STRIDER

NOVEMBER 2025

IN BROAD DAYLIGHT

U.S. Grid Exposed to Risk from PRC-Made Inverter Equipment

STRIDERINTEL.COM

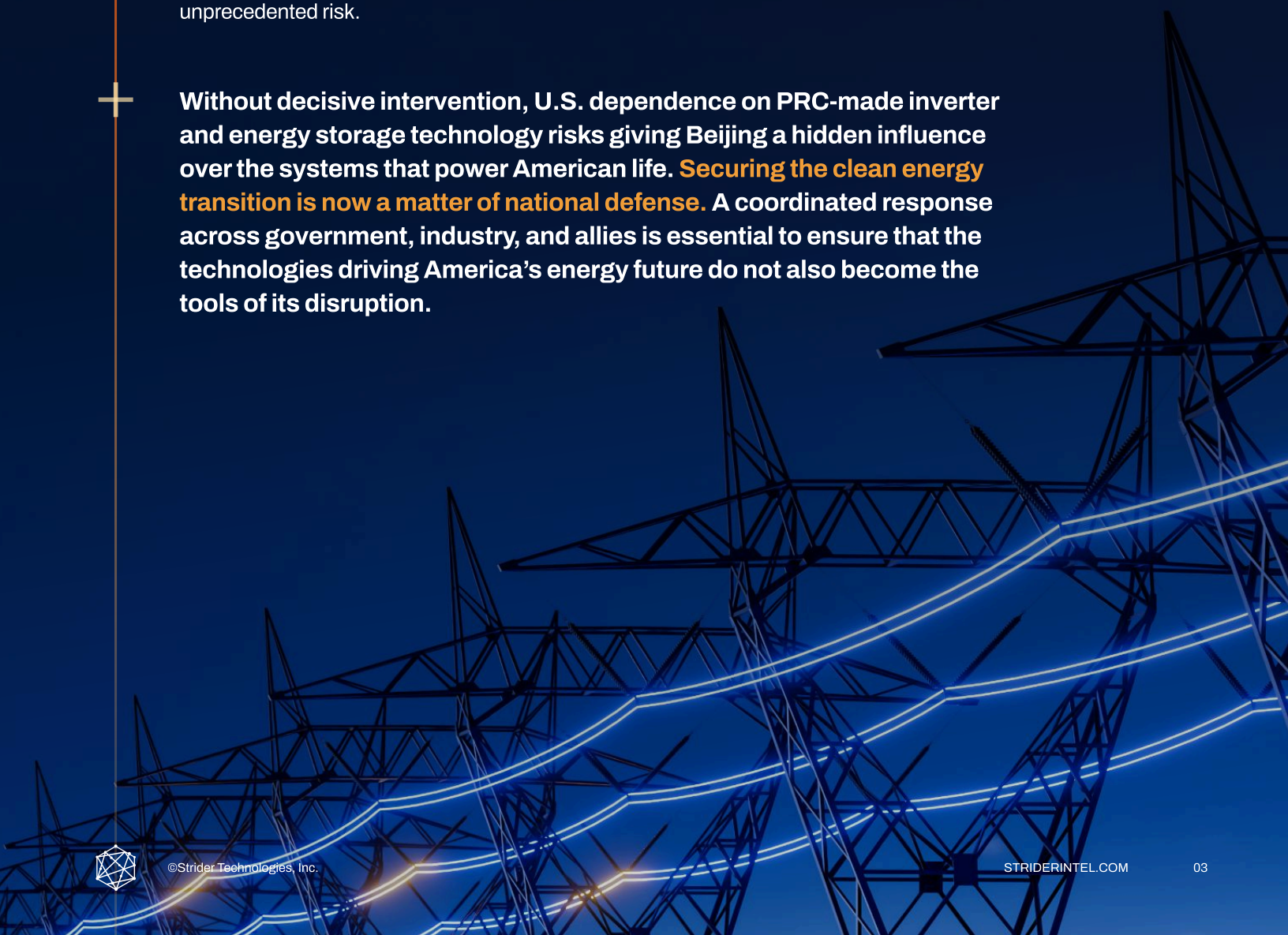
TABLE OF CONTENTS

EXECUTIVE SUMMARY

America's clean energy expansion has created a growing threat to the stability of the power grid. As the United States accelerates its transition to renewable energy, it has become heavily dependent on inverter-based resources (IBRs), including photovoltaic power (commonly referred to as solar power) and battery energy storage systems (BESS), manufactured by companies in the People's Republic of China (PRC). These systems are no longer simple hardware; they are networked, software-driven devices capable of remote communication and control. This connectivity, combined with their PRC origin, exposes U.S. critical infrastructure to unprecedented risk.

PRC manufacturers dominate the global market for renewable energy hardware, offering competitively priced and technologically advanced products that have become deeply enmeshed in U.S. power generation and grid operations. Since 2015, the PRC has exported billions of kilograms of inverters and related equipment into the United States, resulting in widespread deployment across utilities, solar farms, and energy storage networks. This widespread reliance creates a strategic vulnerability: the Chinese government, through its control over PRC firms and data networks, could exploit this access to manipulate or disrupt the U.S. grid in a crisis.

Without decisive intervention, U.S. dependence on PRC-made inverter and energy storage technology risks giving Beijing a hidden influence over the systems that power American life. Securing the clean energy transition is now a matter of national defense. A coordinated response across government, industry, and allies is essential to ensure that the technologies driving America's energy future do not also become the tools of its disruption.



EXECUTIVE SUMMARY: KEY FINDINGS

2.68B

The PRC has dominated U.S. inverter imports since 2015, exporting approximately 2.68 billion kilograms of inverters into the United States. As of 2024, PRC inverter exporters accounted for two-thirds of all inverter shipments globally.

5,400MW

Strider identified U.S. solar sites spread across 22 states that are using risky PRC equipment with combined capacity of at least 5,400 megawatts (MW)—enough to power over one million homes for a year. This widespread integration of PRC-made equipment is not a localized issue, but a nationwide vulnerability.

23%

Of the more than 800 PRC inverter/BESS manufacturers identified for this report, 184 companies (~23%) present direct statecraft risks, such as the organization is a sanctioned entity or as a direct connection to a high-risk entity.

2,723

Research by PRC defense institutions—including the People's Liberation Army (PLA) and national defense universities—shows a sustained effort to identify vulnerabilities and develop methods to disrupt the U.S. power grid.

Strider found 2,723 PRC research publications studying attacks to, or vulnerabilities of, power grids—many of which have never been translated into English. At least 225 of these publications are highly relevant to potential U.S. grid attacks according to Strider's methodology.

86%

86% of U.S. utilities surveyed for this report (which represent ~12% of U.S. installed capacity) rely on at least one risky PRC supplier.

Large swaths of the U.S. distributed energy resource (DER) ecosystem operate outside a coherent federal security framework, leaving the growing systemic vulnerabilities unaddressed.

INTRODUCTION

The United States and China are engaged in an intensifying strategic competition for economic, geopolitical, and military superiority—a rivalry spanning technology, data, resources, and ideological influence. Energy supply is one area where the U.S. faces mounting challenges. The PRC has achieved an electricity surplus nearly double its typical peak demand, while the U.S. grid operates with a much thinner reserve margin, further strained by accelerating energy demand.

Over the past two decades, the United States has steadily expanded the use of renewable energy technologies. Yet this transition has also introduced a new class of vulnerabilities within the nation's critical infrastructure. Across the country, power generation now relies on inverter-based systems produced by PRC companies. PRC manufacturers now dominate the global market for renewable energy equipment, supplying inverters and battery systems that are both affordable and technologically advanced. **As U.S. utilities race to meet rising demand for clean power, these PRC-made systems have become embedded in the nation's grid infrastructure.**

Recent intrusions by Volt Typhoon—a PRC state-sponsored cyber group that infiltrated U.S. critical infrastructure networks—have underscored the growing risk of foreign access and control over domestic systems. These operations reveal how China's cyber capabilities can exploit commercial dependencies and pre-position for potential disruption. Modern inverters are not merely converters of current; they are networked systems that manage energy flow, stabilize frequency, and communicate across the grid. That connectivity now represents a strategic liability. **Each device can be accessed remotely, creating a web of potential entry points into America's power infrastructure.** Without stronger oversight, this dependence could give the PRC government asymmetric leverage—the ability to influence or disrupt systems critical to America's energy future.

While there are many facets regarding U.S. critical infrastructure protection from state-sponsored attacks, this report will focus exclusively on potential risks to inverters as an illustrative example of the risks posed by the PRC state on U.S. critical infrastructure.

THE RISE OF DISTRIBUTED ENERGY RESOURCES AND GAPS IN THE REGULATORY LANDSCAPE

The U.S. power grid currently runs with very little spare capacity. According to North American Electric Reliability Corporation's (NERC) 2025 Summer Reliability Assessment, many regions in the United States already project reserve margins to be insufficient during extreme weather conditions. At the same time, national electricity demand is rising sharply. Bank of America estimates an average annual growth rate of 2.5% through 2035, five times higher than the past decade.

Under these conditions, renewable energy resources —particularly solar power and battery energy storage systems—have become necessary alternatives to conventional power generation due to their lower cost barrier, faster installation times, and the ability to fill in the gaps in electricity demand. These advantages are driving rapid adoption, transforming how the United States produces and manages power amid growing pressure on grid reliability.

Power from inverter-based resources (IBRs) is less centralized than traditional generation, with distributed energy resources (DERs), such as community solar farms and commercial solar installations, integrating excess power into the grid through Power Purchase Agreements with utility companies. **While large utility-scale producers have mandatory, prescriptive safeguards, thousands of IBR power installations across the United States do not, leaving them vulnerable.**

Even with stricter rules enacted in 2025, smaller IBR operators lack compliance requirements, often operating with insufficient security hygiene and little to no oversight from government authorities. Data from the U.S. Energy Information Administration (EIA) shows that more than 5,300 solar power sites in the United States have between 1 and 20 MW of capacity. These sites are below NERC's new 20 MW reporting limit that began in January 2025, leaving the majority of utility-scale solar projects outside of any federal reliability standards (EIA defines "utility-scale" as plants with ≥1 MW). Moreover, NERC only applies strong security rules to very large power plants—those above 1,500 MW in total size—**meaning that nearly all U.S. solar facilities are required to follow only basic requirements.**

FROM VOLT TYPHOON TO ADVERSARIAL RESEARCH

HOW THE PRC IS TARGETING THE U.S. GRID

PRE-POSITIONING FOR DISRUPTIONS

In 2024, U.S. agencies confirmed that PRC state-sponsored group Volt Typhoon had compromised networks across communications, energy, transportation, and water system sectors, intrusions believed to be preparation for potential disruption during a future crisis. Citing PLA text, **the U.S. Department of Defense assessed in 2024 that PRC actors could launch cyberattacks that, "at a minimum, cause localized, temporary disruptions to U.S. critical infrastructure."** Dragos, an operational technology cybersecurity firm, documented a 300-day intrusion at a Massachusetts utility by Volt Typhoon, illustrating this threat.

REMOTE ACCESS AND UNDOCUMENTED COMPONENTS

In November 2024, PRC company Deye disabled inverters in the United States, United Kingdom, Puerto Rico, and Pakistan following a dispute with a U.S. distributor. This episode demonstrated that PRC manufacturers retain operational control over installed systems.

In 2025, multiple media and industry outlets reported on undocumented components found in PRC-made inverters that may create access risks unknown to end users. Even if not intentionally concealed, undocumented components pose a material risk to power operators, including those with mature security programs.

PRC RESEARCH ON U.S. GRID ATTACKS

Strider reviewed research publications from PRC-based organizations from 2010 to present that focused on vulnerabilities in the U.S. power grid.

Strider found 2,723 research publications studying attacks to, or vulnerabilities of, the U.S. power grid. Of these publications, 1,083 were originally published in Chinese and many have never been translated into English. Using proprietary risk methodology, Strider assessed that at least 225 of these publications are highly relevant to potential attacks against the U.S. grid, with many being authored by organizations or individuals connected to PRC state-owned enterprises or PLA-affiliated organizations.

Many of these publications reveal that PRC researchers have a sophisticated understanding of U.S. power grid vulnerabilities. Three examples include:

In 2025, a researcher at Jiangsu Open University proposed a new method of identifying critical nodes in scale-free networks. **To test the method, the researcher ran a simulation of the western U.S. power grid and was able to trigger structural collapse through the used algorithm.**

In 2023, four researchers from Lanzhou Jiaotong University—a public university which implements civil-military integration work—proposed penalized local structural entropy as an improvement on local structural entropy's ability to identify critical nodes in complex networks. **The researchers tested their new method in a simulated attack on the western U.S. power grid.**

In 2024, nine researchers from China Southern Power Grid, the Guangdong Provincial Key Laboratory of Power System Network Security, and Shanghai Jiao Tong University (SJTU)—all organizations overseen by the PRC government, and SJTU cooperates with defense companies—presented research on a novel attack strategy that uses runtime code fault injection to interfere with deep learning neural network models used for diagnosing faults in power grids. When tested against three models used for fault detection, the researchers managed to decrease their fault detection accuracy to 0%.

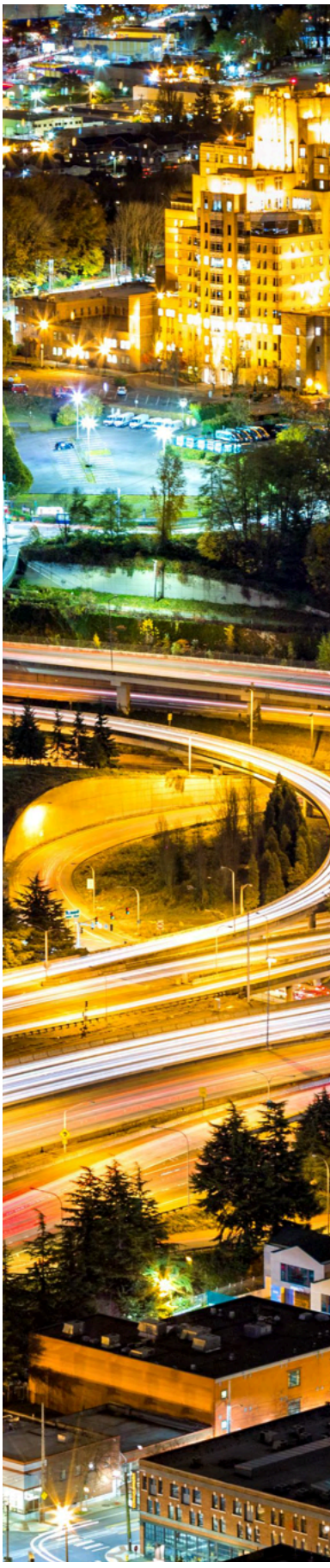
Three of the PRC organizations producing the most "high risk" research that is relevant to potential U.S. grid attacks include:

People's Liberation Army National University of Defense Technology (NUDT): Since 2018, NUDT-affiliated researchers have produced nine high risk publications. NUDT is the PLA's premier institution for scientific research and education and is directly subordinate to the Central Military Commission. The university is also hosts at least 10 major defense laboratories and is included in the U.S. Commerce Department's Entity List.

North China Electric Power University: Since 2014, researchers affiliated with North China Electric Power University campuses produced 17 high risk publications. North China Electric Power University was directly administered by the PRC's national power sector up until 2003 and is now jointly administered by the Ministry of Education and a council comprised of 12 state-owned power utility companies in the PRC.

State Grid Corporation of China (SGCC): Since 2012, SGCC-affiliated researchers produced 12 high risk publications. SGCC is a PRC state-owned enterprise, controlled by the State-owned Assets Supervision and Administration Commission under the PRC's State Council and one of the world's largest utility companies. It operates energy networks in the PRC, Brazil, the Philippines, Portugal, Australia, Italy, Greece, Oman, and Chile—many of which were established under the Belt and Road Initiative. This count is not inclusive of all SGCC subsidiaries.

The 2,723 PRC research publications focused on topics that could be used to facilitate an attack on the U.S. power grid, as well as the high-risk PRC entities conducting the research, collectively show a sustained effort to research disruption capabilities against U.S. infrastructure.



PRC EQUIPMENT PENETRATION AND RISKS IN THE U.S. MARKET

Since 2015, the PRC has been the largest exporter of inverters to the United States. As of 2024, four of the top five inverter exporters are PRC companies, accounting for two-thirds of all shipments globally. During this period, the PRC exported approximately 2.68 billion kilograms of inverters of all sizes and battery storage equipment (BESS) to the U.S.

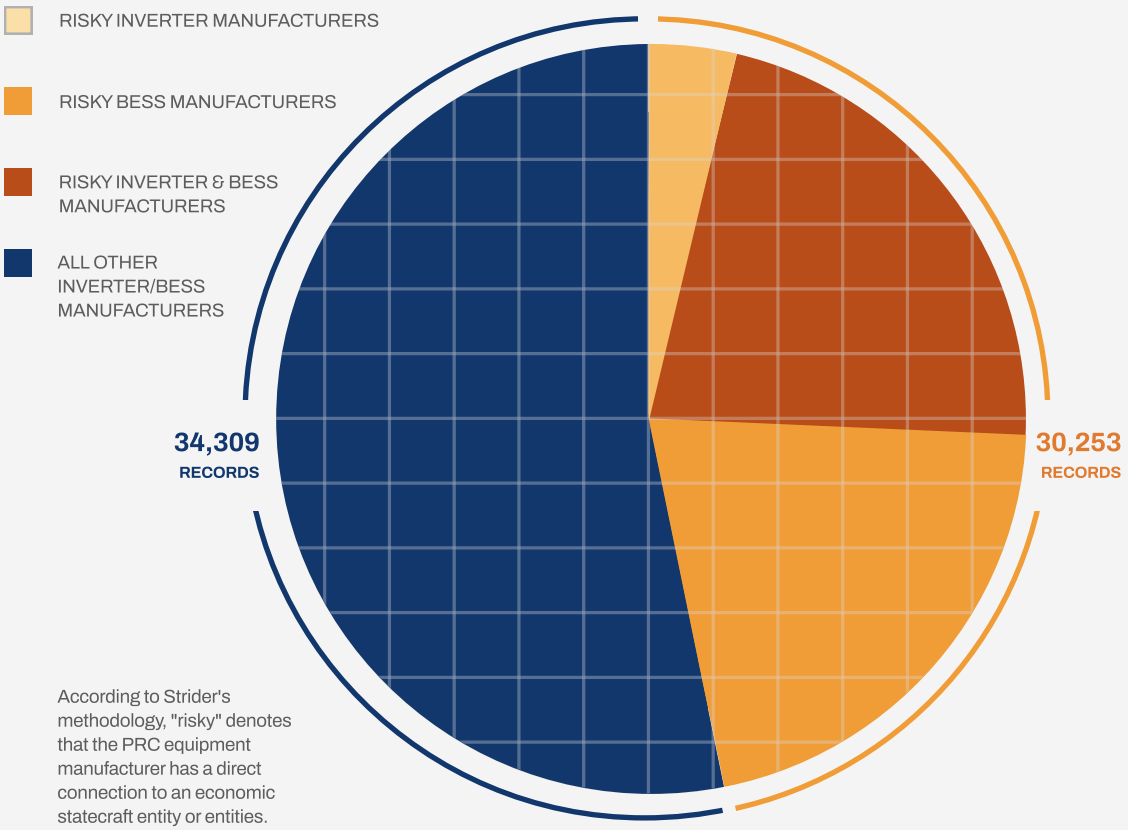
The PRC share of U.S. imports has fallen in recent years due to tariffs, but until 2019, t**he PRC was so dominant in the U.S. inverter market that its share was greater than the next 10 countries combined.** PRC manufacturers have also diverted manufacturing to countries such as Thailand, Malaysia, Vietnam, and India, meaning that the most recent U.S. customs data does not fully capture the flow of IBR equipment made by PRC companies. PRC dominance in inverters—bolstered by vertical integration, state support, and aggressive pricing—exerts practical pressure on U.S. IBR operators to source PRC equipment given its wide availability, competitive quality, and cost advantage.

Among the more than 800 PRC inverter/BESS manufacturers identified for this report, **184 companies (~23%) were identified as having a direct affiliation to a high-risk entity under Strider's methodology, such as the PRC military.**

At least **38 of these risky companies traded with the United States** in the past 10 years.

Nearly half (30,253 of 64,566) of U.S. inverter shipment records from 2015 to 2024 **were connected to PRC manufacturers with direct risks.**

SCALE OF PRC-LINKED EQUIPMENT IN THE U.S. MARKET, BASED ON SHIPMENT DATA (2015–2024)



According to Strider's methodology, "risky" denotes that the PRC equipment manufacturer has a direct connection to an economic statecraft entity or entities.

COMPANY	NUMBER OF RECORDS	PRODUCTS
Ecoflow	3829	BESS and Inverters
CATL	2572	BESS
Jinko Solar	2296	BESS and Inverters
JA Solar	1590	BESS and Inverters
CHINT/NOARK Electric	1186	Inverters
Huawei	498	BESS and Inverters
Sungrow	358	BESS and Inverters
GoodWe	120	BESS and Inverters
Gotion/Gotion High Tech	110	BESS
Other Risky Companies	17694	

PRC IBR EQUIPMENT USED BY U.S. UTILITY COMPANIES

Strider surveyed utility and energy companies representing approximately 12% of U.S. installed capacity and identified 23 PRC inverter and BESS suppliers. Of these suppliers, 13 had at least one statecraft "risk signal" according to Strider's risk methodology. 86% of the surveyed companies reported at least one risky PRC supplier in their power composition. For example, 71% reported equipment from Sungrow; 43% reported Huawei; 29% reported JinkoSolar; and 14% reported CATL.

To further illustrate the risk landscape, Strider chose to profile the following PRC companies for their high statecraft risk, level of integration into U.S. utilities, and volume of trade with the United States:

BYD

BYD is a leading PRC electric vehicle and battery manufacturer and maintains several high-risk connections with defense industry enterprises and U.S. government sanctioned entities. The company also plays a key role in PRC government talent recruitment programs.

CHINT Group Corporation (CHINT)

CHINT is a major PRC energy and electrical equipment company with global operations in renewable power and smart-grid systems. The company is a registered contract party to the People's Liberation Army and has frequently collaborated with PRC defense organizations.

Contemporary Amperex Technology (CATL)

CATL is the world's largest producer of electric vehicle batteries and energy-storage systems. In 2025, the U.S. Department of Defense labeled CATL a "Chinese military company," flagging national-security and sanctions exposure.

Huawei

Huawei has a documented history of IP theft accusations, export control violations, and close alignment with the PRC military, intelligence and law enforcement entities. The company was added to the U.S. Commerce Department's Entity List and banned from U.S. 5G networks due to espionage risks, but there is no federal rule banning Huawei solar inverters.

JinkoSolar

JinkoSolar is a Shanghai-based solar module manufacturer which supplies the PRC government and state-owned defense conglomerates. Along with Sungrow, JinkoSolar shapes PRC national PV standards and policies as a leader of the China Photovoltaic Industry Association. The firm maintains research partnerships with PRC defense universities and is the parent of at least three wholly owned subsidiaries in Xinjiang (may be subject to provisions in the Uyghur Force Labor Prevention Act).

Sungrow

Sungrow is a top PRC manufacturer of solar inverters widely used in global and U.S. energy infrastructure. 71% of U.S. utilities surveyed by Strider currently use Sungrow inverters, with several of them identifying Sungrow as a supplier of concern. The company has undertaken PRC state-funded R&D through the National Key R&D Program, which encourages overseas affiliates to support foreign expert recruitment and PRC innovation goals. Sungrow's CEO and Chairman is a member of the National People's Congress (NPC), legislative body of the PRC state, and nearly 30% of the company's senior management are Chinese Communist Party (CCP) members.

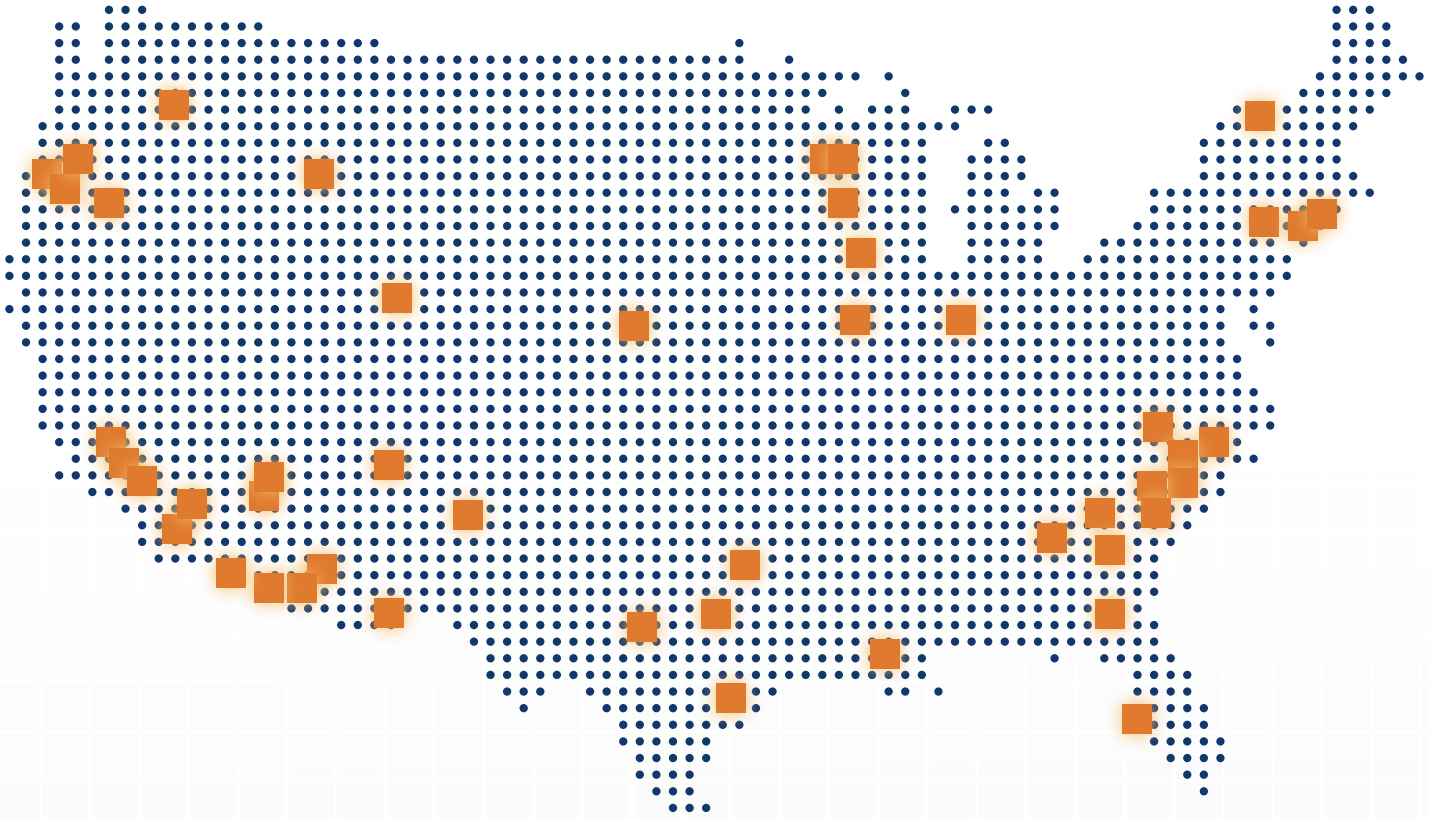
This report highlights a subset of PRC IBR equipment manufacturers with known statecraft risks. However, it must be emphasized that the PRC government has the capacity to compel any PRC entity to assist in state intelligence efforts through its 2017 National Intelligence Law. **Thus, PRC-manufactured IBR technologies carry latent vulnerabilities regardless of the supplier's apparent lack of risks or assurances of independence from the PRC government or the CCP.**

PRC EQUIPMENT IN U.S. SOLAR SITES

For a more narrowly scoped illustration of the vulnerabilities from PRC-made IBR equipment, Strider analyzed 66 solar sites using risky PRC suppliers (among 6,000+ strictly solar photovoltaic sites in the U.S.), with combined installed capacity of at least 5,400 megawatts. While this is a small subset of U.S. solar installations (the number of U.S. solar sites using risky PRC IBR equipment is certainly much higher than 66), these sites are spread across 22 states and represent a mix of PRC equipment installed into solar sites around the United States.

Here is a breakdown of the equipment used by the 66 solar sites:

- **51** Sites with Sungrow equipment
- **4** Sites with CHINT equipment
- **10** Sites with BYD equipment
- **1** Site with CATL equipment



Modern inverters collect real-time operational data to optimize performance and support grid stability. **Without effective access controls, this sensitive data can be exposed to third parties without operator knowledge or consent.** Such visibility enables near-real-time surveillance of U.S. distributed energy resources and aids the targeting and timing of disruptions with serious operational and national-security implications.

CONCLUSION

The U.S. power grid is one of the most critical assets underpinning our nation's security and prosperity. It powers every facet of modern life—hospitals, defense installations, communications networks, water systems, manufacturing, the financial and transportation sectors, homes, and more. The grid also fuels technological innovations like AI and quantum computing. Without a secure and resilient grid, these vital systems would falter, paralyzing both daily operations and national defense capabilities. The grid's interdependence with telecommunications, energy, and digital infrastructure makes it not just an engineering marvel, but the backbone of America's economic vitality and strategic readiness. **Safeguarding it is therefore not only an energy imperative but a national security necessity.**

The United States' clean energy transition, while vital for economic and energy resilience, is progressing with critical blind spots that pose growing national security risks. PRC-made inverter and battery systems are deeply embedded across the U.S. power grid, creating dependencies that could be exploited in a crisis. Evidence of PRC-linked cyber operations such as Volt Typhoon, combined with documented research by PRC defense-affiliated institutions on power grid disruption, underscores that these risks are not theoretical—they are strategic. **Weak oversight of distributed energy resources, fragmented regulatory standards, and limited visibility into foreign-made components collectively expose the U.S. grid to potential compromise.** Addressing these vulnerabilities is essential to ensuring that America's pursuit of clean energy enhances, rather than undermines, its security and resilience.

U.S. policymakers must develop a coordinated, forward-looking strategy on renewable energy technology that addresses the national security dimensions of foreign procurement. As demand for electricity accelerates, the U.S. grid will become more reliant on distributed generation and energy storage. Without intervention, the U.S. renewable energy infrastructure will serve as potential entry points for adversaries to disrupt and manipulate the power supply.

U.S. security planners should assume that **the PRC has capability and the will to affect U.S. grid stability in a time of crisis.** This assumption should guide strategic planning, procurement decisions, and threat exercises across every level of government.

Security regulations governing IBRs should be tightened, such as adjusting the thresholds for NERC's Low Impact category, or requiring a separate set of broader, prescriptive operational and security programs for IBRs.

Similar to policies over the last six years banning the Huawei from 5G networks, **U.S. policymakers should enact laws that integrate security with energy policy,** such as banning equipment manufactured by certain PRC companies, coupled with appropriate rate recovery mechanisms to offset the cost of government-mandated equipment replacements.

STRIDER

In this new era of Great Power Competition, **securing the resilience of U.S. critical infrastructure is not optional.** A coordinated effort among government, industry, and allies is critical to ensure that America's clean energy transition strengthens—not weakens—its security posture.

For sourcing information or more insight into information detailed in this report and Strider's tools, reach out to our team via email at info@striderintel.com.

STRIDERINTEL.COM