Carnegie Mellon Institute
for Strategy & Technology

JANUARY 2025

WHITE PAPER

SUN SHIELD

How Clean Tech & America's Energy Expansion Can Stop Chinese Cyber Threats

By Harry Krejsa

Carnegie Mellon University

About the Author

Harry Krejsa is the Director of Studies at the Carnegie Mellon Institute for Strategy & Technology. Harry joined Carnegie Mellon from the White House's Office of the National Cyber Director, where he led development of the 2023 National Cybersecurity Strategy, established national clean 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 U.S.-China competition for the Department of Defense, the Cyberspace Solarium Commission, and the Center for a New American Security.

Acknowledgements

The author is indebted to many friends, colleagues, and mentors who contributed immeasurably to the production of this report. The support and feedback from Audrey Kurth Cronin, Ralph Lopez, and Costa Samaras were invaluable. Project guidance and design provided by Jess Regan and Carolyn Just were critical. Editing by Sandra Tolliver was excellent. While many contributed to this research effort, the views herein are the author's alone, along with any errors of fact, omission, or interpretation.

This report and its findings are the sole responsibility of the author. Cover illustration by Jess Regan.

TABLE OF CONTENTS

Executive Summary 1

Distinct Threats With the Promise of Shared Solutions 3

Preparing the Battlefield for Zero-Carbon Reinforcements 5

- Architecture 6
- Technology 8
  - Smart Inverter Controls & Power Conversion Equipment 9
  - Batteries 10
  - Virtual Power Plants 11
- Governance 13
  - Technical Standards and Design Principles for Security 14
  - Industry Coordinating Bodies and Public-Private Information Sharing 15

Policy Recommendations: Building Strategic Unity Against Both Climate Change and Great Power Conflict 17

- Line of Effort 1: Make Clean Energy Security a Core Area of Competition with China 18
- Line of Effort 2: Build and Strengthen a “China Risk / Climate Risk” Community of Practice Across the Public and Private Sectors 21
- Line of Effort 3: Adopt a Near-Term Risk and Opportunity Prioritization Framework 24

Endnotes 28

EXECUTIVE SUMMARY

China's cyber operatives are actively embedding disruptive capabilities on America's critical infrastructure, seeking to sow chaos during a potential conflict and slow our ability to mobilize in response.

This infiltration, confirmed by the United States' top security officials, exploits decades of haphazard digitization that has left U.S. infrastructure aging and vulnerable. The clean energy transition and broader energy expansion—accelerated by recent federal investments and growing artificial intelligence electricity demand—presents an opportunity to counter this threat. If implemented strategically, this transformation will offer a once-in-a-generation chance to replace fragile legacy systems with inherently more defensible, software-defined clean energy technologies. If implemented poorly, however, this transition will risk magnifying our infrastructure's existing weaknesses.

The clean energy transition is fundamentally reshaping our electrical grid's architecture, replacing centralized, "analogue" fossil generation with distributed, "digitally-native" clean energy technologies. These more sophisticated components of the transition, like smart inverters, battery storage, and virtual power plants, were designed from the ground up to be software-defined and networked, unlike our legacy infrastructure, which had internet connectivity awkwardly grafted onto systems that were never meant to be accessible to the outside world. Moreover, these technologies are capable of more than just decarbonization and cyber resilience—they could fundamentally reshape our relationship with energy scarcity itself. Digitally-enabled clean electricity generation that requires little to no additional fuel or maintenance to operate—like zero-marginal-cost solar, geothermal, or nuclear—could drive an unprecedented level of resource abundance and affordability, catalyzing broader economic and security benefits that we are only beginning to understand.

Realizing these benefits requires overcoming significant challenges. Heavy dependence on Chinese manufacturing in key clean energy technologies creates supply chain vulnerabilities. Fragmented regulatory oversight leaves significant portions of electrical infrastructure beyond federal cybersecurity oversight. New, clean energy market entrants often lack security expertise, while traditional energy stakeholders are struggling to adapt to and capitalize upon the novel dynamics of zero-carbon technologies. Success requires modernizing not just our

technology, but also foundational parts of our infrastructure governance and security frameworks.

This white paper recommends three lines of effort in pursuit of these goals. First, the U.S. government should prioritize clean energy security and competitiveness in its competition with China, including a focus on immediate cybersecurity needs while building toward greater supply chain diversity in systemically critical technologies.

The U.S. government should prioritize clean energy security and competitiveness in its competition with China, including a focus on immediate cybersecurity needs while building toward greater supply chain diversity in systemically critical technologies.

Second, we must drive better integration across the security and clean energy communities, such as by modernizing industry coordination bodies to better incorporate clean energy stakeholders, updating critical infrastructure protection frameworks to reflect zero-carbon grid dynamics, and ensuring that the recently announced National Energy Council (a potential successor to the outgoing administration's National Climate Task Force) includes cybersecurity agencies. Finally, government and industry alike require a more nuanced risk assessment methodology for clean energy technologies, including coordinated cybersecurity practices tailored to clean energy systems and an R&D strategy prioritizing opportunities for "leap-ahead" technology advantage.

The United States can use the clean energy transition's historic investments in our infrastructure as a moment to build a more defensible and abundant energy future. Success requires unprecedented collaboration between the clean energy and national security communities, matched with reformed governance and risk frameworks capable of ensuring security at the pace and scale of the transition. The transformation of our energy infrastructure is already underway; the next task is to ensure that decarbonization brings fortification alongside it.

The transformation of our energy infrastructure is already underway; the next task is to ensure that decarbonization brings fortification alongside it.

DISTINCT THREATS WITH THE PROMISE OF SHARED SOLUTIONS

Climate change and great power conflict—especially with the People's Republic of China (PRC)—are two of the only existential threats to Americans' way of life.

Both threats have been consistently identified by national security leaders as fundamental challenges to U.S. interests, with the PRC representing the nation's primary strategic competitor and climate change bringing unprecedented risks to global stability. These dangers hold such a position of preeminent strategic attention because they are uniquely capable of fundamentally altering the political, economic, and ecological foundations upon which American security and prosperity depend.

Beijing views its early advantage in clean energy as a strategic asset that can help insulate it against the kind of economic isolation that Russia faced following its 2022 invasion of Ukraine.

[Hangzhou, China, Sept. 4. 2016 - Chinese president Xi Jinping (R) welcomes Russian President Vladimir Putin (L) to the G20 summit in Hangzhou; Shutterstock Standard Image License]

The U.S. government has warned consistently that the PRC is the only country with both the capability and intent to upend the international order. Chinese President Xi Jinping reportedly has directed the People's Liberation Army (PLA)—China's military—to be prepared to do just that in a conflict over Taiwan by the year 2027.[i] In anticipation of such a conflict, Beijing has been investing in cyber capabilities and operations intended to disrupt services designated by the United States to be its "critical infrastructure." This includes services we consider foundational to the basic functioning of modern society, from running water, to electricity, to our telecommunications system. Unfortunately, much of this infrastructure is built on a hodgepodge of technologies that are difficult to secure. Decades-old plumbing and power line

controls that never were intended to be connected to the internet are increasingly being managed with remotely-accessible software, creating inconsistent "seams" in digitization that are too easy for cyber actors to exploit.

Exploiting these "seams" in critical infrastructure during a crisis would have both military and civilian costs. Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA), told the House Select Committee on China[ii] earlier this year that PRC cyber actors are seeking to preposition disruptive cyber effects on U.S. infrastructure to stymie Washington's ability to project power abroad while sowing societal chaos at home.[iii] FBI Director Christopher Wray similarly has warned that these malicious cyber campaigns are "broad and unrelenting," and that Beijing's "plan is to land low blows against civilian infrastructure to try and induce panic and break America's will to resist."[iv] Recent research into cyberattacks against hospitals by criminal ransomware gangs suggests that even simple disruptions to computer services can meaningfully raise patient mortality rates; if paired with disruptions to water or power, it is easy to imagine how human consequences could worsen quickly within and beyond the healthcare system.[v]

Microsoft in 2023 publicly exposed one PRC state-backed hacking group responsible for a variety of critical infrastructure intrusions, issuing them the taxonomic moniker "Volt Typhoon."[vi] Volt Typhoon was notable for its stealth, using a variety of means to secure a user's valid credentials and then wielding those credentials so that their nefarious activities blended into legitimate network traffic (cyber tradecraft known as "living-off-the-land techniques"). Volt Typhoon apparently has been active on U.S. systems since 2021 and motivated some of the federal government's most urgent recent warnings about the vulnerability of Americans' infrastructure.[vii]

Yet Americans' infrastructure is also suffering from damage not nearly as subtle as a cyberattack. Early research indicates that climate change made Hurricane Helene much more powerful and enduring than the recorded norm.[viii] Unusually hot waters in the Gulf of Mexico imbued Helene with the additional energy necessary for it to reach far further inland with greater severity than typical storms, bringing historic flooding to Appalachia that resulted in hundreds of deaths.[ix] Researchers in the Journal of the American Medical Association have found that extreme heat is also driving deaths directly, including a sharp increase of more than 16 percent per year since 2016.[x] Climate change-driven effects like these will hit more tropical regions of the world even harder, threatening untold human costs and the destabilization of global supply chains, agriculture, and economic flows upon which Americans depend.

The clean energy transition has intertwined these two seemingly disparate sources of risk. Accelerated by 2021's Bipartisan Infrastructure Law, 2022's Inflation Reduction Act, and growing data center demand, this overhaul of our critical infrastructure is creating a dual opportunity to protect Americans against both hackers and hurricanes. The shift to more sophisticated, distributed energy technologies like smart inverters, battery storage, and virtual power plants offers a once-in-a-generation opportunity to modernize our grid. If done well, this transformation could eliminate outdated and vulnerable infrastructure—our "technical debt"—that is ill-equipped for today's digital landscape in favor of a modern architecture more defensible against cyber threats. If done poorly, however, this transformation could magnify underlying vulnerability, bringing new sources of risk and exploitation to our infrastructure while fixing none of the cracks in its shaky, century-old foundation.

The clean energy transition's overhaul of our critical infrastructure is creating a dual opportunity to protect Americans against both hackers and hurricanes.

PREPARING THE BATTLEFIELD FOR ZERO-CARBON REINFORCEMENTS

The overwhelming majority of the United States' critical infrastructure was not designed for the shape and requirements of our digital economy.

Many of the technologies that define our various infrastructure sectors were never intended to be as digitally interconnected as they are now, and no single government agency has the authority to enforce modern security standards across all these interconnected systems. The resulting "seams" in our infrastructure's digital defenses are imperiling many sectors but are especially present in the electricity sector and its fragmented regulatory environment.

While the electricity sector has been navigating the implications of digitization for decades, the clean energy transition is revealing an increasingly bifurcated ecosystem of carbon-free technologies that are generally digitally *native*, and legacy fossil technologies that are generally digitally *adapted*. The latter digitally-adapted infrastructure long has been recognized as a growing source of national security risk, with too many instances of digital connectivity being imperfectly integrated with technologies that are not designed for or securable against such connectivity. Clean energy technologies, which in contrast are more sophisticated and digitally native, can modernize that infrastructure if they are integrated well. But if more complex and software-defined clean tech is integrated into our infrastructure without consideration of its present and future vulnerabilities, the clean energy transition instead could *add* to national security risk by layering over our grid's flaws, offering more opportunities for malicious actors to exploit them.

To capitalize on clean energy's potential to transform our electricity system's defensibility and resilience against growing PRC cyber threats, our aging power infrastructure will need to update its aging institutions.

To capitalize on clean energy's potential to transform our electricity system's defensibility and resilience against growing PRC cyber threats, our aging power infrastructure will need to update its aging institutions—from its fundamental architecture, to its technology ecosystem, to the convening structures through which industry and government collaborate.

Architecture

The United States' electricity grid is divided into three functions: 1) *generation*, or the power plants that produce electricity for end use; 2) *transmission*, which moves electricity (typically at very high voltages) from geographically distant generation closer to where it will be consumed; and 3) *distribution*, which converts electricity from the transmission system into more locally-useful forms and carries it into residential, commercial, and industrial destinations. For decades this architecture has been organized around a few large nodes of generation, a primary transmission backbone (like the large transmission towers sometimes seen alongside interstate highways), and a simple distribution system (like local substations and neighborhood power line poles), all largely pushing electricity in one direction (from generation to end use). In this architecture, power plants have kept energy supply and demand

in a perpetual state of near-perfect balance by adjusting upward or downward how much fossil fuel they were burning at any given moment.

The clean energy transition is scrambling this architecture. Instead of a few central nodes of generation—such as the large coal-fired power plants that provided much of the country's electricity across the twentieth century—the grid is moving rapidly toward more numerous and distributed generation sources, like photovoltaic solar panels or collections of wind turbines. While fossil-based generation adjusts the supply of electricity up or down based on demand, many clean energy technologies generate electricity on the intermittent "supply" schedule of the sun or wind. This new pattern requires a more flexible grid capable of moving renewable energy from areas of surplus to areas of scarcity or storing it during times of surplus for use during times of scarcity. Already, some sunnier states like Texas or California are struggling with midday solar energy so abundant that prices can drop below zero, and they are working to either build transmission capable of moving excess energy to other *regions* (such as via new transmission lines) or build new forms of storage to move that excess energy to other *times* (such as via utility-scale batteries).[xi] Excessively abundant zero-carbon energy is an excellent problem to have, but one that will need to be solved with a more modern grid capable of moving electricity in more directions and in greater quantities than our legacy energy architecture can.

Yet building a more flexible, modern grid architecture is about more than handling new clean energy sources better—it also can present more opportunities for resilience against disasters and defensibility against attack. For example, **a more sophisticated grid armed with distributed energy sources, precisely controlled battery storage, and multidirectional electricity flows could more easily recover from storm damage, surge power to unexpected needs, or temporarily divide an unstable electricity system into quarantined "microgrids." All these capabilities would not just help people who are struggling with natural disasters like floods or hurricanes, but also prevent targeted cyberattacks from snowballing into countrywide consequences.**[xii]

This is not yet the grid architecture we have today. The clean energy transition is making progress in driving modernization, but the rigid "generation, transmission, storage" paradigm is straining against our energy demand, and offers a vulnerable target to national security threats. Holding this paradigm back from the pace of change it needs are the aging and difficult-to-secure technologies that underpin it, and the fragmented regulatory frameworks that govern it.

Technology

Even for a grid that was never designed for digitization, the economic case for adding network connectivity and remote access after the fact has been irresistible for years. Long before the recent shift toward decarbonization, infrastructure operators eagerly adopted remote management tools that allowed them to monitor and even control far-flung facilities that were difficult, time consuming, or dangerous to access. Being able to monitor and control operational technologies without having to dispatch a specialized technician to spend time or incur risk in doing so had a clearly beneficial business case—a business case that only improved as the resulting data allowed infrastructure operators to more precisely understand and model their systems and identify opportunities for efficiency gains as well. In many cases, this pursuit of remote management represented a novel combination of *information technologies* (IT), like the relatively new computers, servers, and internet connectivity we think of as comprising our digital ecosystem, and *operational technologies* (OT), the older category of sensors, switches, and pumps that make up much of our infrastructure's industrial control systems. But this post-hoc digitization brought with it unintended consequences.

Cybersecurity for *IT* is a mature field of technical and policy discourse, while cybersecurity for *OT* is much younger. The best and most appropriate frameworks for encryption are a perennial debate among IT architects, but the integration of operational technologies with networked connectivity is so recent a paradigm that OT communications traditionally have not been encrypted at all.[xiii] The growing adoption of internet-of-things (IoT) devices in industrial applications, and GPS communications for grid synchronization operations, only magnifies these concerns.[xiv] These concerns transitioned from theoretical to actual when, in 2015, Russia-backed cyber actors used a combination of stolen remote access credentials, malware, and denial of service attacks to disrupt Ukraine's electrical grid and leave hundreds of thousands without power.[xv]

While clean energy's greater reliance on software raises its cybersecurity stakes, it also opens new paths to make our power grid more secure and capable. Unlike fossil fuel systems that were retrofitted with digital controls as an afterthought, clean energy technologies are built from the ground up with software at their core. This "digitally-native" design means they can incorporate modern security features and—crucially—can be updated when knowledge of new threats emerges. This is a notable contrast to our aging power infrastructure, where many critical components cannot be patched against new cyber threats and must remain in service for decades despite known vulnerabilities. By embracing and responsibly implementing clean

energy's technical flexibility, we can build a power grid that not only emits lower carbon but is fundamentally more defensible than what we have today.

Three key clean energy technologies show how this digital innovation can either strengthen or weaken our power grid, depending on how we deploy them:

Smart Inverter Controls & Power Conversion Equipment

Smart inverters are critical safety checkpoints for our power grid, leveraging sophisticated computing and connectivity to manage the different types of electricity the grid requires.

Regional electrical grids run on alternating current (AC) of particular frequencies, and any electricity flowing onto those grids must match their respective frequencies or risk destabilizing them. Many traditional power plants meet these requirements by burning fossil energy to rotate turbines at a mechanically determined frequency in sync with the grid to which they are connecting.

Many clean energy technologies, including solar, wind, or power being disbursed from battery storage are natively generating electricity in *direct* current (DC) and need tools like inverters to convert their DC power into AC power at its connecting grid's appropriate frequency. Modern smart inverters can be even more sophisticated than that, not only converting DC to AC but also leveraging digital connectivity and networked communications to help support broader grid stability. This can include helping to maintain grid frequency against or in the aftermath of disruptive events, serving as "firebreaks" that automatically shut down their grid connection if they detect anomalous power behavior, or even managing failover maneuvers into microgrids or grid "islands." Smart inverters can help transition our grid architecture into one of self-healing electrical networks and assets that can individually fail without causing

Utility-scale battery facilities, like this complex in Riverside County, California, can leverage digital communication and sophisticated computing to support grid reliability and provide sources of resilience against power disruption or attack.

[Aerial view of Desert Sunlight Solar Farm battery storage units; Shutterstock Standard Image License]

cascading outages. These capabilities show potential for the clean energy transition to transform IT/OT convergence from a vulnerability into an asset. If designed and integrated with secure software and hardware development practices, smart inverters and distributed energy generation could replace our haphazard approach to digitization with a more secure and resilient infrastructure.

Batteries

Recent breakthroughs in manufacturing efficiencies—and failures to expand land use policies—mean batteries are playing a more central role in the clean energy transition than analysts expected just a few years ago. Prices for lithium-ion and related battery technologies fell 90 percent between 2008 and 2023[xvi] and are expected to fall another 50 percent by 2026,[xvii] helped along by economies of scale from consumer electronics and electric vehicle supply chains, and technological innovation reducing the need for critical minerals. Simultaneously, permitting, siting, and related land use obstacles are

delaying broader power plant and transmission investments, in some cases stranding abundant clean energy in time or geographies in excess of demand. Batteries are easier to site and can absorb and time-shift some of this local surplus of clean energy, but like smart inverters, utility-scale battery facilities are also able to leverage digital communication and sophisticated computing to support grid reliability and provide sources of resilience against power disruption.

If properly designed with secure software, the proliferation of grid-connected batteries will continue to transform clean energy economics and strengthen our critical infrastructure.

If properly designed with secure software, the proliferation of grid-connected batteries will continue to transform clean energy economics and strengthen our critical infrastructure. Already, huge deployments of Californian and Texan battery facilities are making intermittent solar look and act more like a traditional power plant. By storing low-cost (or even free) electricity from the midday sun and releasing it back onto the grid in time for the typical early-evening surge in consumer power use, these batteries are turning variable resources like sunlight into a resource that functions like a traditional power plant burning more or less fuel depending on demand.[xviii] Residential batteries are also benefiting from these dynamics, giving individual households similar advantages in resilience and demand-shifting at rapidly declining prices. An end user can charge their residential battery with rooftop solar panels during the day, and then tap into that stored power to run their evening appliance use and reduce the electricity they need to pull from the larger grid while its prices spike during nighttime periods of higher demand and lower supply.

Virtual Power Plants

Virtual power plants (VPPs) are software tools that combine and coordinate numerous (even thousands) of separate energy resources to create a single "virtual" resource that can be managed and dispatched as though it were a traditional power plant. VPP software is a novel capability made possible by sophisticated, digitally-native energy technologies, including those proliferating as a result of the clean energy transition.

For example, a utility may find that its traditional energy generation capacity is likely to be briefly insufficient to meet demand one afternoon as the sun is setting and its customers are returning home and starting to run their air conditioners, stoves, dishwashers, and clothes dryers in rapid succession. In a world of distributed, digitally connected energy resources and systems, the utility might simultaneously begin tapping utility-scale battery facilities and compensate a few thousand customers for access to 1 percent of the energy stored in each of their EVs or for turning their smart thermostats up one degree. The utility would be able to treat these thousands of small demand and supply adjustments as though it were a single, coherent entity—a virtual power plant capable of dispatching that aggregated energy wherever and however it is needed to manage grid requirements.

As purely software-defined creations with systemic impact on regional infrastructure, virtual power plants represent some of the most innovative new capabilities of our digitally enabled clean energy transition. They also present an aggregation of all our infrastructure's digitally enabled risk; a malign actor with the ability to reach into thousands of connected sources of electricity, aggregate them, and direct them at their whim would be a dangerous possibility indeed.

As the clean energy transition integrates these technologies into our infrastructure in greater numbers and positions of influence, the United States has the potential to enjoy a more secure, resilient, and flexible electricity ecosystem than a fossil-fuel based, haphazardly digitized grid ever could have provided. That potential can only be realized, however, if these disproportionately digitally-native clean energy technologies are built and integrated as secure and resilient by design. Without that confidence, the energy transition's promise of greater ambition and systemic resilience could be perverted into greater systemic risk via an even larger threat surface than our infrastructure has now. Unfortunately, the convening and governance structures through which industry and government collaborate are struggling to provide that confidence.

Governance

Across the public and private sectors, formal and informal governance frameworks are struggling to keep pace with the speed of both digitization and decarbonization—much less to be able to capitalize on the opportunities of their combination.

The Government Accountability Office has sounded the alarm for years that our electrical grid's growing vulnerability to cyber threats is exacerbated by its regulatory complexity.[xix] The grid's distribution system—the layer likely to see the largest proliferation of digital connectivity—is generally regulated by the states and exempt from many federal cybersecurity requirements. While the Federal Electricity Regulatory Commission (FERC), via the North American Electric Reliability Corporation (NERC), helps set mandatory critical infrastructure protection standards, their jurisdiction is remarkably limited against the scope and scale of cybersecurity and technology risk. A 2022 Atlantic Council report warned that, because of the distribution system's various exemptions from FERC's jurisdiction, only ten to twenty percent of the entire U.S. electricity sector was, in practice, subject to their requirements. In 2023, the United States produced a National Cybersecurity Strategy that committed the federal government to pursue binding, minimum cybersecurity requirements in all critical infrastructure sectors, but that federal effort is meeting uneven progress.[xx] [xxi]

Non-federal governance frameworks face similar challenges. Traditional infrastructure cybersecurity is built on a lattice of sectoral convening bodies, public-private intelligence analysis organizations, and frameworks of technical standards and design principles—most of which are straining to move at the speed and scale of the clean energy transition. Clean energy technologies often work in fundamentally different ways than their fossil-based forebears and require novel, first-order integration, security, and resilience considerations that these structures were not built to support. The clean energy transition is deploying at a speed matching its significant cost advantages and potential to avert the worst effects of climate change, but also at a speed these institutions never anticipated serving. And finally, the clean energy transition's greatest asset—the dynamism and diversity of its private sector ecosystem—is also one of its greatest liabilities. Unlike large traditional power companies with decades of security experience, many clean energy companies are newer, smaller startups that may not fully understand the security threats they face or how their technologies could be vulnerable to attack.

Two illustrative and critical areas of our infrastructure protection institutions are struggling to keep up with the promise of clean energy technologies:

Technical Standards and Design Principles for Security

Traditional infrastructure cybersecurity generally has relied upon consensus-based technical standards—such as those facilitated by the National Institute of Standards and Technology (NIST)—to promote the consistent application of best practices. These standards, when paired with overarching design principles (like secure-by-design and secure-by-default software planning development guidelines),[xxii] seek to provide both philosophical and technical roadmaps that engineers, planners, and executives alike can apply to their products and services. Ensuring the security and resilience of clean energy technologies' novel fusion of IT and OT will require, depending on the specific case, either entirely new standards, new implementation guidance of existing standards, or a combination of both.

Ensuring the security and resilience of clean energy technologies' novel fusion of IT and OT will require either entirely new standards, new implementation guidance of existing standards, or a combination of both.

The U.S. government, via NIST, CISA, multiple national labs, and the Departments of Energy and Transportation, have made significant progress in this arena and are committed to delivering more.[xxiii] Successfully developing these standards also requires deep engagement from industry, however, as companies building and deploying clean energy technologies best understand their technical complexities and operational realities. Because of this (necessary and proper) public-private collaboration, standards development is a deliberative, consensus-based, multi-stakeholder process that is frequently time-consuming and dependent on a small community of specialized experts, often making it difficult to scale or accelerate.

Vehicle electrification has been a pioneering effort in navigating these challenges, with innovative bodies like the Joint Office of Energy and Transportation ("the Joint Office") bringing together technical experts and programmatic funding experts from the Departments of Energy and Transportation into a nimble, high-performing integration cell that collaborates with automakers and parts suppliers. The Joint Office is helping

industry and the U.S. government rapidly identify gaps in standards requirements and commission the research and convenings necessary to fill them—all while simultaneously pursuing a deployment schedule aggressive enough to meet growing consumer demand and international climate goals.[xxiv] Cultivating a *culture* of security, resilience, and upgradeability—across both the public and private sectors—has proven to be a key step in maintaining this agility while standards development learns and "catches up," but this will be a harder lesson to port to other diffuse and globally-interdependent sectors of the clean energy transition.

Industry Coordinating Bodies and Public-Private Information Sharing

Most of the United States' critical infrastructure is privately owned or operated, and the primary architects of our digital ecosystem and its cybersecurity are similarly situated in the private sector. The leading role of public-private partnerships in these fields has been conventional wisdom for decades, and it has driven the development of a mature ecosystem of sectoral coordinating bodies and information sharing organizations. These bodies, like the Electricity Subsector Coordinating Council and various Information Sharing & Analysis Organizations (ISAOs),[xxv] help facilitate data flows, distribute threat intelligence, coordinate crisis response and preparedness, and develop strategic and policy agendas.

These kinds of coordinating councils and ISAOs have become very effective at serving their traditional memberships and technological contexts. They have had decades of experience working with their regulators, analyzing and anticipating threat actors and other forms of systemic risk, and securing a relatively slow-moving technology ecosystem. The clean energy transition represents, in many ways, an exogenous shock to these structures; a consolidated and mature membership community is being asked to suddenly and swiftly incorporate new technologies and stakeholders who, in many cases, have far less of the policy, risk, and security intuition that the incumbents spent years developing.

Yet that kind of shock may be precisely what is required. **Incumbent electricity stakeholders are charged with defending an aging technical ecosystem with haphazard digitization against mounting threats from cyber actors backed by Beijing and others. The dynamism and technical sophistication offered by new, clean energy market entrants can be an asset in overcoming that challenge, but those new entrants also need the traditional incumbents' partnership in navigating national security considerations they may never have been prompted to consider previously.** While longstanding energy stakeholders regularly handle intelligence that illustrates the bracing nature of PRC capabilities and intent, many newer clean energy market entrants (whose supply chains disproportionately run through China) have been slow to internalize these realities.

Rapidly declining prices for clean energy technologies mean that zero-carbon generation, like this solar farm in Nevada, now account for the overwhelming majority of new electricity being added to the U.S. grid.

[February 28th, 2024: Solar panel farms outside of Las Vegas, Nevada.; Shutterstock Standard Image License]

Traditional energy incumbents, however, also need to make room for those new entrants as co-stakeholders. Sector coordinating councils and analysis organizations have been slow to admit clean energy representatives or adapt their processes to accommodate their more diffuse market structure, even as zero-carbon generation has surged to the point that it now accounts for the overwhelming majority of new electricity added to the grid.[xxvi] New clean energy market entrants hold tremendous promise to help the electricity sector become a far more secure, resilient, and ambitious ecosystem—but only if armed with the intelligence, collaboration structures, and authorities necessary to be full partners in doing so.

New clean energy market entrants hold tremendous promise to help the electricity sector become a far more secure, resilient, and ambitious ecosystem—but only if armed with the intelligence, collaboration structures, and authorities necessary to be full partners in doing so.

POLICY RECOMMENDATIONS: BUILDING STRATEGIC UNITY AGAINST BOTH CLIMATE CHANGE AND GREAT POWER CONFLICT

The United States cannot afford to confront two of its only existential threats in isolation, especially when their technological implications are so deeply intertwined. The following recommendations are intended to promote that unity of effort from strategic direction, to tactical prioritization, to technical implementation. They are anchored in building resilience against the risk of PRC cyberattacks on our critical infrastructure but can and must inform the United States' broader technological competition with China—which is increasingly likely to have clean energy industrial leadership at its core.

Line of Effort 1: Make Clean Energy Security a Core Area of Competition with China

The United States should resist the temptation to reactively mirror the moves of its competitors—but it also shouldn't be afraid to react when its competitors are right. Beijing clearly views its early advantage in clean energy manufacturing and deployment as a strategic asset.[xxvii]

Global investment flows into clean energy are approaching $2 trillion a year, and the technologies leading those investments (like solar photovoltaics and lithium-ion batteries) remain largely dependent on Chinese supply chains.[xxviii] The PRC is enmeshing itself into one of the largest global capital investment opportunities in history, generating favorable investment returns while insulating itself against the kind of economic isolation that Russia has faced following its 2022 invasion of Ukraine. It is no surprise that Xi Jinping repeatedly has emphasized the crucial role of Chinese leadership in clean energy, telling a recent study session of the Chinese Communist Party's Central Committee to prioritize "new energy" while exhorting them to "[coordinate] the development of new energy with national energy security" considerations.[xxix]

The PRC is enmeshing itself into one of the largest global capital investment opportunities in history, generating favorable investment returns while insulating itself against the kind of economic isolation that Russia has faced following its 2022 invasion of Ukraine.

The United States should signal a similar political, financial, and, critically, national security commitment to clean energy technologies. **In the immediate term, the United States should prioritize cybersecurity and vendor trust so that these technologies can play the role we need them to in strengthening the defensibility of our grid—even while they are disproportionately sourced from some of the very countries against which we need to defend that grid. In the longer term, the United States will need to focus on supply chain diversity more directly.**

This **supply chain diversification should be a source of expeditious concern for U.S. policymakers—but not an irrational panic**. Global interdependencies in the markets for oil and semiconductors are instructive contrasts. Gasoline refineries need uninterrupted flows of crude oil inputs to keep producing energy, whereas solar panels require almost no additional inputs for long-term operation; unlike in the case of oil, if the United States were one day suddenly cut off from every photovoltaic producer in the world, an energy crisis would not ensue immediately. And while clean energy technologies are generally much more sophisticated than their fossil fuel counterparts, their manufacturing requirements are still simpler than the vast expense and complexity that drive concentration in the semiconductor market. Even so, lessons from the painful and expensive semiconductor reshoring process will be valuable; an ounce of prevention is worth a pound of cure, and policymakers should seek to quickly erode the PRC's early lead in clean energy manufacturing before a CHIPS & Science Act-style "major surgery" is required.

An ounce of prevention is worth a pound of cure, and policymakers should seek to quickly erode the PRC's early lead in clean energy manufacturing before a CHIPS & Science Act-style "major surgery" is required.

But while contesting leadership in clean energy manufacturing will be important for maintaining both cybersecurity and manufacturing competitiveness during the world's clean energy transition, its most potent impact could be in capturing the *upside* potential of clean energy technologies. Some clean energy technologies—especially solar, the cheapest and fastest-deploying—are capable of near-zero-marginal-cost electricity generation. In contrast to fossil fuel-based power plants, a solar farm need be constructed only once to generate electricity for decades without the need for additional "fuel" and with strikingly low maintenance costs.[xxx] Similarly rapid declines in prices for utility-scale batteries are allowing sunny states to capture solar-generated electricity when it is so abundant that prices reach or fall below zero as solar supply exceeds the grid's ability to absorb it, transforming wasted midday surplus into usable evening stores.[xxxi] Decoupling energy

Decoupling energy generation from environmental damage, unstable international oil dependencies, or (in the case of solar) even near-term scarcity itself could drive a level of resource abundance capable of catalyzing breakthroughs in innovation, research, and international competitiveness that we do not yet know how to fully quantify.

generation from environmental damage, unstable international oil dependencies, or (in the case of solar) even near-term scarcity itself could drive a level of resource abundance capable of catalyzing breakthroughs in AI development, scientific research, and international competitiveness that we do not yet know how to fully quantify.[xxxii]

This upside potential is speculative—but when that upside potential is so high, so should be our tolerance for uncertainty. The national mobilization around artificial intelligence development, for example, is motivated by the (at least somewhat well-founded) hunch that AI capabilities will have significant national security implications, and that understanding and realizing those implications holds such potential that the United States should race to maintain its first-mover advantage. While the pace of clean energy innovation may be slightly slower, recent breakthroughs in solar efficiency, batteries, nuclear fission reactors, nuclear fusion research, enhanced geothermal wells, and materials science suggest it may not be far behind and could indeed be crucial to our AI ambitions. **The possibility of electricity generation so clean, cheap, and abundant as to test the bounds of energy scarcity is increasingly linked to the concept of artificial superintelligence, and arguably possesses a scientifically clearer pathway to near-term deployment. The U.S. government should invest a similar urgency in understanding the potential of this abundance agenda as it is investing in artificial intelligence, and in assessing whether it should be racing to realize it before Beijing.**

- **Recommendation:** The U.S. government should adopt a clean energy security and competitiveness strategy.
    - This strategy should focus in the near term on the cybersecurity, availability, and vendor trustworthiness of key clean energy technologies, especially those with high dependence on PRC supply chains.
    - In the medium term, it should adapt lessons learned from U.S. and allied semiconductor supply chain diversification efforts, including maintaining both leading-edge innovative engines and trailing-edge production capacities.
    - This strategy should prioritize maintaining U.S. and allied leadership in international clean energy financing. This should ensure that cyber-secure and trusted technology is accessible to emerging markets, that those markets' demand can contribute to U.S. and allied manufacturing capacity, and in so doing, balance PRC influence over the future of those markets' energy security.[xxxiii]

- **Recommendation**: The Council of Economic Advisors and the President's Council of Advisors on Science and Technology (or appropriate analogues) should issue a joint report on the potential for clean energy abundance and its national security implications.
    - This report should study how to maximize the potential of zero-marginal-cost clean energy deployment, identify any policy and scientific barriers to near-term energy abundance, and outline the economic and national security implications that policymakers should consider to achieve, and as a result of achieving, that abundance.

Line of Effort 2: Build and Strengthen a "China Risk/Climate Risk" Community of Practice Across the Public and Private Sectors

The clean energy transition is deeply intertwined with U.S.-China competition, but the leading stakeholders behind each are not.

Climate leaders often hail from energy and advocacy backgrounds, organize around ambitiously affirmative policy agendas, and are focused on mitigating climate risk. China hands often emerge from "hard national security" backgrounds, organize around issues like deterrence and decoupling, and spend much of their intellectual capital on interdicting hostile PRC intent. There are obvious areas of overlap and cross-pollination between these communities, but rarely at the levels and depths necessary to promote the unity of purpose and strategic prominence it seems to enjoy in Beijing. A more coherently integrated "China risk/climate risk" community of practice is needed across both the public and private sectors.

The U.S. government should take steps to structurally promote that integration in its policymaking processes. Policy councils in the Executive Office of the President, for example, coordinate functional expertise from across the various departments and agencies—e.g., by convening representatives from every cyber policy office in government—but in so doing, sometimes can recreate silos *across* those functional areas of expertise. Critical infrastructure protection, for example, depends on both teams and policy frameworks that often focus on Chinese cyber threats, but have not been updated yet to incorporate clean energy-specific considerations, despite a) the fundamentally distinct way clean energy technologies interact

with digital connectivity in comparison to their fossil fuel-based predecessors, and b) the historically unprecedented adoption of these technologies in the United States and around the world. The reverse is also true, with many clean energy processes deploying technologies that will fundamentally alter the nature of cyber risk on our critical infrastructure, but with little integration of national security-focused professionals to mitigate this risk, much less turn it into the opportunities proposed by this white paper. Minor changes to policy processes to intentionally intermingle PRC and climate professionals would return significant benefits.

Industry and sectoral coordination bodies also require this intentional intermingling. Traditional energy companies and stakeholders have significant experience mitigating cyber threats generally and those from the PRC specifically, but that experience needs to be better integrated into the clean energy community and to inform the ongoing transformation of our energy infrastructure. Intelligence analysis and distribution mechanisms need to be updated to better serve the clean energy vendor community, who are generally smaller, more numerous, and more diffuse than their fossil energy counterparts. These bodies and sectoral coordinating mechanisms similarly need to better represent the communities they serve, ensuring that membership reflects the prominence of new clean energy participants in their respective marketplaces. Tesla, for example, is by a large margin the United States' largest electric carmaker, producer of one of the most popular individual car models in the world,[xxxiv] and arguably the most software-defined car on the market but it still has not joined the Automotive Information Sharing and Analysis Center (ISAC)—a handicap to both Tesla and the sector's ISAC.[xxxv]

Traditional energy companies and stakeholders have significant experience mitigating cyber threats generally and those from the PRC specifically, but that experience needs to be better integrated into the clean energy community and to inform the ongoing transformation of our energy infrastructure.

- **Recommendation:** The U.S. government should intentionally integrate relevant national security and clean energy policymaking processes and frameworks.
    - The newly announced National Energy Council, potentially a successor to the National Climate Task Force (a principals committee created in 2021 to adjudicate whole-of-government climate and energy policy from inside the Executive Office of the President), should add CISA and the National Security Agency to its membership.

- The next National Infrastructure Risk Management Plan, a White House-directed policy update coordinated by CISA and due later in 2025, should explicitly incorporate the novel considerations introduced by clean energy technologies.
- The Joint Office of Energy and Transportation should be expanded to improve the scope of impact of its uncommonly successful model for integrating both rapid technology deployment and nimble standards development.

- **Recommendation:** Industry coordination and intelligence sharing bodies should ensure their membership and processes are designed to incorporate and engage with the clean energy ecosystem and its structural novelties.
  - Information Sharing and Analysis Organizations and Centers (ISAOs/ISACs) should review a) their membership to ensure they reflect the clean energy influence in their marketplaces, and b) restructure their coordination mechanisms to better integrate with smaller, more numerous, and less risk-sophisticated clean energy stakeholders.
  - ISAOs/ISACs and sector coordinating councils should adapt security and resilience resources, including those on secure-by-design principles, technical standards implementation, and open-source software security, for clean energy stakeholders' unique considerations.

- **Recommendation:** Electricity sector stakeholders, from utilities to the tech industry, should drive coordinated cybersecurity practices that are tailored to and scalable among the broader clean energy marketplace.
  - The country's energy utilities should coordinate on shared guidance for "what right looks like" for the unique cybersecurity considerations of integrating clean energy technologies into their grids. This will make it easier for clean energy vendors to scale their contributions to security and resilience across different regional regulatory jurisdictions and integrate into different regional grids more efficiently, all while helping make up for the distribution-level regulatory gap in electricity infrastructure cybersecurity.
  - Cloud computing hyperscalers, whose next-generation AI training data centers are helping to propel historic increases in electricity demand, should use their purchasing power to inform and drive new clean energy cybersecurity practices. Hyperscalers paid utilities a "green premium" above market rates during their initial 2010s-era data center buildouts to ensure the first generation of cloud computing ran on clean energy, also helping to seed the clean energy

marketplace that we know today. As some of the few actors in the U.S. economy possessing deep expertise in both energy economics and PRC exploitation of flawed software, today's AI-driven hyperscalers should use their influence over the next generation of energy deployment to inform and drive the development of clean energy-specific security practices.

Line of Effort 3: Adopt a Near-Term Risk and Opportunity Prioritization Framework

The United States must strategically prioritize technical vulnerabilities in our rapidly evolving energy ecosystem. The challenge is immense, requiring the simultaneous protection of the energy sector, which represents 7 percent of the U.S. economy, with the transformational modernization of its technological and institutional foundations. [xxxvi] This effort presents three overlapping imperatives: securing existing infrastructure during an unprecedented modernization and transition to clean energy, seizing opportunities to build enhanced security into new systems, and countering China's demonstrated intent to target our infrastructure with cyberattacks. These complex demands require a clear framework to adjudicate priorities and trade-offs as we transform our energy ecosystem.

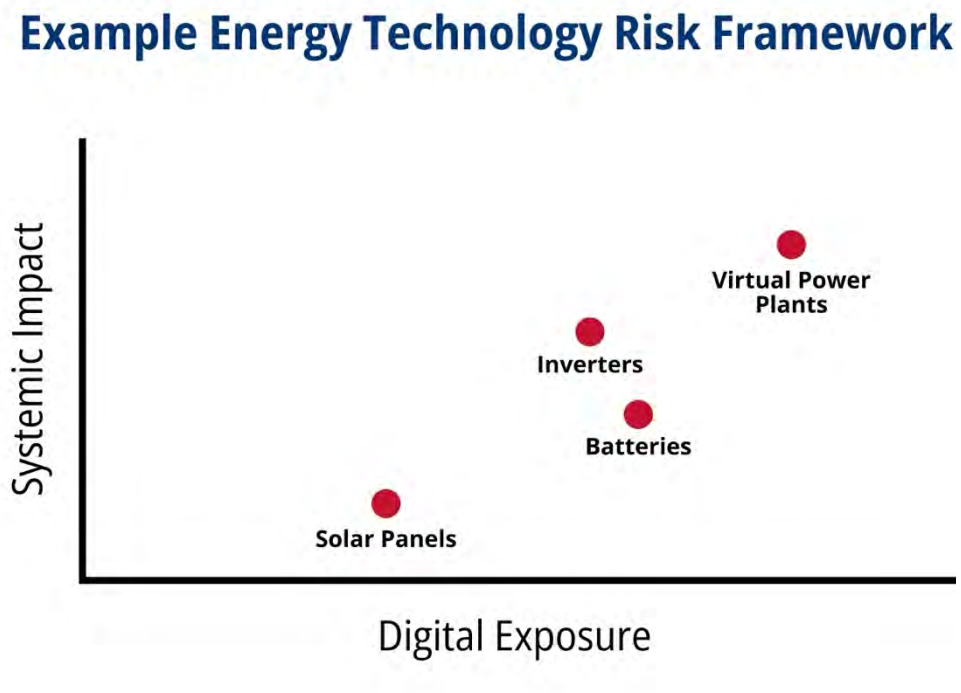
In 2024, the United States made a down payment on that framework for near-term cybersecurity considerations, highlighting a set of "linchpin technologies" it views as critical to the immediate success of the energy transition and that are disproportionately defined by digital connectivity.[xxxvii] The energy security community now requires a more nuanced framework to consider the relative risk and reward of these technologies against one another, where to surge its resources, and where synergistic investments might have benefits across technologies and sectors.

These frameworks should consider:

Relative Risk

Which modern energy technologies have the highest exposure of digital connectivity into their core functions? Which technologies have the most systemic influence over our electricity infrastructure?

For example, while photovoltaic solar panels may have embedded sensors or other efficiency-maximizing technologies, they are digitally relatively "dumb" compared to other parts of the clean energy ecosystem. Similarly, solar panels are unlikely by themselves to have systemic influence over the electrical grid, because solar panel electrical flows are typically aggregated into a more central inverter. In contrast, virtual power plants are *entirely* software-defined and can have significant systemic influence over the electrical grid. Smart inverters and batteries are likely somewhere in the middle—more mechanical than VPPs and less digitally defined, but more systemically influential than solar panels and still possessing significant IT/OT convergence.



Difficulty of Remediation

Which priority digitally-exposed and systemically-significant clean energy technologies have the "easiest" route to delivering greater security and resilience to our electrical grid? Which have scalable solutions applicable to multiple technologies, and which will require more bespoke investments in attention and expertise?

Virtual power plants, for example, are an appealing early priority. Being entirely digitally defined would suggest—despite their high potential for systemic impact on the

electrical grid—they may be the easiest to remediate. The application of secure-by-design software development principles, established methods for penetration testing and validation, and potential to leverage the open-source software community appear to be scalable approaches to VPP security that are portable to and from other software-dependent sectors. Even better, achieving that confidence in VPP software security and resilience—even going so far as to only whitelist VPPs from the United States and trusted partners—would not require uprooting a complex and decades-old manufacturing supply chain from around the world.

Batteries, in contrast, are likely to be more challenging. Per the above chart of an example risk framework, utility-scale battery deployments appear firmly in the "middle" of digital exposure and systemic impact, likely complicating a precise analysis of sources of risk and routes to mitigation. While software controlling how batteries interface with the electrical grid ostensibly can be vetted in a scalable manner, firmware operating closer to the battery cells themselves can be much more challenging to review—especially when considering that most of those cells are currently manufactured in China.[xxxviii] The Inflation Reduction Act made resources available in an attempt to diversify battery supply chains, but Beijing's advantage in the sector is immense; the most practical approach may be investing in ways to vet the cybersecurity of today's battery technologies while simultaneously betting on leap-ahead technologies—such as recent breakthroughs in solid state battery commercialization—that could allow the United States a potential leg up on future supply chain security.[xxxix]

- **Recommendation:** The Department of Energy, the Cybersecurity and Infrastructure Security Agency, and the National Security Agency should develop a joint risk and remediation assessment framework for clean energy technologies.
    - The assessment should evaluate the U.S. government's clean energy "linchpin technologies" according to digital exposure, systemic impact, and relevant threat intelligence. It should identify areas of scalable interventions—such as with broader adoption of certain secure software development practices—and areas where bespoke interventions may be required.
    - The assessment should consider near-term cybersecurity considerations as well as longer-term supply chain dependencies that may impede greater certainty in relevant technologies' security and resilience.

- **Recommendation:** The Office of Science & Technology Policy, the Department of Energy, and the Department of Commerce should establish an R&D strategy for clean energy technologies that not only are game-changing decarbonization tools, but also provide "leap-ahead" substitution opportunities for U.S. and allied manufacturers currently dependent on PRC supply chains.
    - Informed by the above risk and remediation assessment, this R&D strategy should identify and accelerate emerging technologies that could help break U.S. and allied dependence on vulnerable supply chains.
    - This strategy should adjudicate for which technologies the United States is willing to tolerate relative PRC dominance—perhaps including, for example, relatively "dumb" and commodity clean energy components—and those which are more systemically impactful and over which the United States should seek to retain influence, such as in battery storage.

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

[ii] Formally, "Select Committee on Strategic Competition Between the United States and the Chinese Communist Party"

[iii] "Testimony of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, on the CCP Cyber Threat to the American Homeland and National Security, to the Select Committee on Strategic Competition Between the United States and the Chinese Communist Party," Congress.gov, 31 January 2024, https://docs.house.gov/meetings/ZS/ZS00/20240131/116776/HHRG-118-ZS00-Wstate-EasterlyJ-20240131.pdf.

[iv] "Wray: Chinese government poses 'broad and unrelenting' threat to U.S. critical infrastructure." FBI, 18 April 2024, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says.

[v] Zac Amos, "The Link Between Health Care Cyberattacks and Patient Mortality," The Journal of mHealth, 8 January 2024, https://thejournalofmhealth.com/the-link-between-health-care-cyberattacks-and-patient-mortality/.

[vi] "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft Security Insider, 25 May 2023, https://www.microsoft.com/en-us/security/security-insider/emerging-threats/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques.

[vii] Julian E. Barnes, "China Could Threaten Critical Infrastructure in a Conflict, N.S.A. Chief Says," The New York Times, 17 April 2024, https://www.nytimes.com/2024/04/17/us/politics/china-cyber-us-infrastructure.html.

[viii] Haley Thiem and Rebecca Lindsay, "Hurricane Helene's extreme rainfall and catastrophic inland flooding," Climate.gov, 7 November 2024, https://www.climate.gov/news-features/event-tracker/hurricane-helenes-extreme-rainfall-and-catastrophic-inland-flooding.

[ix] Alejandra Borunda and Rachel Waldholz, "Climate change made Helene more dangerous. It also makes similar storms more likely," NPR, 9 October 2024, https://www.npr.org/2024/10/09/nx-s1-5144216/climate-change-hurricane-helene.

[x] Mary Cunningham, "Heat-related deaths accelerated in the last 7 years, Journal of American Medical Association study finds," CBS News, 26 August 2024, https://www.cbsnews.com/news/heat-related-deaths-american-medical-association/;
Jeffrey T. Howard, Nicole Androne, and Karl Alcover, et al, "Trends of Heat-Related Deaths in the US, 1999-2023," Journal of American Medical Association, 2024;332(14):1203–1204. doi:10.1001/jama.2024.16386.

[xi]Shannon Osaka, "Rooftop solar panels are flooding California's grid. That's a problem," The Washington Post, 22 April 2024, https://www.washingtonpost.com/climate-environment/2024/04/22/california-solar-duck-curve-rooftop/.

[xii] "Microgrids and Backup Power Systems," Idaho National Laboratory, June 2024, https://inl.gov/document/microgrids-and-backup-power-systems/;
Wilson Rickerson, Jonathan Gillis, and Marisa Bulkeley, "The Value of Resilience for Distributed Energy Resources: An Overview of Current Analytical Practices," National Renewable Energy Laboratory, June 2024, https://www.nrel.gov/docs/fy24osti/90139.pdf.

[xiii] "Securing the Energy Transition Against Cyber Threats: Report of the Atlantic Council Task Force on Cybersecurity and the Energy Transition," Atlantic Council Global Energy Center, July 2022, https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Securing-the-Energy-Transition-against-Cyber-Threats.pdf.

[xiv] "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," Government Accountability Office, August 2019, GAO-19-332, https://www.gao.gov/products/gao-19-332.

[xv] "Cyber-Attack Against Ukrainian Critical Infrastructure," Cybersecurity & Infrastructure Security Agency ICS Alert, 20 July 2021, IR-ALERT-H-16-056-01, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01;
Michael Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS Institute, 6 January 2016, https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

[xvi] "Electric Vehicle Battery Pack Costs for a Light-Duty Vehicle in 2023 Are 90% Lower than in 2008, according to DOE Estimates," Department of Energy Fact of the Week #1354, 5 August 2204, https://www.energy.gov/eere/vehicles/articles/fotw-1354-august-5-2024-electric-vehicle-battery-pack-costs-light-duty.

[xvii] "Electric vehicle battery prices are expected to fall almost 50% by 2026," Goldman Sachs Insights, 7 October 2024, https://www.goldmansachs.com/insights/articles/electric-vehicle-battery-prices-are-expected-to-fall-almost-50-percent-by-2025.

[xviii] "Batteries are a fast-growing secondary electricity source for the grid," U.S. Energy Information Administration In-Brief Analysis, 5 September 2024, https://www.eia.gov/todayinenergy/detail.php?id=63025;
Felicity Bradstock, "The U.S. Battery Boom Is Revolutionizing Renewable Energy," OilPrice.com, 15 May 2024, https://oilprice.com/Energy/Energy-General/The-US-Battery-Boom-Is-Revolutionizing-Renewable-Energy.html.

[xix] "Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems," Government Accountability Office, March 2021, GAO-21-81, https://www.gao.gov/assets/gao-21-81.pdf;
"Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," Government Accountability Office, August 2019, GAO-19-332, https://www.gao.gov/products/gao-19-332.

[xx] David E. Sanger, "New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms," The New York Times, 2 March 2023, https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

[xxi] Tim Starks, "Legal challenge to EPA rule poses obstacle to Biden's cyber agenda," The Washington Post Cybersecurity 202, 19 April 2023, https://www.washingtonpost.com/politics/2023/04/19/legal-challenge-epa-rule-poses-obstacle-biden-cyber-agenda/.

[xxii] Secure By Design, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securebydesign.

[xxiii] "Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future," The White House, 9 August 2024, https://www.whitehouse.gov/oncd/briefing-room/2024/08/09/fact-sheet-biden-harris-administration-announces-priorities-for-enhancing-the-digital-ecosystem-to-support-a-secure-energy-future/.

[xxiv] "Securing EV Charging Infrastructure Part 2: Game-Changing Research," Department of Energy, 17 April 2024, https://www.energy.gov/ceser/articles/securing-ev-charging-infrastructure-part-2-game-changing-research.

[xxv] The author is using ISAOs as an umbrella term to also include the related but older, more sector-specific category of Information Sharing & Analysis Centers (ISACs) and is not intending to conflate their unique histories or nuanced structures and charters.

[xxvi] Julian Spector and Maria Virginia Olano, "Chart: Nearly all new US power plants built in 2024 will be clean energy," Canary Media, 23 February 2024, https://www.canarymedia.com/articles/clean-energy/chart-nearly-all-new-us-power-plants-built-in-2024-will-be-clean-energy.

[xxvii] Statement of Nikos Tsafos, CSIS, on China's Climate Change Strategy and U.S.-China Competition, to the U.S.-China Economic and Security Review Commission," CSIS, 17 March 2024, https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts220316_Nikos_Tsafos.pdf?VersionId=HfxOoz6eF_Si7w._roa_FDVWKT.oQ0Gz.

[xxviii] Executive Summary of the World Energy Outlook 2024, International Energy Agency, October 2024, https://www.iea.org/reports/world-energy-outlook-2024/executive-summary.

[xxix] "Xi Jinping Emphasizes Vigorously Promoting High-Quality Development of New Energy in China to Make Greater Contributions to Building a Clean and Beautiful World during the 12th Collective Study Session of the CCP Central Politburo," CSIS Interpret: China policy document translation, published by Xinhua News Agency, 29 February 2024, https://interpret.csis.org/translations/xi-jinping-emphasizes-vigorously-promoting-high-quality-development-of-new-energy-in-china-to-make-greater-contributions-to-building-a-clean-and-beautiful-world-during-the-12th-collective-study-sessio/.

[xxx] David Wallace-Wells, "What Will We Do With Our Free Power?," New York Times Opinion, 28 August 2024, https://www.nytimes.com/2024/08/28/opinion/solar-power-free-energy.html.

[xxxi] Shannon Osaka, "Rooftop solar panels are flooding California's grid. That's a problem," The Washington Post, 22 April 2024, https://www.washingtonpost.com/climate-environment/2024/04/22/california-solar-duck-curve-rooftop/.
[xxxii] Costas Arkolakis and Conor Walsh, "The Economic Impacts of Clean Power," National Bureau of Economic Research, Working Paper 33028, October 2024, https://www.nber.org/system/files/working_papers/w33028/w33028.pdf.
[xxxiii] Brian Deese, "The Case for a Clean Energy Marshall Plan: How the Fight Against Climate Change Can Renew American Leadership," Foreign Affairs, 20 August 2024, https://www.foreignaffairs.com/united-states/case-clean-energy-marshall-plan-deese.
[xxxiv] Felipe Munoz, "Tesla Model Y secures position as world's best-selling car in 2023," JATO, 13 June 2024, https://www.jato.com/resources/media-and-press-releases/tesla-model-y-worlds-best-selling-car-2023#:~:text=Impressively%2C%20the%20Model%20Y%20secured,gained%20popularity%20in%20developing%20economies.
[xxxv] Automotive ISAC Membership Roster, 2024, https://static1.squarespace.com/static/618a9a805a5be466f28052a2/t/672529e6a8b54016db8c8f81/1730488806898/2024_11_01_Member_Roster_Website.pdf.
[xxxvi] "U.S. Energy System Factsheet," University of Michigan Center for Sustainable Systems, 2024, https://css.umich.edu/publications/factsheets/energy/us-energy-system-factsheet.
[xxxvii] "Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future," The White House, 9 August 2024, https://www.whitehouse.gov/oncd/briefing-room/2024/08/09/fact-sheet-biden-harris-administration-announces-priorities-for-enhancing-the-digital-ecosystem-to-support-a-secure-energy-future/; Fact Sheet: Office of the National Cyber Director Publishes an Energy Modernization Cybersecurity Implementation Plan to Secure an Ambitious Energy Future," The White House, 20 December 2024, https://www.whitehouse.gov/oncd/briefing-room/2024/12/20/fact-sheet-office-of-the-national-cyber-director-publishes-an-energy-modernization-cybersecurity-implementation-plan-to-secure-an-ambitious-energy-future/;
Note: The author co-chaired the development of these priorities while serving at the White House's Office of the National Cyber Director.
[xxxviii] Suvrat Kothari, "How China Became A Battery Manufacturing Juggernaut," Inside EVs, 12 March 2024, https://insideevs.com/news/711990/how-china-became-global-battery-manufacturing-leader/.
[xxxix] Varun Sivaram, "How the United States Can Win the Battery Race: To leapfrog China, Washington should shift away from lithium-ion batteries," Foreign Policy, 21 October 2024, https://foreignpolicy.com/2024/10/21/us-china-competition-battery-production-ev-minerals-solid-state/.