replace the 40 million units (roughly half the total installed in the US) that are already beyond their expected service life.[16] The lack of high-voltage lines and transformers means even if the US can boost its power-generating capacity, it will still be unable to transport that energy to meet increased demand.

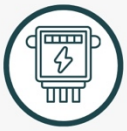
The scale of this demand exposes a structural deficit in American industrial and strategic capacity. The United States cannot build, secure, and operate its way out of this bottleneck without a domestic (or allied) electrotech sector capable of producing the components, integrating the systems, and hardening the architecture at the speed and scale the moment requires. That capacity does not currently exist at sufficient scale, and without deliberate investment, it will not ever exist.

With New Demand Comes New Possibilities

The same data center buildout straining the grid is also accelerating the deployment of exactly the modern, software-defined electrotech that, if deployed well, holds the potential to rebuild the grid on stronger foundations than legacy infrastructure ever could.

The Grid is Modernizing, But Governance Isn't

America's electrical grid is rapidly evolving from a centralized, unidirectional system, where large power plants push electricity outward to passive consumers, into a dynamic, software-coordinated network where energy can be generated, stored, and redirected at thousands of points. Several developments illustrate the shift:



- **Behind-the-meter (BTM)** assets are energy resources located on the customer's side of the utility meter, ranging from rooftop solar and residential batteries to the gas turbines and utility-scale battery storage now being co-located with hyperscale data centers. Because they can generate, store, and dispatch electricity independent of the public grid, they give facilities like data centers a degree of flexibility and independence. But they also mean that consequential energy decisions are often being made by private operators outside the visibility of traditional grid authorities.[1]

- **Battery energy storage systems (BESS)** can absorb excess generation, discharge during peak demand, stabilize frequency, and even "island" a facility—electrically separating it from the broader grid to maintain operations during an outage. Their value depends on sophisticated, software-defined battery management systems (BMS) that control charging, safety protocols, and grid interaction in real time, often via cloud-connected platforms.[2]

- **Virtual Power Plants (VPPs)** aggregate distributed energy resources (DERs)—such as rooftop solar, batteries, EV chargers, smart appliances, or even the aforementioned behind-the-meter assets—and coordinate them through software to behave as a single, dispatchable power source. A VPP can respond to peak demand or grid stress by drawing on thousands of small assets simultaneously, functioning as a "shock absorber" for the grid. Because VPPs depend entirely on software-defined orchestration, they embody both the promise and the sourcing questions at the heart of the electrotech stack.[3]

- **Reconductoring** replaces the physical cables along existing transmission corridors with higher-capacity alternatives. Today's upgraded conductors increasingly incorporate digital controls and sensors capable of adjusting flows in real time, making transmission infrastructure smarter—but also introducing software-defined components into parts of the grid that were previously purely physical.[4]

- **Inverters** convert the direct current produced by assets like solar panels or battery storage into the alternating current the grid uses. Once passive devices that simply disconnected at any disturbance, inverters are becoming increasingly "smart" in actively supporting the grid, such as by regulating voltage, riding through faults, and adjusting output to stabilize electrical frequency in real time. Smarter inverters' firmware, communications protocols, and cloud connectivity are increasingly turning them into operationally consequential control nodes.[5]

Each of these developments is leveraging digitally-native electrotech tools to make the grid more capable, defensible, and resilient, but they are also spotlighting a widening regulatory gap. Federal cybersecurity standards for the grid—principally the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) requirements—were designed specifically for the large-scale generation plants and high-voltage transmission of the bulk power system. Most of the grid's digital evolution, however, is happening outside that perimeter in distributed assets, behind-the-meter installations, and the software platforms that coordinate them.[6] The result is that the fastest-growing and most digitally complex parts of America's energy infrastructure are the least governed by the cybersecurity and supply chain frameworks meant to protect it.

1. Thomas Seeber, "Behind-the-Meter Power: The New Backbone of Data Center Growth," *Data Center Dynamics*, January 8, 2026, https://www.datacenterdynamics.com/en/opinions/behind-the-meter-power-the-new-backbone-of-data-center-growth/.
2. Alejandro Robles, "BESS Europe: Storage Industry Growth and Examples of Its Application," Green Power Monitor, April 2, 2026, https://www.greenpowermonitor.com/articles/bess-europe-storage-industry-growth-and-application/.
3. "The Symbiotic Role of Virtual Power Plants in Grid Stability," GridScape, February 26, 2024, https://grid-scape.com/the-symbiotic-role-of-virtual-power-plants-in-grid-stability/.
4. Yannic Rack, "Rewiring the Power Grid," *Our Industrial Life*, February 21, 2025, https://www.aveva.com/en/our-industrial-life/type/article/rewiring-the-power-grid/.
5. Interstate Renewable Energy Council (IREC), "Smart Inverters," accessed April 18, 2026, https://irecusa.org/our-work/smart-inverters/.
6. NERC, *Critical Infrastructure Protection Roadmap* (NERC, 2026), https://www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf.

First, behind-the-meter assets—energy resources located on a customer's side of the utility's consumption meter—offer critical facilities new sources of electricity that may never interact with the public grid. Unlike grid-dependent solutions, this means behind-the-meter deployment partially but meaningfully offsets the infrastructure shortage described above. These assets also create potential de facto microgrids that, if hardened, could maintain operations through disruptions or outages. The trend is already significant; an estimated 25–33% of incremental data center demand through 2030 will be met by BTM solutions and co-located generation, where developers pair a new data center with dedicated on-site power, typically gas-fired generation combined with battery storage. [17]

Flexible load management is poised to take these capabilities even further, allowing the grid to evolve from one-way distribution into a multi-directional network that can shift consumption, inject stored energy, and curtail imbalances on demand. Google has demonstrated what this can look like in practice for data centers, operating facilities able to modulate the timing and intensity of computation to shift the impact of their demand on the public grid. The company has designated up to one gigawatt of data center capacity for curtailment under demand response agreements with five US utilities.[18]

This kind of coordination increasingly depends on exactly the kind of software-defined, digitally active control layers that this paper's framework identifies as the most systemically consequential. Cloud-hosted platforms like Virtual Power Plants—which aggregate distributed resources and coordinate them through software to behave as though they were singular dispatchable assets—now orchestrate real-time dispatch decisions across behind-the-meter generation, storage, and consumption at speeds and sophistication that legacy infrastructure operations cannot match. By additionally pooling compute resources across facilities and dynamically allocating workloads, cloud operators can achieve 40–60% average server utilization when compared to 5–15% utilization in conventional data centers,[19] translating to three-to-five times more computing work per watt.

Deployed well, these capabilities would make our electricity architecture more dynamic and defensible. Software-orchestrated infrastructure can extract more capacity from existing systems, deliver more compute per watt, reduce the land and energy footprints of an historically-disruptive expansion, and—because a meshed, multi-directional grid has inherently greater capacity for self-healing and recovery—make the resulting system more resilient to disruption and attack.[20]

Software-orchestrated infrastructure can extract more capacity from existing systems, deliver more compute per watt, reduce the land and energy footprints of an historically-disruptive expansion, and—because a meshed, multi-directional grid has inherently greater capacity for self-healing and recovery—make the resulting system more resilient to disruption and attack.

Whether that happens depends on who builds, governs, and secures the software-defined control layers, and today, those layers are largely ungoverned.[21] Historically, utilities and infrastructure operators bore direct accountability for grid reliability—they owned the assets, controlled the flows, and answered to regulators for every deviation. The addition of behind-the-meter generation, storage, VPPs, and software-driven energy management systems fundamentally changes that balance. A hyperscaler running a cloud-managed demand flexibility program across thousands of facilities, for example, is making real-time decisions that affect grid behavior, but outside the visibility and control of any traditional grid operator. A critical facility running co-located solar and storage, with flexible load optimized by an AI-assisted energy management system, is more resilient in most scenarios, but its failure modes are novel, harder to model, and potentially synchronized across facilities in ways that create systemic risk that no single operator can see.

The US regulatory architecture was not built for this landscape. National cybersecurity standards for the grid, principally through the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) requirements, were designed for a power system built around large, centralized plants and high-voltage transmission lines that defined the grid for most of the twentieth century. However, most of these new technology additions to the grid are happening outside that perimeter. The most capable components of America's grid are also the most digitally active, the most systemically influential, and, at present, the least subject to the security frameworks meant to protect critical infrastructure.

When States Fill Governance Gaps: Subnational Policy with Global Consequences

California's vehicle emissions standards provide a historical case study demonstrating how a single state's regulatory choices can reshape national and even global markets. When a subnational jurisdiction represents enough demand, manufacturers often design to that jurisdiction's standards rather than maintain parallel product lines.[1] Virginia and Texas are emerging as holding similar potential influence over energy infrastructure and electrotech equivalents.

Northern Virginia is the largest data center market in the world, with 40 GW of contracted data center power demand as of late 2024—up 88% in just six months.[2] By 2030, data centers may consume as much as 57% of Virginia's total electricity.[3] Virginia's state legislature has responded with measures like HB 434, which requires utilities to demonstrate they are deploying batteries, virtual power plants, and demand response to extract latent capacity before relying solely on new construction, and the FAST Act, which targets interconnection queue delays—the years-long backlog of projects waiting for permission to connect to the grid—by allowing new storage projects to connect at underutilized renewable sites with spare capacity.[4]

Texas, with its cheap land, cheap energy, and relatively deregulated grid, hosts 375 operating data centers with more under construction.[5] Meta's gigawatt-scale facility in El Paso may be among the Lone Star State's highest-profile projects, but the density of activity across Austin, Houston, Dallas, and San Antonio suggests the region is beginning to function as a coherent computing cluster market rather than a collection of discrete projects.[6]

What Virginia and Texas require of electrotech components—in procurement standards, interconnection rules, and cybersecurity baselines—could shape supplier behavior well beyond their borders, potentially as widely as California's tailpipe standards effectively set a longtime floor for the national and international automobile market.

1. Richard Perkins and Eric Neumayer, "Does the 'California Effect' Operate across Borders? Trading- and Investing-Up in Automobile Emission Standards," *Journal of European Public Policy* 19, no. 2 (2012): 217–237, https://doi.org/10.1080/13501763.2011.609725; Dirk A. Heyen, "Influence of the EU Chemicals Regulation on the US Policy Reform Debate: Is a 'California Effect' within REACH?" *Transnational Environmental Law* 2, no. 1 (2013): 95–115, https://doi.org/10.1017/S2047102512000118.
2. Zachary Skidmore, "Dominion Energy Nearly Doubles Data Center Capacity under Contract to 40GW," *Data Center Dynamics*, February 14, 2025, https://www.datacenterdynamics.com/en/news/dominion-energy-nearly-doubles-data-center-capacity-under-contract-to-40gw/.
3. Katherine Blunt and Jennifer Hiller, "America's Biggest Power Grid Operator Has an AI Problem—Too Many Data Centers," *Wall Street Journal*, January 13, 2026, https://www.wsj.com/business/energy-oil/power-grid-ai-data-centers-1235f296.
4. Virginia Legislative Information System, "HB434 - 2026 Regular Session," March 12, 2026, https://lis.virginia.gov/bill-details/20261/HB434; Virginia Legislative Information System, "SB508 - 2026 Regular Session," March 12, 2026, https://lis.virginia.gov/bill-details/20261/SB508.
5. John Bleasby, "Renewable Energy Is Key to Powering Texas Data Centers," *Construction Connect News*, January 5, 2026, https://news.constructconnect.com/renewable-energy-is-key-to-powering-texas-data-centers.
6. Marshall Benveniste, "Meta Announces Plans for $1.5B Texas Data Center in El Paso," *ConstructConnect News*, October 20, 2025, https://news.constructconnect.com/meta-announces-plans-for-1.5b-texas-data-center-in-el-paso.

THREAT LANDSCAPE: DISTINGUISHING REAL RISKS

The electrotech stack faces well-documented security risks, and the United States too often compounds them with siloed, narrow, or undisciplined responses. The security risks themselves are serious; our energy ecosystem's hodgepodge of old and new technology platforms already faces a bevy of cybersecurity and supply chain challenges. It is untenable for our much-needed wave of expansion and modernization to depend so deeply on a strategic competitor for the digitally-active components that increasingly govern how power is generated, stored, and directed across the grid.

But the emerging policy response risks an additional and different kind of failure—one not of inadequate defense, but of overreach and paralysis. By treating every Chinese-manufactured component as equally dangerous or every supply chain dependency as equally urgent, Washington risks stalling the very energy and manufacturing buildout the United States needs to regain industrial leadership. Refusing to build because one cannot yet build "perfectly" may be as perilous as building without security at all.

Malicious Cyber Capability and Intent Amid a Digitizing Grid

China's interest in disrupting US energy infrastructure is not speculative; it is doctrinally grounded, operationally resourced, and already in execution. People's Liberation Army (PLA) military strategy texts explicitly identify energy systems alongside telecommunications, transportation, and financial infrastructure as priority targets for cyber and electromagnetic attack, with the strategic logic that disrupting civilian infrastructure would impede US decision-making and fracture the political will to intervene in Taipei's defense in any contingency over Taiwan.[22] Chinese President Xi Jinping has reportedly directed the PLA to develop the capabilities to execute such disruption by 2027—the centennial of the PLA and the target year for achieving the military readiness Beijing considers essential for any operation to forcibly reunify with Taiwan.[23]

The prepositioning to enable such attacks on American infrastructure has already begun. Senior US officials have testified before Congress that PRC cyber actors—publicly tracked under monikers including "Volt Typhoon"—are actively establishing persistent, remote access to US critical infrastructure networks, including energy systems.[24] Their activities suggest their intent is not intelligence collection, but contingency preparation: patient movement from internet-connected networks into operational technology systems, and digital burrowing so as to be ready to enable disruptive attacks if a crisis materializes. While the PRC has been attempting to gain cyber-enabled footholds inside US infrastructure for years, this current campaign reflects a tempo and focus consistent with capability being built for a specific decision window.

But the PRC is not the only cyber threat to US energy infrastructure. Russian, Iranian, and North Korean actors have long targeted US critical infrastructure and that of allies and partners, and in Russia's case, demonstrated the capacity to cause real operational disruption. As Russia's conventional military campaign stalled in late 2022, Russian actors escalated cyber operations against Ukrainian power companies, building on industrial control systems (ICS) intrusion techniques developed in their 2015 attacks on Ukrainian energy infrastructure.[25] Most recently, following US strikes on Iran in 2026, Iranian actors compromised US industrial control systems in a direct attack on US energy infrastructure.[26] Each of these examples highlights that the cyber threat to electrotech components is not limited to any one adversary and will persist regardless of whether tensions escalate with the PRC.

Much of this prepositioning and disruption have exploited the "seams" between legacy and modern systems—the patchwork of old and new infrastructure where security models conflict with useability, visibility is limited, and attackers can too easily traverse systems largely undetected. These vulnerabilities predate the current electrotech era; they are artifacts of decades of bolting network connectivity onto industrial systems never designed for it.[27] The electrotech transition is not creating this problem, but it does raise the stakes. As software-defined components assume greater control over grid operations, the consequences of exploiting those seams grow more severe, and the digitally active control layers being deployed into that environment inherit the security debt of the infrastructure they connect to.[28]

Concentration Risk and Economic Security Threats in an Interdependent but Asymmetric Market

The PRC also maintains systematic dominance of the electrotech stack's supply chain, giving Beijing an economic pathway to hobble the United States' rapidly-digitizing infrastructure. Beijing built this dominance through a multidecade industrial strategy to acquire intellectual property, scale manufacturing, drive domestic adoption of electrotech technologies within the PRC, and lock in market share across key layers of the stack, with staggering results.[29] PRC vendors in 2025 controlled as much as 90% of the cellular Internet-of-Things module market and 85% of the cellular chipset market.[30] As of 2024, PRC inverter exporters accounted for two-thirds of all inverter shipments globally.[31] And in 2023, China produced 74% of the world's battery pack and component exports.[32] This dominance creates enormous leverage for the PRC to exert over the United States and other nations.

Beijing has already shown its willingness to weaponize supply leverage. Its recent restrictions on US access to critical minerals essential for electric motors, inverters, and battery systems demonstrated both the capability and intent to deprive US markets of electrotech inputs at

> *Without a coherent industrial strategy, the United States risks financing its own strategic vulnerability one procurement decision at a time.*

moments of geopolitical tension.[33] If China continues to dominate these key supply chains, Beijing could not only cut off inputs, but finished goods as well—leverage that in a prolonged crisis becomes a potential chokehold on the very infrastructure buildout the United States is racing to complete. Without a coherent industrial strategy, the United States risks financing its own strategic vulnerability one procurement decision at a time.

Yet for much of our electrotech infrastructure, a hostile supply disruption would likely manifest more akin to a chronic industrial problem—however painful—than an acute operational emergency. If, for example, Beijing cut off US access to Chinese-manufactured solar panels tomorrow, every panel already installed would continue generating electricity with no fuel or material resupply required. The crisis would be one of future deployment pace and cost, not of immediate grid failure. The same is broadly true across much of the electrotech stack's commodity hardware.

Slower-moving does not, of course, mean lower stakes. Industrial capacity is itself a national security asset and chronic dependency on our principal strategic competitor for the technologies underpinning our critical infrastructure is still an intolerable long-term risk. The technical risk embedded in these supply chains is the clear and present danger, the failure that would register first in any crisis, and that policymakers will have to triage most urgently. But triage is not a strategy; reducing the underlying concentration risk is the work of a decade, not a budget cycle, and that course correction must begin while the acute risks are still being managed.

When Supply Chain Dependency Worsens Cyber Vulnerability

This supply-chain dependency worsens another category of risk: cybersecurity exposure through the digitally active control layers that vendors build, maintain, and retain persistent access to long after sale.

Unlike theoretical backdoor "spy chips" or observed cyberattacks, which require active exploitation of physical component access or software bugs to enable remote operation, many modern infrastructure components are explicitly designed with routine remote control built directly into their firmware (the embedded software that governs a device's core operations). This

access is not inherently malicious, but rather, enables continued diagnostic monitoring, software updates, and performance management long after sale. But this same remote access channel provides technical capability to surveil operational patterns, degrade performance, alter operating parameters, or even disable equipment entirely.[34] China's National Intelligence Law reinforces this concern: it requires Chinese organizations and citizens to "support, assist, and cooperate" with national intelligence operations—a legal framework under which manufacturers cannot refuse government directives to modify firmware, retain access, or support intelligence objectives through their products.[35]

In 2020, Russian state-backed hackers compromised SolarWinds, a widely used IT management platform, by inserting malicious code into a routine software update that was then distributed to thousands of organizations—including US government agencies—through the company's own trusted update channel. The breach demonstrated at scale how legitimate channels can be turned into a delivery mechanism for persistent, difficult-to-detect access across thousands of downstream systems. The same logic applies to digitally-orchestrated grid systems; the remote access channels that enable routine firmware updates also provide the technical architecture for supply-chain-mediated compromise at fleet scale.

The remote access channels that enable routine firmware updates also provide the technical architecture for supply-chain-mediated compromise at fleet scale.

That theoretical vulnerability has since materialized in reality. In December 2025, Russian state-directed cyber actors executed the first documented attack against distributed energy resources at fleet scale, targeting over thirty facilities connected to Poland's electrical grid. The attackers focused *not* on generation equipment or commodity hardware like solar panels, but on the digital control layer—remote terminal units, human-machine interfaces, firmware controllers, and the VPN infrastructure enabling remote management. Their tradecraft was strikingly similar to Volt Typhoon's operational approach, despite originating from a different state actor, suggesting that the underlying weaknesses to digitizing infrastructure are structural.[36]

The proliferation of undocumented communications hardware in Chinese-origin products compounds these risks. Cellular radios and other communications devices not listed in product specifications have repeatedly turned up in Chinese-origin equipment including port cranes, batteries, and inverters.[37] While this phenomenon is more likely the result of inconsistent inventory management than deliberately nefarious "spy chip" insertion, it still creates latent vulnerabilities

that could facilitate de facto backdoor access. Such undocumented hardware is potentially widespread across deployed infrastructure, representing a tempting asset for a state actor in any future crisis. These risks compound against the governance shortfalls described in the preceding section; remedying electrical equipment vulnerabilities is a challenge when only an estimated 10–20% of the US electricity system falls under federal cybersecurity oversight, and the fastest-growing parts of the grid's digital architecture remain largely outside the security frameworks meant to protect it.[38]

Countering Panic and Paralysis

The risks described above are serious, but the *policy response* faces a different kind of peril. The most strategically underweighted danger to the US energy ecosystem may not come from Beijing, but from self-inflicted paralysis—whether through overcorrection that delays adoption of modern technologies and throttles the industrial buildout, or through indecision that continues ceding agency to our competitors. Cyber threats from the PRC and other actors are grave, but conflated security concerns around specific technologies are inhibiting effective mitigation of them. Indiscriminate bans on foreign equipment with no rapidly available domestic or allied substitutes, for example, will not protect the US industrial base. Technical risk imprecision instead creates deployment and regulatory uncertainty, threatening to derail grid modernization and handing Beijing a different kind of victory than the one it could achieve through active disruption—the stalling of US energy expansion by our own hand.

Cyber threats from the PRC and other actors are grave, but conflated security concerns around specific technologies are inhibiting effective mitigation of them.

At its root, much of this overreaction stems from a failure to distinguish between different categories of risk and from attempting to treat entire product sectors with the same policy instruments. Trade dependency on a strategic competitor for critical industrial inputs is a serious economic security concern that warrants sustained industrial policy attention. But, if the PRC were to cut off US access to Chinese inputs, such a move would not immediately disable infrastructure already in service, but rather, would disrupt manufacturing pipelines and slow future electrotech deployment. That makes supply concentration a serious strategic vulnerability deserving focused industrial policy—such as pursuing allied sourcing, domestic manufacturing investment, or strategic stockpiling—but one whose consequences would unfold over weeks and months, not hours.

Technical compromise of digitally active control layers, in contrast, is an immediate operational emergency. Manipulated firmware or hijacked fleet orchestration software does not wait for a procurement cycle or delayed shipment to inflict damage—it can disable assets, destabilize grid balancing, or trigger cascading infrastructure failures the moment an adversary chooses to act. Supply chain dependency and technical security vulnerability are different problems requiring different solutions and conflating them produces policy that addresses neither well. This paper urges policymakers to prioritize their response according to a framework that takes these factors into consideration, not because commodity input dependence is unimportant, but because the clear-and-present danger of technical compromise in infrastructure control layers demands the most urgent allocation of finite security resources and political capital.

Supply chain dependency and technical security vulnerability are different problems requiring different solutions and conflating them produces policy that addresses neither well.

Part of what makes these distinctions so difficult to draw in practice is that the expertise and authority needed to identify them are themselves also fragmented. No single federal actor sees the electrotech stack as a whole. Technical understanding of grid-connected control systems sits primarily at the Department of Energy (DOE), the asset owners, operators, their suppliers, and the national labs; cyber threat intelligence and network defense expertise sit at the Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA); defense industrial base equities and supply chain tools sit across the Pentagon and Commerce; and sectoral authorities like FERC and NERC operate within jurisdictional perimeters that predate the digital architecture now being deployed inside them. The result is that even when individual agencies identify specific risks accurately, the policy response tends to default to the blunt instruments each can wield independently rather than the calibrated strategy a shared analytical framework would make possible.

And these distinctions do not stop at the product boundary. A single procurement label like “battery storage” can encompass both a digitally active battery management system (BMS) that governs grid interaction and the more passive collection of electrochemical cells beneath it—sometimes irreverently called “electrolyte goo.” These two components carry fundamentally different risk profiles despite being sold together. Policy instruments that operate only at the product level miss this internal gradient and respond to both layers with the same blunt tool.

And even within individual product categories, not all devices present equivalent risk. Much of the public reporting and policy concern regarding inverters, for example, has focused on small residential inverters—devices that, in terms of consequence to the grid, function more like consumer Internet-of-Things hardware than critical infrastructure. Far less scrutiny has been directed at utility-scale central inverters, which are substantially more consequential: They manage large shares of grid-connected generation, function at the operational technology layer, and represent a meaningfully different risk profile. Treating residential and utility-scale inverters as a single product category obscures where the real vulnerability lies—and treating all PRC-manufactured electrotech as a uniform security threat dilutes the credibility of the more serious and urgent concerns.

Treating all PRC-manufactured electrotech as a uniform security threat dilutes the credibility of the more serious and urgent concerns.

The alternative to this indiscriminate posture is not less scrutiny, but more disciplined scrutiny—concentrating defense where compromise would be most consequential and accepting managed exposure where it would not. That discipline is not only analytically necessary but economically enabling; continued or even expanded access to globally sourced commodity hardware—the electrochemical cells, passive solar panels, and other "dumber" inputs where, for example, Chinese manufacturing scale keeps prices low—will help make our industrial buildout more affordable while simultaneously creating the economic headroom to invest seriously in securing the control and orchestration layers where compromise would be most consequential.

That discipline is essential because the same digital architecture that creates these vulnerabilities can be engineered to contain them. When advanced components are properly secured, they can function as "firebreaks," actively containing risks that would otherwise propagate to more vulnerable parts of our infrastructure's digitizing tech stack. A hardened smart inverter with proper access controls and segmented communication, for example, can prevent lateral movement, stopping an attacker who compromises one node from reaching adjacent systems. A properly configured microgrid controller can detect disturbances and electrically "island" itself before a cascading fault can reach the broader grid.

The record of cyberattacks on critical infrastructure demonstrates what happens without these firebreaks. Across documented state-directed cyber campaigns targeting energy infrastructure—from Volt Typhoon, to Poland's recent intrusions, to Russia's attacks on the Ukrainian grid—adversaries have exploited lower-level devices as entry points and stepping stones, but have consistently directed their efforts toward the more software-defined control layers where systemic effect is achievable.[39] Attackers compromise commoditized hardware to gain a foothold, but it is the

control and orchestration layers that determine whether an intrusion can scale from a single device to grid-wide consequence—and it is at those layers that properly architected defenses can stop it. The question facing infrastructure defenders is not whether to deploy digitally active components, but whether the control layers governing their behavior are secured, sourced, and architected to function as the "firebreaks" that contain risk rather than the pathways that propagate it.

Getting these distinctions right is both possible and consequential. A policy posture that discriminates between control-layer and commodity risk can concentrate defense where it matters while preserving the deployment speed the buildout demands. Getting it wrong weakens US technology security policy, risks triggering the industry skepticism and allied resistance that would undermine the broad-based coalitions necessary to address the real threats, and hands adversaries a ready-made narrative that legitimate security concerns are merely thinly-veiled protectionism—making coordinated action harder to sustain at precisely the moment it is most required.

A "MONEYBALL" RISK AND OPPORTUNITY PRIORITIZATION FRAMEWORK

Getting those distinctions right—ranking risk according to a component's reach and systemic influence, mediating trust at the boundaries between layers, and architecting interlocking defenses that contain compromise rather than assuming it away—requires a discipline that already has a proven model in digital security. Zero-trust networking, which is now standard practice across federal systems and major enterprises, replaced the older perimeter-defense model. Rather than assuming that anything inside the network boundary is safe, the zero-trust approach builds an architecture that assumes a cyber breach is inevitable, authenticates and monitors at every boundary, and contains breaches so they cannot propagate laterally. A digitizing grid demands the same logic—and the electrotech stack, if properly architected, can deliver it.

The same software-defined, networked capabilities that make electrotech components a target also makes them capable of functioning as an active security architecture: monitoring behavior at every layer, enforcing trust boundaries between globally sourced commodity hardware and the control systems that govern grid operations, and isolating compromised components before disruption can propagate. The question becomes not whether to use globally sourced components, but which layers of the stack must be secured and sourced to function as those trust boundaries, and which can tolerate diverse global supply chains because the architecture above them constrains risk.

But the scale of applying that principle to the electrotech buildout is enormous. America's electrical infrastructure spans millions of components with deeply globalized supply chains, each product assembled from bills of materials that may cross dozens of borders before reaching a single substation or data center. And as this paper has established, the components in question do not stay in the energy sector—they are the same industrial base increasingly underpinning competitiveness in defense, autonomous systems, AI infrastructure, and advanced manufacturing. Every sourcing decision made for today's grid expansion is rippling across those sectors, making the cost of getting prioritization wrong, or of failing to prioritize at all, compound far beyond electricity. No government has the resources, regulatory bandwidth, or political capital to subject every component to the same level of security scrutiny, and attempting to do so would paralyze the very buildout that national competitiveness depends on. The question is where to concentrate.

Even the F-35, the most advanced fighter aircraft in the US arsenal, does not have zero Chinese-made components.[40] The defense industrial base applies a risk-based framework to distinguish which components genuinely demand domestic control from those that can be safely sourced elsewhere, accepting managed risk at lower-consequence layers in order to concentrate resources on the components whose compromise would be most catastrophic. The electrotech stack demands

similar discipline, applied through the zero-trust lens established above, where the goal is not to vet every component equally but to identify which layers must function as trust boundaries and concentrate the most rigorous sourcing, security, and industrial investment there.

This question is fundamentally a resource allocation problem. A smaller-market sports team cannot afford to pay top dollar at every position—it wins by identifying where investment produces disproportionate returns. The same "Moneyball" discipline applies here. A trailing industrial power—especially one with a smaller population and industrial base—wins by identifying the positions where a single, well-placed investment can determine the outcome of the whole game.

A trailing industrial power—especially one with a smaller population and industrial base—wins by identifying the positions where a single, well-placed investment can determine the outcome of the whole game.

First, policymakers must assess the technologies across the electrotech stack to determine which to prioritize using the following three tests:

1. **Which technologies enable the most urgent needs in our current energy moment?** This assesses how quickly this technology is being deployed at scale, whether the cost-curve lock-in (the point at which a technology's manufacturing economics become so entrenched that switching to alternative sources becomes prohibitively expensive) is imminent, and what standards are being developed.
2. **Which technologies constitute the biggest vehicles for risk—but also the most systemically influential opportunities to mitigate it?** This assesses how operationally dependent the ecosystem is on that component, whether the component, if foreign made, creates plausible attack vectors, and the expected scope of systemic damage—the "blast radius"—if that component were compromised or disabled. A related design question is whether the technology stack can be architected with deliberate firebreaks—the trust boundaries described above—that segment systemically important components and higher-risk layers in ways that allow policymakers and engineers to capture the economic and technical advantages of globally sourced hardware while containing the security exposure of the control and communications layers that govern grid behavior.
3. **What technologies possess security and capacity solutions that would also position us for future industrial competitiveness?** This assesses whether control of this component provides significant cross-sector spillover advantage, thus offering opportunity for industrial leadership.

Using this assessment to identify the key electrotech products or sub-components, the United States must then make the hard choices of sorting each into one of three tiers of priority:

- **Tier 1: Tight domestic control requirements:** Components where the combination of security consequence, deployment urgency, and industrial leverage is highest. Policy should prioritize domestic manufacturing capacity and procurement restrictions on adversary-origin equipment, similar to the urgent attention given to semiconductors with the CHIPS and Science Act.
- **Tier 2: Cyber-shoring and trusted-ally-sourcing:** Components with meaningful security risk but where trusted-ally supply chains (e.g., those of the Five Eyes, Japan, South Korea, or the European Union) can adequately substitute. Policy should focus on vetting, standards, and ally-shoring agreements rather than full domestic mandates.
- **Tier 3: Managed global sourcing with risk mitigation:** Components where security risk is lower, alternatives are readily available, or domestic strategic value doesn't justify the cost of restriction. Policy should focus on transparency, testing regimes, and procurement hygiene rather than sourcing restrictions.

This tiering logic should apply not only across product categories but within them. In practice, product-level tiering may be the necessary starting point for policymakers and procurers—distinguishing batteries from solar panels, or a Virtual Power Plant's orchestration software from the thermostats it communicates with. But as supply chain strategy matures and competition intensifies, disaggregating higher-tiered products into their "smarter" and "dumber" constituent components will be essential to implementing sourcing and security goals with the precision the framework—and industrial expansion—demands. A battery system that is Tier 1 at the product level could contain electrochemical cells that are Tier 3 at the component level, and policy that fails to make that internal distinction will either over-restrict commodity inputs or under-secure the control layers that actually determine systemic risk.

Contrasting Case Studies: Batteries and Solar Panels

Grid-scale battery storage systems and photovoltaic solar panels are two of the most visible technologies in America's energy expansion, together making up more than 80% of all new electricity capacity added to the grid in 2025.[41] They are frequently cited together as both essential to the grid's modernization, as well as omens of dangerous and deepening Chinese supply chain dependencies. But security and sourcing policies that treat technologies like these as interchangeable obscures many of the critical distinctions this paper spotlights. They differ fundamentally in how they interact with the grid, where their risk concentrates, and what kind of policy response each demands. No responsible strategist would apply the same security frameworks and resources to a single oil derrick in West Texas as they would the Strait of

Hormuz, even though they are both part of the same hydrocarbon technology stack. The distinction is about systemic consequence: one is a commodity asset, the other is a chokepoint capable of cascading disruption.

Realizing the electrotech stack's potential to deliver the industrial abundance and modern resilience it promises will require similarly discriminating logic. Running contemporary battery storage systems and photovoltaic solar panels through this "Moneyball" framework's three tests illustrates not just what each requires, but why the distinction between commodity hardware and systems with systemically influential control layers is the difference that matters most.

1. Which technologies enable the most urgent needs in our current energy moment?

Battery Storage Systems	Photovoltaic Solar Panels
Grid-scale battery storage systems are rapidly becoming a foundational, general-purpose technology across the economy. Their speed, flexibility, and ability to be orchestrated across thousands of distributed assets make them uniquely capable instruments of resilience—a grid-scale battery can island a critical facility during a hurricane, absorb demand spikes during a heatwave, and respond to a cyberattack-induced outage in milliseconds, capabilities that no other single technology currently matches. The scale of deployment reflects growing recognition of that value: US utility-scale battery storage capacity increased 66% over the course of 2024 and batteries will account for 28% of new US power plant capacity in 2026, with data centers serving as the primary drivers of that buildout.[42]	Photovoltaic panels are no less important to the energy buildout, but they occupy a fundamentally different position in it. Solar generation is a scalable, low-cost source of electricity, and an increasingly core procurement strategy for hyperscalers pairing behind-the-meter solar with battery storage. But unlike batteries, PV panels do not perform grid balancing or orchestration functions, and their contribution is more easily substitutable: There are many ways to generate electricity. Batteries, meanwhile, solve a sophisticated, dispatchable resilience problem in a way few other technologies can. Photovoltaic panels are also comparatively low in capital intensity, globally commoditized, and relatively passive by design. These characteristics are making them critical in aggregate but place them in a different category for risk prioritization than the operationally potent, digitally-active role that batteries occupy.[43]

2. ***Which technologies constitute the biggest vehicles for risk—but also the most systemically influential opportunities to mitigate it?***

Battery Storage Systems

Batteries and specifically their battery management systems (BMS), the embedded software and hardware layer that governs how a battery charges, discharges, monitors its own safety, and communicates with the broader grid and cloud orchestration systems—sit at the intersection of generation, storage, and grid dispatch. A battery storage system's compromised BMS could not only disable a single asset, but if connected to the larger ecosystem of control could also destabilize the coordinated load-balancing and frequency response functions that battery-connected infrastructure increasingly depends on. Modern battery storage systems of the kind now being deployed at breakneck speeds are complex products with software-defined, network-connected components whose management and orchestration carry fundamentally different risk profiles than their "dumber" components, such as their electrochemical cells. A compromised BMS could contribute to thermal runaway in individual units. These control and orchestration layers determine whether a battery is an asset or a vulnerability, and they are where near-term technical risk concentrates.

Integrated Battery Energy Storage Systems can thus be considered a Tier 1 system at the product level for this dimension—but the framework's disaggregation principle applies here too. The BMS and its associated firmware and cloud connectivity are squarely Tier 1; the "electrolyte goo" beneath them, while often highly chemically advanced, has a "dumber" cybersecurity profile more akin to passive commodity hardware, and absent the BMS control layer, is likely closer to Tier 3. The trust boundary between them is where a firebreak must sit.

Photovoltaic Solar Panels

Photovoltaic (PV) solar panels themselves are about as "dumb" as electrotech components get, with no embedded software, no network connection, and no real-time command-and-control interface. The picture is growing more complex as associated inverters—the devices that convert a solar panel's direct current output into the alternating current the grid uses—trend toward greater intelligence and tighter integration into consolidated solar hardware, but even a PV system equipped with a smart inverter has a comparatively limited "blast radius." A single compromised solar inverter does not sit at the intersection of generation, storage, and dispatch the way a BMS does. Even in the case of integrated inverters, achieving grid-scale consequence through solar inverters would require aggregating large numbers of them—such as through the very battery storage systems and grid orchestration software that this framework already identifies as Tier 1. The systemic influence, in other words, still concentrates in the control and orchestration layers above the panels, not in the panels themselves.

For the commodity PV hardware, the primary risk remains PRC supply chain concentration disrupting US access through export controls, geopolitical escalation, or targeted coercion—a serious trade dependency warranting industrial policy attention, but a fundamentally different category of vulnerability than the technical security exposure that concentrates higher in the stack. A diversified domestic and global sourcing of PV panels with risk mitigation steps such as country-of-origin disclosure and procurement hygiene could thus protect against that economic risk, and place PV panels in Tier 2 at most.

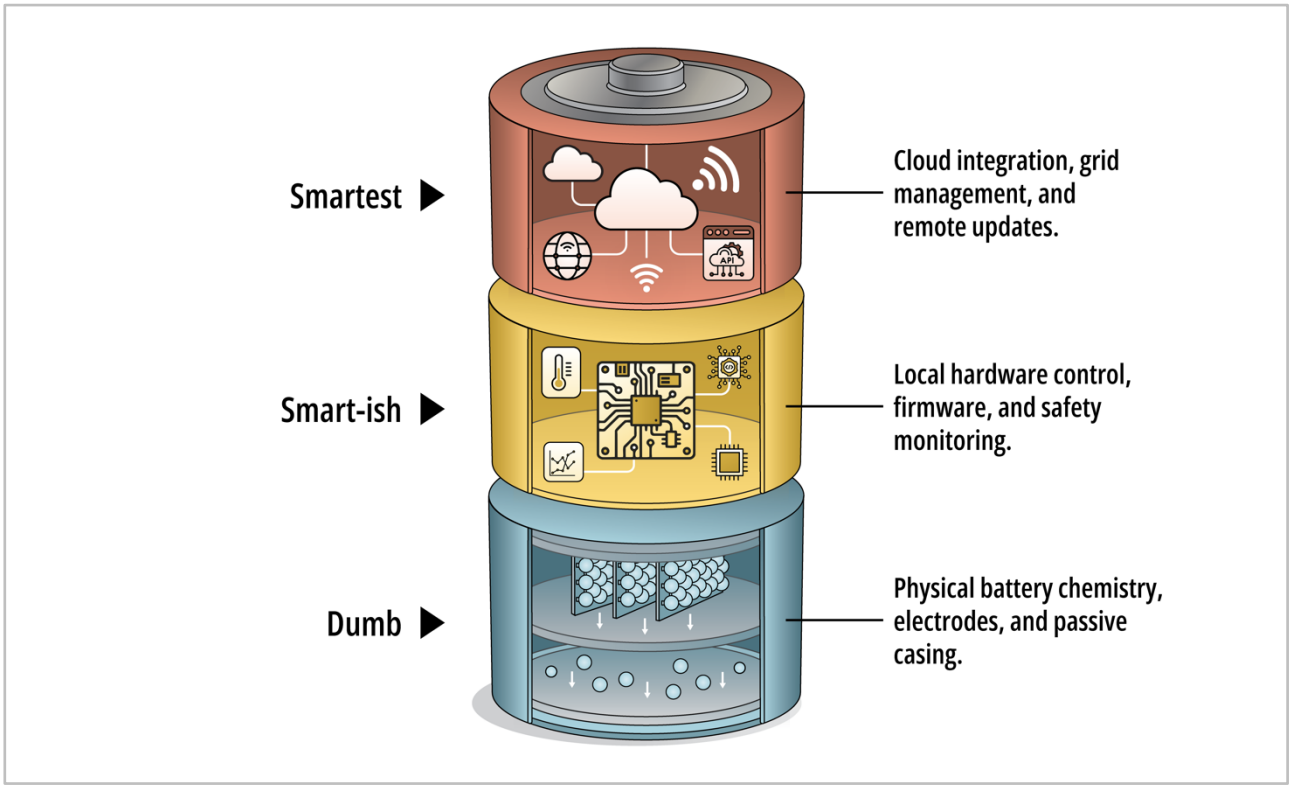


Fig 2: Applying Risk Prioritization to a Grid-Scale Battery System: In modern batteries, the digitally active control layer—cloud-connected software and onboard firmware—is where security risk concentrates and trusted sourcing matters most, while the passive electrochemistry "below" that layer can tolerate diverse global supply chains without comparable consequence.

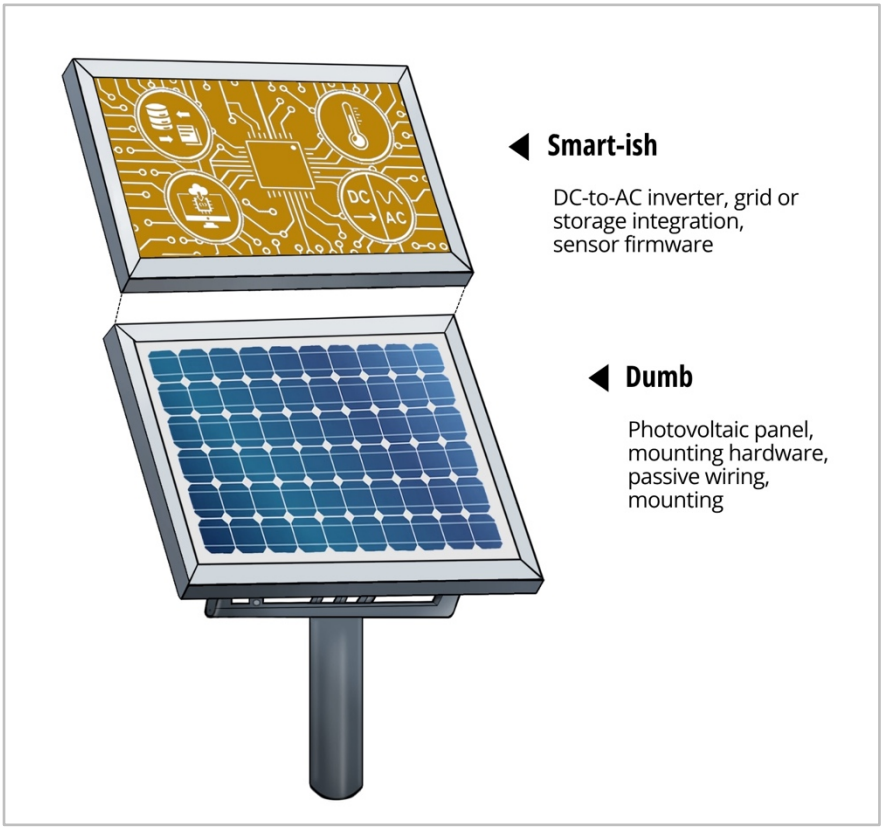


Fig 3: Applying Risk Prioritization to a Photovoltaic Solar System: In photovoltaic solar systems, the digitally active layer is thin—limited primarily to the smart inverter and its grid-interactive firmware—while the bulk of the system is more passive commodity hardware whose primary risk is supply chain concentration, not technical security exposure. Policy attention shifts accordingly, from strict domestic control to diversified allied sourcing and procurement hygiene.

3. ***What technologies possess security and capacity solutions that would also position us for future industrial competitiveness?***

Battery Storage Systems	Photovoltaic Solar Panels
The competitiveness case for batteries is unusually broad. Unlike technologies whose strategic value is confined to a single sector, battery manufacturing sits at a nexus where energy, defense, transportation, and advanced computing increasingly share supply chains, engineering talent, and production economics. The power electronics governing grid-scale battery dispatch share design lineage with those in EV drivetrains and military platforms; the firmware architectures managing fleet orchestration are applicable across autonomous systems and industrial robotics. National leadership in batteries will not stay in the energy sector; it will compound, generating spillover advantages that make battery technology not just an energy security priority but a foundational industrial competitiveness asset. This combination of grid criticality, data center utility, PRC supply chain dominance, rapid deployment timelines, and cross-sector industrial leverage place them at the intersection of every dimension of risk and opportunity this framework is designed to surface.	The competitiveness case for PV panels is narrower and more sector-specific than for batteries. The panels themselves are globally commoditized—mass-produced, low-margin hardware where competing on cost against entrenched Chinese manufacturing scale offers limited strategic return. The stronger competitiveness case lies in the higher-value-add layers above and below the commodity product: upstream in the specialized materials and processing—such as high-purity polysilicon and precision-cut wafers, where China controls more than 80% of global solar manufacturing capacity and over 90% of wafer production specifically—and downstream in the smart inverters and grid-management software where US and allied firms retain genuine technological advantages that policy can actively reinforce.[44] While PV panels in and of themselves are not as compelling a vehicle for driving broad industrial competitiveness as batteries, the upstream and downstream layers where value and strategic leverage concentrate offer real opportunities for targeted policy returns.

The logic embedded in this framework is not an invitation to complacency about Tier 2 and Tier 3 components—defense in depth requires attention at every layer. But layered defense and zero-trust architectures work best when the most rigorous controls are concentrated at the trust boundaries where systemic consequence is highest, precisely because that architecture is what allows components below those boundaries to be sourced more flexibly without accepting proportional risk. The battery case study illustrates the point: a Tier 1 BMS with proper access controls, segmented communications, and trusted sourcing can function as a firebreak that constrains the security exposure of the Tier 3 electrochemical cells beneath it—cells that can then continue to be procured globally at the cost and speed that rapid deployment demands.

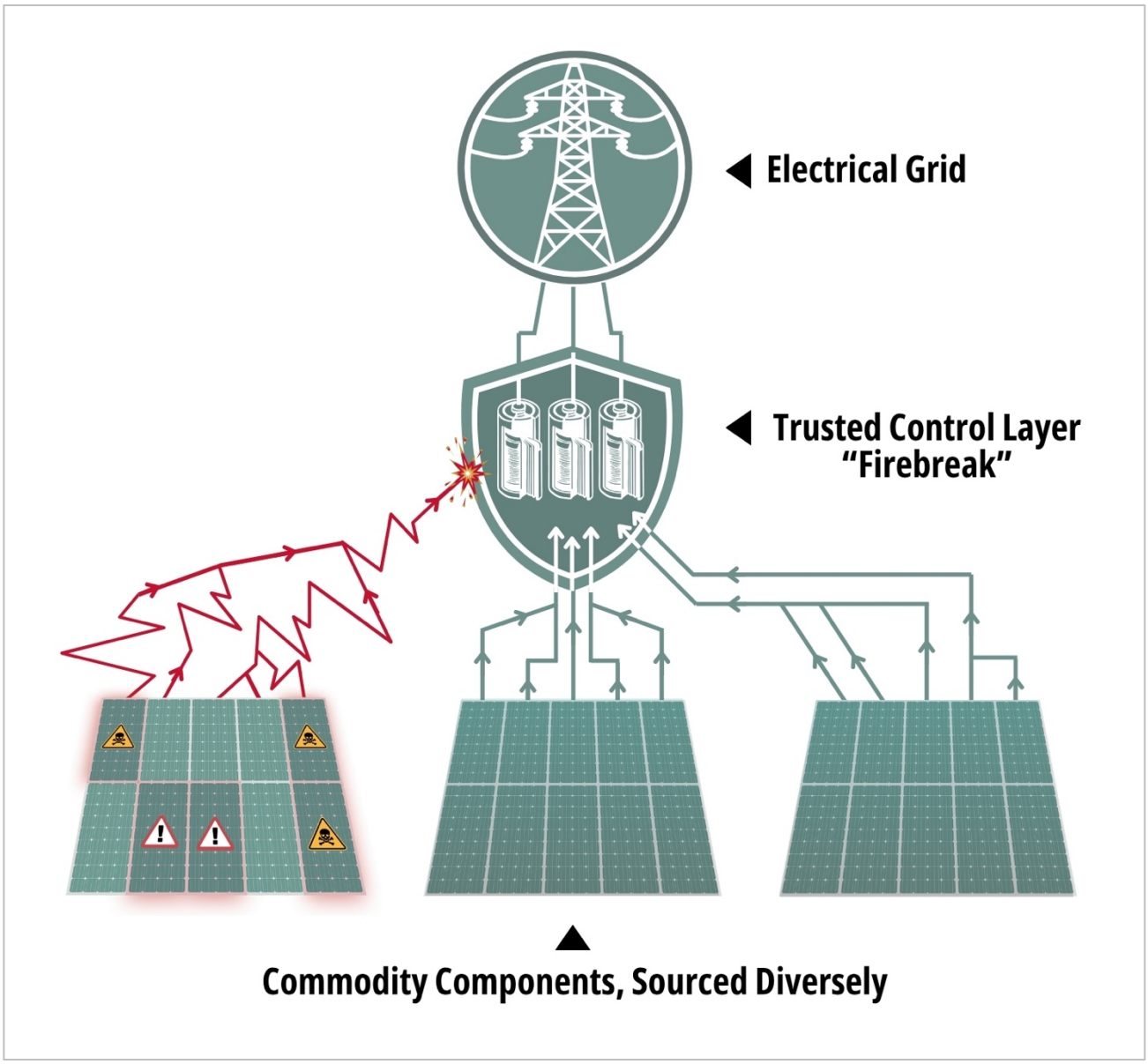


Fig 4: Risk Prioritization and Tech Stack "Firebreaks": A trusted control layer—secured battery management and aggregation software—acts as a "firebreak" between commodity components with diverse (and potentially compromised) supply chains and the grid itself, detecting and isolating anomalous behavior before it can propagate.

POLICY RECOMMENDATIONS

This framework demands discipline about where finite resources, regulatory bandwidth, and political capital concentrate. The United States cannot treat the entire electrotech stack as a national security emergency simultaneously, and attempting to do so risks diluting attention away from the control and communications layers where compromise would be most catastrophic—while simultaneously throttling the commodity procurement that the buildout's pace requires.

The policy recommendations that follow translate this prioritization into action across three horizons: embedding security standards at the most consequential layers of the buildout now underway, building the domestic and allied industrial capacity to make those standards credible, and pursuing the broader electrotech industrial strategy that reduces structural dependency over time.

The United States faces a rare opportunity to secure the infrastructure upon which the next generation of innovation will depend while also maximizing its industrial competitiveness. In pursuit of this goal, Washington should prioritize the following policy approaches.

Near Term: Embed Security at the Buildout's Trust Boundaries

The most urgent priority for policymakers and industry is ensuring the deployment-phase security of the buildout now underway—not after it is complete when remediation costs compound and architectural decisions are too deeply locked in. The core organizing principle should be the framework's "smart vs. dumb" distinction: e.g., a battery system's commodity electrochemical cells warrant less scrutiny than the BMS, firmware, inverter control logic, fleet management platforms, and cloud orchestration layers that give them grid-interactive capability. Applying rigorous security requirements at these systemically influential Tier 1 layers creates a firebreak against risks that could otherwise propagate down the entire stack, while preserving the cost advantages and deployment speed of commodity components where security exposure is lower.

Importantly, this is a near-term risk management posture, not a substitute for the longer-term industrial strategy that must follow. Firebreaks can control risk while domestic and allied supply chains are built to depth, but they do not eliminate the structural vulnerability that comes from sourcing high-consequence components from adversaries in the first place.

Closing the governance gap the preceding sections have identified is central to this effort. Federal cybersecurity standards for the grid have historically been designed for the traditional bulk

electric system and largely focused on generation and interregional transmission. Most of the grid's digital evolution, however, is happening outside that perimeter in distributed assets, behind-the-meter installations, and in software platforms that increasingly coordinate them. The result is that the fastest-growing and most digitally complex parts of America's energy infrastructure are often the least governed by the cybersecurity frameworks meant to protect it. No single federal mandate can close this gap. The diversity of state and federal jurisdictions across which these technologies operate demands a similarly diverse set of governance instruments, from voluntary industry commitments and state-level policy to updated federal frameworks were jurisdiction and influence allows.

To that end, the United States should pursue the following near-term actions:

- **Government and industry should extend cybersecurity guidance to the distributed and behind-the-meter digital layers that often lack federal oversight.** This should proceed through multiple, complementary directions, from voluntary commitments by industry consortia establishing shared baselines for what secure integration of digitally active electrotech looks like across diverse utility environments; to state-level procurement and interconnection requirements in high-leverage jurisdictions like Virginia and Texas, where data center concentration makes the stakes concrete and where state-level standards can function as de facto national benchmarks; and updated federal frameworks like NERC-CIP where possible. No single mechanism will span the full regulatory landscape these technologies traverse, and policy should be designed accordingly.

- **Hyperscalers whose data center buildouts are driving the electrotech expansion should co-develop and adopt consequence driven, cyber-informed-engineering procurement baselines for Tier 1 control layers**—such as for BMS firmware, inverter control logic, fleet orchestration software, and cloud-connected energy management platforms. As some of the few actors in the US economy possessing deep expertise in both energy economics and adversary exploitation of software, these companies are uniquely positioned to set market-shaping security practices where regulatory timelines lag deployment realities. Their purchasing power paid a "green premium" that seeded the clean energy marketplace a decade ago; a comparable "security premium" applied to the electrotech control layers they are now procuring at unprecedented scale could catalyze industry-wide adoption of baselines that regulation alone could never deliver at the necessary speed and scale.

- **Policymakers and deployers should prioritize strategic substitution of adversary-origin control components in the highest-consequence locations already in operation**—such as smart inverters, BMS firmware, and communications modules in grid-critical facilities. This could be akin to removing Huawei equipment from telecommunications networks, but earlier in the equipment's deployment cycle where the costs of replacement are significantly lower and the window to act has not yet closed.

Medium Term: Align Trade, Industrial, and Allied Tools to the Framework's Prioritization

Deployment-phase security standards buy time; they do not resolve the underlying structural dependency that makes adversary-origin components a long-term vulnerability. Closing that gap will require aligning the United States' trade, procurement, and industrial policy instruments to the same prioritization logic this paper's framework establishes—and doing so with the within-product precision the case studies illustrate will be necessary.

Today's policy toolkit is not built for that precision. Too many provisions, be they from Foreign Entity of Concern (FEOC) requirements, domestic content mandates, or import security provisions, are applied at the product level—"batteries," "inverters," "solar panels"—rather than distinguishing between a product's digitally active control layers and its commodity subcomponents. The result is a mismatch in both directions: sourcing restrictions that are too frequently applied uniformly across an entire product category risk throttling the commodity procurement the buildout's pace demands, while the same blanket treatment can obscure the control-layer components whose sourcing more directly determines systemic risk. Battery procurement guidance, for example, that treats electrochemical cells, critical mineral content, and cloud-connected BMS firmware as interchangeable inputs conflates risk more than it controls it. Aligning these instruments to a "Moneyball" tiering—concentrating the most rigorous sourcing and domestic content requirements on Tier 1 control layers while allowing managed global procurement for Tier 3 commodity components—would simultaneously sharpen security focus and reduce unnecessary deployment friction.

The same logic applies to the affirmative side. Industrial strategy policies and investments calibrated to this framework's prioritization, rather than spread across the entire electrotech stack, are far more likely to produce durable competitive advantage. The CHIPS and Science Act's apparent early success at catalyzing diversified high-end semiconductor production suggests a model to emulate in its deep investment in relatively narrow technical priorities that sit at chokepoints with significant downstream impact across multiple sectors.[45] The electrotech stack

offers a structurally similar opportunity. Because of the shared industrial heritage this paper has documented—the same production ecosystems and design lineages serving energy, defense, autonomous systems, AI infrastructure, robotics, and other advanced manufacturing—concentrated investment in a small number of linchpin technologies at Tier 1 could generate compounding spillover advantages across all of them in a way that diffuse subsidies across the full stack cannot.

But industrial strategy and sourcing restrictions are only credible *if trusted alternatives exist at scale*. Procurement restrictions on the supply of adversary-origin Tier 1 components that outpace reasonable timelines for domestic and allied manufacturing capacity are more likely to produce paralysis than resilience. Building that capacity will require both proactive investment and demand certainty—the confidence that manufacturers need before committing capital to production lines intended to compete with entrenched Chinese-scale economies.

To that end, Congress, the Executive Branch, and (where appropriate) state and local governments should pursue the following:

- **Calibrate security provisions, Foreign Entity of Concern/Foreign Country of Concern/Prohibited Foreign Entity requirements, and domestic content mandates to a "Moneyball" framework's tiered risk assessment rather than applying them too widely at a product level.** Tier 1 control layers should face the most rigorous sourcing requirements, up to and including country-of-origin restrictions on adversary-manufactured components. Tier 2 components should be governed by trusted-ally sourcing and cybersecurity vetting—rigorous, but short of full domestic mandates where allied supply chains can credibly substitute. Tier 3 commodity components should face transparency, testing, and procurement hygiene requirements rather than sourcing restrictions that would impede deployment speed. Joint venture structures involving adversary-origin partners are not *inherently* disqualifying, they can accelerate capacity and lower costs in commodity layers, but they warrant particular scrutiny where a partner's manufacturing role could provide operational access to Tier 1 control-layer design or firmware, the very channels through which supply-chain-mediated compromise could occur.

- **Prioritize durable demand commitments for domestic and allied manufacturers of Tier 1 components**—be it in federal procurement, state-level interconnection requirements, or hyperscaler purchasing agreements—giving upstart producers the market confidence to invest in scaling capacity against entrenched competitors. Data center builders procuring battery storage systems, inverters, and energy management platforms at unprecedented volumes are the natural anchor customers for this demand signal;

structured procurement commitments from hyperscalers, paired with federal and state purchasing requirements, could provide the demand floor that nascent domestic and allied manufacturers need to justify the capital expenditure of scaling production.

- **Develop coordinated allied procurement frameworks and mutual recognition of security certifications.** Natural partners include Five Eyes nations, Japan, South Korea, and the European Union—allies whose manufacturing capacity can complement domestic production at the tiers where trusted sourcing is most critical. Mutual recognition agreements would reduce the duplicative compliance costs that currently disadvantage allied suppliers relative to cheaper adversary-origin alternatives, accelerating the availability of trusted higher-tier substitutes. Interoperability standards co-developed with these partners would further ensure that allied-sourced components integrate seamlessly with domestically produced Tier 1 control layers, preventing the fragmentation that would undermine the architecture's coherence.

- **Pursue a focused electrotech industrial strategy that treats the highest-priority control layers as a coherent industrial target**—not the entire stack, and not a collection of separate procurement problems. Following the CHIPS and Science Act's model of relatively deep, narrow investment at high-leverage chokepoints, the United States should identify a small number of linchpin electrotech technologies—battery management systems, power electronics, grid-edge software, and motors and actuators among the leading candidates—where domestic or allied manufacturing leadership would generate the broadest cross-sector returns. The goal is a flywheel of self-reinforcing capacity: enough domestic and allied manufacturing depth to ensure that geopolitical disruption cannot strand capital, delay critical buildout, or compromise the control layers that determine whether America's infrastructure grows on its own terms or on its competitors'.

CONCLUSION

This paper has argued that the United States can meet the security demands of its generational energy buildout without sacrificing the speed and scale that buildout requires—but only through the kind of disciplined prioritization the electrotech stack has so far lacked. The "Moneyball" framework it proposes concentrates sourcing scrutiny, security investment, and industrial strategy on the digitally active control layers where systemic compromise would be most consequential, while preserving the managed global procurement that keeps commodity components deployable at necessary speed and cost. The case studies demonstrate that logic on two of the stack's most apparent technologies—the more demanding applications, where the smart-vs.-dumb line blurs further or a risk firebreak must sit at a finer boundary—remain ahead, and will require sustained analytical work across institutions taking the electrotech security challenge seriously.

With the help of frameworks like this, the same forces currently stressing the grid can instead become the basis for structural advantage. The technical foundation for this transformation already exists: dynamic response models, operating agreements governing large load behavior, and cyber-informed engineering embedded at the design stage. A grid whose trust boundaries are architected to contain compromise, rather than assume it away, can confidently absorb gigawatt-scale loads without emergency orders or cascading instability, becoming a platform for accelerated AI deployment, advanced manufacturing, and strategically onshored industrial capacity. Reliability, in this framing, becomes the enabling condition for abundance.

The economic dividends will also compound. A US-anchored electrotech stack reduces long-term cost of capital by lowering systemic risk and improving supply assurance for private investors. It generates domestic manufacturing multipliers through the compounding sectors that share the same industrial base. It creates standards-setting leverage, positioning US firms to define the firmware, interoperability, and cybersecurity norms that shape global markets rather than inherit them. And secure-by-design grid architectures become a differentiated export offering in allied markets, translating domestic industrial policy into international commercial competitiveness.

The choice the United States makes now about how to build, source, and govern its electrotech stack will determine not just grid reliability, but the terms on which it competes for the rest of this century.

[1] The term "electrotech" is not yet standardized across the field. Related formulations include "electrotechnology," used in industrial and engineering contexts to refer broadly to electrical and electronic systems, and "electrotech stack," "electro-industrial stack," or other variants as emerging terms of art in policy and industry discourse. The authors are indebted to the precision and insight of Ember Energy Research's "electrotech" taxonomy.
Ember Energy Research CIC. "The Electrotech Revolution | Ember." Ember, September 16, 2025. https://ember-energy.org/latest-insights/the-electrotech-revolution/#foreword.

[2] Nankya, Mary, Robin Chataut, and Robert Akl. "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies." Sensors (Basel, Switzerland) 23, no. 21 (2023): 8840. https://doi.org/10.3390/s23218840.

[3] Cisa.Gov. "Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA." 2026. https://www.cisa.gov/topics/industrial-control-systems; Alanazi, Manar, Abdun Mahmood, and Mohammad Jabed Morshed Chowdhury. "SCADA Vulnerabilities and Attacks: A Review of the State-of-the-art and Open Issues." *Computers & Security 125* (February 2023): 103028. https://doi.org/10.1016/j.cose.2022.103028.

[4] NERC Critical Infrastructure Protection Roadmap. NERC, 2026. https://www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf.

[5] Smith, Noah. "Why Every Country Needs to Master the Electric Tech Stack." Substack, September 23, 2025. https://www.noahpinion.blog/p/why-every-country-needs-to-master.

[6] Mahan, Josh. "How Many Data Centers Are in the US? Latest Statistics and Trends - C&C Technology Group." Data Centers. C&C Technology Group, May 31, 2025. https://cc-techgroup.com/how-many-data-centers-are-in-the-us/; Fitzpatrick, Alex. "America's Data Center Growth Hot Spots, Mapped." Axios, December 18, 2025. https://www.axios.com/2025/12/18/data-center-growth-map-states.

[7] Moss, Sebastian. "US DOE Identifies 16 Sites on Federal Land for 'Rapid Data Center Construction,' Including 1GW Location." Data Center Dynamics Ltd, April 2, 2025. https://www.datacenterdynamics.com/en/news/us-doe-identifies-16-sites-on-federal-land-for-rapid-data-center-construction-including-1gw-location/.
Zico Kolter, "AI and Its Growing Energy Demand," Work That Matters: Energy Innovation, Carnegie Mellon University, accessed April 30, 2026. https://www.cmu.edu/work-that-matters/energy-innovation/ai-and-its-growing-energy-demand

[8] Energy.Gov. "DOE Releases New Report Evaluating Increase in Electricity Demand from Data Centers." December 20, 2024. https://www.energy.gov/articles/doe-releases-new-report-evaluating-increase-electricity-demand-data-centers.

[9] IEA. "Global Electricity Demand Is Set to Grow Strongly to 2030, Underscoring Need for Investments in Grids and Flexibility - News." February 6, 2026. https://www.iea.org/news/global-electricity-demand-is-set-to-grow-strongly-to-2030-underscoring-need-for-investments-in-grids-and-flexibility;
IEA. "Global Trends – Global Energy Review 2025— Analysis." March 2025. https://www.iea.org/reports/global-energy-review-2025/global-trends.

[10] Federal Energy Regulatory Commission, Energy Infrastructure Update (monthly reports), 2023–2025, https://www.ferc.gov/staff-reports-and-papers.

[11] Reuters, "Big Tech shifts to 'all of the above' strategy to power AI," December 11, 2025, https://www.reuters.com/business/energy/big-tech-shifts-all-above-strategy-power-ai--reeii-2025-12-11/.

[12] Robinson Meyer, "It's the Age of Electricity and America Isn't Ready," New York Times, April 27, 2026, https://www.nytimes.com/interactive/2026/04/27/opinion/electricity-power-grid-infrastructure.htm

[13] *Assessment of Gaps in Existing Practices, Requirements, and Reliability Standards for Emerging Large Loads NERC Large Loads Working Group White Paper.* NERC, 2026. https://www.nerc.com/globalassets/our-work/guidelines/reliability/white-paper---assessment-of-gaps.pdf.

[14] U.S. Department of Energy, "Speed to Power Initiative," Office of Electricity, September 18, 2025, https://www.energy.gov/speed-to-power.
U.S. Department of Energy, "Speed to Power through Accelerated Reconductoring and other Key Advanced Transmission Technology Upgrades (SPARK)," Office of Electricity, March 12, 2026, https://www.energy.gov/oe/speed-power-through-accelerated-reconductoring-and-other-key-advanced-transmission-technology.

[15] "New Report Reveals U.S. Transmission Buildout Lagging Far Behind National Needs." Americans for a Clean Energy Grid. Press Releases, July 21, 2025. https://cleanenergygrid.org/new-report-reveals-u-s-transmission-buildout-lagging-far-behind-national-needs/.

[16] Rosner-Uddin, Rafe, Nassos Stylianou, Dan Clark, Caroline Nevitt, and Jamie Symth. "The Power Crunch Threatening America's AI Ambitions." Financial Times, December 8, 2025. https://ig.ft.com/ai-power/; Patel, Sonal. "Transformers in

2026: Shortage, Scramble, or Self-Inflicted Crisis?" POWER Magazine, January 2, 2026. https://www.powermag.com/transformers-in-2026-shortage-scramble-or-self-inflicted-crisis/.

[17] Clavenna, Scott. "Behind-the-Meter Generation Is Picking up Traction." Latitude Media, October 22, 2025. https://www.latitudemedia.com/news/behind-the-meter-generation-is-picking-up-traction/.

[18] Varun Mehra and Raiden Hasegawa. "Using Demand Response to Reduce Data Center Power Consumption." Google Cloud Blog, October 3, 2023. https://cloud.google.com/blog/products/infrastructure/using-demand-response-to-reduce-data-center-power-consumption; Kearney, Laila. "Google Expands Utility Deals to Curb Data center Power Use during Peak Demand." Boards, Policy & Regulation. Reuters, March 19, 2026. https://www.reuters.com/sustainability/boards-policy-regulation/google-expands-utility-deals-curb-datacenter-power-use-during-peak-demand-2026-03-19/.

[19] Devasia, Anish. "Data Center Energy Consumption Statistics & Data (2026)." Network Installation. The Network Installers, December 29, 2025. https://thenetworkinstallers.com/blog/data-center-energy-consumption-statistics/.

[20] Krejsa, Harry. "Sun Shield—Carnegie Mellon Institute for Strategy & Technology—Carnegie Mellon University." Carnegie Mellon Institute for Strategy and Technology, January 2025. https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html.

[21] *Secure Communications: Interoperability in the Power Grid.* Department of Energy, n.d. https://www.energy.gov/sites/default/files/2023-09/Secure%20Communications%20Interoperability%20Challenges%20in%20the%20Power%20Grid.pdf.

[22] Science of Military Strategy (2013, CASS), translated in "The Science of Military Strategy," in Andrew S. Erickson and Lyle J. Goldstein, eds., Chinese Aerospace Power (Naval Institute Press, 2016); reaffirmed in Science of Military Strategy (2020 edition, CASS) translated in RAND Corporation materials on Chinese military doctrine;
U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China" (2025 Annual Report to Congress), assessment of cyber operations targeting civil infrastructure in crisis scenarios, https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

[23] Aquilino, John C. "Statement of Admiral John C. Aquilino, U.S. Navy, Commander, U.S. Indo-Pacific Command: U.S. Indo-Pacific Command Posture." Testimony before the House Armed Services Committee, March 20, 2024. https://www.congress.gov/118/meeting/house/116960/witnesses/HHRG-118-AS00-Wstate-AquilinoJ-20240320.pdf.

[24] Christopher A. Wray, Statement before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, "The CCP Cyber Threat to the American Homeland and National Security", U.S. House of Representatives, January 31, 2024, https://www.fbi.gov/news/speeches-and-testimony/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party.

[25] Cybersecurity and Infrastructure Security Agency (CISA), "Cyber-Attack Against Ukrainian Critical Infrastructure," ICS-CERT Alert IR-ALERT-H-16-056-01, last modified July 20, 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
Brian E. Humphreys, "Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience," Congressional Research Service Report R48067, May 17, 2024, https://www.congress.gov/crs-product/R48067.

[26] Kevin Collier, "Iranian Hackers Are Breaking into U.S. Industrial Systems, Agencies Warn," NBC News, April 7, 2026, https://www.nbcnews.com/tech/security/iran-hack-break-us-industrial-systems-agencies-trump-target-rcna267162.

[27] Krejsa, Harry. "Sun Shield—Carnegie Mellon Institute for Strategy & Technology— Carnegie Mellon University." Carnegie Mellon Institute for Strategy and Technology, January 2025. https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html.

[28] Chen, Juanwei, Jun Yan, Anthony Kemmeugne, Marthe Kassouf, and Mourad Debbabi. "Cybersecurity of Distributed Energy Resource Systems in the Smart Grid: A Survey." Applied Energy 383 (April 2025): 125364. https://doi.org/10.1016/j.apenergy.2025.125364.

[29] Krugman, Paul. "Chinese Electrotech is the Big Winner in the Iran War." Paul Krugman (Substack), April 14, 2026. https://paulkrugman.substack.com/p/chinese-electrotech-is-the-big-winner.

[30] Takeshi, Niwa. "Cellular IoT Modules Market Outlook 2025-2026: Strong Growth in 2025, Structural Pressures Ahead." IoT Business News, February 10, 2026. https://iotbusinessnews.com/2026/02/10/cellular-iot-modules-market-outlook-2025-2026-strong-growth-in-2025-structural-pressures-ahead/.

[31] Strider Technologies. "Washington Post: '[Strider] Research…Reveals How Deeply Dependent U.S. Power Companies Are on Chinese Inverters.'" December 18, 2025. https://www.striderintel.com/newsroom/washington-post-strider-report-prc-inverters/.

[32] Eia.Gov. "China Dominates Global Trade of Battery Minerals." May 21, 2025. https://www.eia.gov/todayinenergy/detail.php?id=65305.

[33] Tae-Yoon, Kim, Dhir Sobhan, Amrita Dasgupta, and Alessio Scanziani. “With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality—Analysis.” IEA, October 23, 2025. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality.
[34] Ghiretti, Francesca, and Conlan Ellis. “It’s Time to Treat China’s Connected Energy Systems As a National Security Risk | RAND.” Rand, January 21, 2026. https://www.rand.org/pubs/commentary/2026/01/its-time-to-treat-chinas-connected-energy-systems-as-a.html.
[35] National Intelligence Law of the People’s Republic of China (2017), Article 7.
[36] Polish government statement, December 29, 2025; CERT Polska technical report (2026); Dragos threat research (2026).
[37] McFarlane, Sarah. “Rogue Communication Devices Found in Chinese Solar Power Inverters.” Climate & Energy. *Reuters*, May 14, 2025. https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.
[38] Allende, Pedro, Andrew Gumbiner, and John La Rue. *Securing The Energy Transition Against Cyber Threats*. Atlantic Council Task Force on Cybersecurity and the Energy Transition, 2022. https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Securing-the-Energy-Transition-against-Cyber-Threats.pdf.
[39] MITRE Corporation, “ATT&CK for Industrial Control Systems,” ATT&CK Knowledge Base, accessed April 28, 2026, https://attack.mitre.org/matrices/ics/. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI), "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Joint Cybersecurity Advisory AA24-038A, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. The advisory maps Volt Typhoon's activity to the MITRE ATT&CK framework and documents a consistent operational pattern of gaining initial footholds through peripheral assets and moving laterally toward operational technology systems governing critical infrastructure functions.
[40] Hudson, Lee. “Pentagon to Resume F-35 Deliveries after Chinese Materials Discovered.” POLITICO, October 7, 2022. https://www.politico.com/news/2022/10/07/pentagon-f-35-deliveries-chinese-materials-00060962.
[41] Dan McCarthy, "Chart: Clean Energy Remains Dominant in the US—Despite Trump," Canary Media, December 19, 2025, https://www.canarymedia.com/articles/clean-energy/us-new-wind-solar-batteries-2025-trump.
[42] Eia.Gov. “U.S. Battery Capacity Increased 66% in 2024.” March 12, 2025. https://www.eia.gov/todayinenergy/detail.php?id=64705; Spector, Julian. “Suddenly, the US Manufactures a Ton of Grid Batteries.” Canary Media, March 23, 2026. https://www.canarymedia.com/articles/clean-energy-manufacturing/us-capacity-storage-cell-factories.
[43] Krejsa, Harry. “Sun Shield— Carnegie Mellon Institute for Strategy & Technology—Carnegie Mellon University.” Carnegie Mellon Institute for Strategy and Technology, January 2025. https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html.
[44] International Energy Agency, Solar PV Global Supply Chains (Paris: International Energy Agency, 2022), https://iea.blob.core.windows.net/assets/2d18437f-211d-4504-beeb-570c4d139e25/SpecialReportonSolarPVGlobalSupplyChains.pdf
US Department of Energy, Solar Energy Supply Chain Report (Washington, DC: US Department of Energy, February 2022), https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf
[45] Skanda Amarnath, "Did the CHIPS Act Trigger the Manufacturing Construction Boom?" Factory Settings, March 9, 2026, https://www.factorysettings.org/p/did-the-chips-act-trigger-the-manufacturing.
Semiconductor Industry Association and Boston Consulting Group, "Emerging Resilience in the Semiconductor Supply Chain," May 2024, https://www.semiconductors.org/emerging-resilience-in-the-semiconductor-supply-chain/.