Securing Battery Energy Storage Systems from Cyberthreats

BEST PRACTICES AND TRENDS

PREPARED BY

Peter Fox-Penner, The Brattle Group
Phil Tonkin, Dragos
Justin Pascale, Dragos
Noah Rauschkolb, The Brattle Group
Purvaansh Lohiya, The Brattle Group

December 2025

Brattle

DRAGOS

NOTICE

- This white paper reflects the perspectives and opinions of the authors and does not necessarily reflect those of The Brattle Group's clients, Dragos's customers, or other consultants. We appreciate the assistance of Pablo Ruiz, Laura Burns, Abbie Munafo, Jack Kalinski, and Zack Mahon in preparing this report.
- This work was supported by Fluence Energy. We are grateful for input from Katherine Hutton, Ben Smith, Lars Stephan, Suzanne Leta, and Mike Weiner.
- Where permission has been granted to publish excerpts of this white paper for any reason, the publication of the excerpted material must include a citation to the complete white paper, including page references.

Executive Summary

With electricity demand surging worldwide, battery energy storage systems (BESSs) are emerging as a key tool for grid operators to ensure reliability and maximize the use of renewable generation. Over the next five years, BESS deployment is expected to grow at 30% annually in the United States, 45% in the European Union (EU), and 20–25% across Japan, South Korea, Southeast Asia, and India.[*],[†] As BESS deployment accelerates, it is important that the increasing role of batteries in facilitating efficient clean energy and grid reliability is not undermined by cybersecurity vulnerabilities. Conversely, BESS additions with strong cyber-protection will contribute to lower levels of vulnerability for the grid as a whole.

This white paper examines the nature of cybersecurity threats for utility-scale BESSs from the perspective of BESS ODOMs (owners, developers, operators, and maintainers), the evolving regulatory and policy landscape supporting safe integration of BESSs, and actionable strategies for ODOMs that can help mitigate cyber threats for such systems.

THE CYBERTHREAT LANDSCAPE FOR BESS

The cybersecurity threat landscape for BESSs is characterized by several key factors:

- **Component standardization**. BESSs have become increasingly standardized in order to reduce cost and complexity. One consequence of this increase is that the sophistication necessary to organize cyberattacks has decreased. This risk is propagated by the development of industrial control system (ICS)-specific malware able to manipulate a variety of industrial technologies.
- **Reliance on foreign-sourced materials.** Dragos has observed many foreign threat groups specifically targeting electric sector entities, such as VOLTZITE (also known as Volt Typhoon), who have also been identified by the US Cybersecurity and Infrastructure Security Administration (CISA) as seeking to disrupt critical infrastructure via cyber means. VOLTZITE's affiliation with the People's Republic of China (PRC), demonstrates the risk posed by supply chains encompassing foreign-sourced controls and software. In many

[*] Wood Mackenzie, "United States grid-scale energy storage outlook 2024," July 1, 2024, https://www.woodmac.com/reports/power-markets-us-grid-scale-energy-storage-outlook-2024-150289219/ and European Market Outlook for Battery Storage 2025-2029 - SolarPower Europe.

[†] Bloomberg NEF, Global Energy Storage Market to Grow 15-Fold by 2030, Press Release, August 12, 2022, https://about.bnef.com/insights/commodities/global-energy-storage-market-to-grow-15-fold-by-2030/.

cases, asset owners or operators are unable to inspect or monitor these components due to limits set by contractual agreements, endangering the security of their systems.

- **Consequences of a successful attack.** At the individual asset level, revenue losses from forced outages due to a successful cyberattack in the US can reach up to $1.2 million for a single 100 MW, 4-hour duration (400 MWh) system, and similar values in other global markets such as in Germany or the UK. If the asset is permanently damaged, the capital losses can be over an order of magnitude greater. The losses to the regional economy, community, and possible national defense could be larger still.

TRENDS IN CYBER REGULATION OF BESS

To understand where BESS cybersecurity regulations are trending, the Brattle/Dragos team interviewed 9 leading industry experts and former federal officials on emerging trends in cybersecurity policies, regulations, and standards applicable to large-scale batteries in the US and the EU.

Regarding the US, experts agreed that infrastructure security concerns will likely lead to more stringent security measures towards FEOCs (Foreign Entities of Concern). While there was disagreement among the experts on the effectiveness of current federal policies targeted at reducing BESS risks, there was consensus that both Congress and the executive branch are likely to strengthen policies involving FEOCs. These efforts will build on bills already introduced in Congress and executive orders from both the Trump and Biden administrations aimed at protecting critical infrastructure, reviewing supply chains, and reducing dependence on FEOCs. States may also step up to play a larger role, as exemplified in California (Cal-CSIC), Texas (Lone Star Infrastructure Protection Act), Arizona (HB 2736), and Georgia (SB 346). Furthermore, experts saw the potential that prescriptive standards from the industry may play a role in enhancing the security of supply chains and component verification efforts, though not as a substitute for federal policies.

In the EU, owners and operators are subject to the risk-based NIS2 (Network and Information Security 2) directive, where they must demonstrate that all their controls are “defendable” under attack. NIS2 also expanded from NIS1 to include smaller BESS systems, reflecting that in an interconnected grid, even small BESS systems can cause significant damage. The EU also introduced the Cyber Resilience Act, which when it goes into effect in 2027, will certify every product for sale in the EU meets EU cybersecurity standards. While experts agree that consistent, EU-wide policy is the correct method to approach grid cybersecurity, member states do not have the same agenda or policies, creating a lack of harmonization among operators on the same grid. Diverging rules between European countries create vulnerability to the highly interconnected European power network, resulting in higher regulatory compliance costs for investors and differing levels of cybersecurity implementation in the European internal energy market.

PROACTIVELY MANAGING BESS CYBERTHREATS

To effectively mitigate cyber risks for new BESS installations, ODOMs should implement the following safety measures:

- Secure Design and Development Assurance
  - Require vendors to provide documentation on secure development lifecycle practices
  - Require verified Hardware and Software Bill of Materials (HBOMs and SBOMs) for OEMs and other vendors to identify and assess if software components come from trustworthy sources and to analyze geographic and corporate source components and associated vendors
  - Control over software updates that incorporate vulnerability exposure checks and mitigation
- Supply Chain Risk Management
  - Require vendors to demonstrate due diligence on sub-suppliers and contract manufacturers
  - Require vendors to demonstrate chain of custody procedures for component delivery, installation, and post-deployment verification
- Product Security Controls
  - Create a defensible architecture with proper segmentation or zoning of assets and safe shutdown modes
  - Secure remote access provisions, such as role-based access controls
  - Log all network connections between and within operating sections of the facility
  - Harden guidelines for secure configuration baselines
- Operations and Maintenance
  - Monitor network activity and asset inventory for threat activity, vulnerabilities, changes, and misconfigurations
  - Document the incident response process and collaboration plan between asset owners, operators, and vendors in case of breach
  - User access lifecycle management, such as periodic access reviews and revocation upon role changes

  - Upgradable/evergreen digital architecture to support integration of future cybersecurity capabilities to support continued resilience during the lifetime of the system
- Contract Commitments
  - Define response times for vulnerabilities, breaches, patch releases, and support requests
  - Require vendor to provide recent third-party security assessment attestation or allowing asset owner to conduct testing
  - Require vendor to maintain formal coordinated vulnerability disclosure policy
  - Require vendor to verify cyber insurance coverage for liabilities arising from security failures

For all these measures, a proactive approach is important to mitigate the risks of a cyberattack and is much more cost-effective than a retrospective approach. These measures, applied proactively, can ensure BESSs are able to effectively contribute to grid security in the face of increasing electricity demand around the world.

LIST OF ACRONYMS

AC	Alternating current
AESCF	Australian Energy Sector Cybersecurity Framework
ALEC	American Legislative Exchange Council
BESS	Battery Energy Storage Systems
BMS	Battery Management System
BTM	Behind-the-meter
C2	Command and Control
Cal-CSIC	California Cybersecurity Integration Center
CERT	Cyber Emergency Response Team
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Administration
CRA	Cyber Resilience Act
CVE	Common Vulnerabilities and Exposures
DC	Direct current
ERCOT	Electric Reliability Council of Texas
FEOC	Foreign Entity of Concern
HBOM	Hardware Bill of Materials
HMI	Human-Machine Interface
ICS	Industrial Control System
INL	Idaho National Lab
ISO	Independent System Operator
LOTL	Living off the Land
MFA	Multi-Factor Authentication
NERC	North American Electric Reliability Council
NIS	Network and Information Security
ODOMs	Owners, Developers, Operators, and Maintainers
OEM	Original Equipment Manufacturer
OOB	Out-of-band
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology: the industrial equivalent of information technology (IT)
PCS	Power Control System
PLC	Programmable Logic Controllers
RAT	Remote Access Trojan
RTU	Remote Telemetry Unit
RDP	Remote Desktop Protocol
SBOM	Software Bill of Materials
SLA	Service Level Agreement
SRA	Secure Remote Access
TTP	Tactics, techniques, and procedures: a framework used to understand and categorize the behaviors of threat actors

I. Introduction

A. Overview

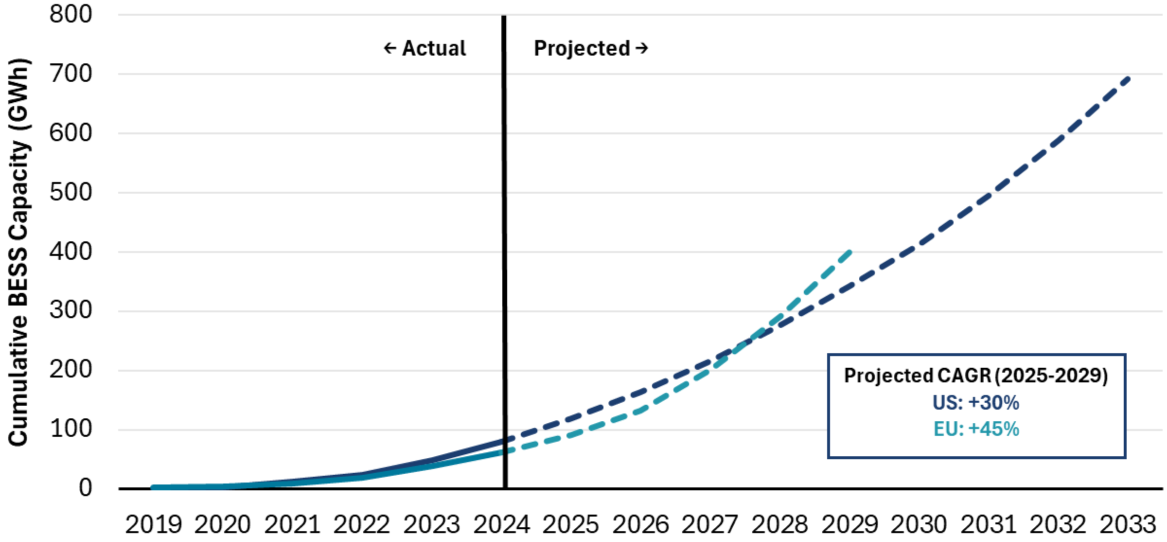
Electric power systems across the globe are entering a new era of transformation, spurred by the convergence of rapid growth in demand from data centers and electrified load, a long-term shift to decarbonized energy, and increased geopolitical tensions. To manage this vastly larger and more complex architecture, new systems will be highly digitized, intelligent, and interconnected. Within this environment, grid-scale batteries are improving grid stability and reliability while reducing production costs and increasing the utilization of energy from low-cost generation, including renewables.

The deployment of grid-scale battery energy storage systems (BESSs) is expected to surge dramatically. In the United States, utility-scale BESS capacity is projected to increase by more than 300% by 2033, according to forecasts from Wood Mackenzie.[1] Within the European Union, sales of BESSs are expected to reach 80 GWh annually by 2028, up from 17.2 GWh in 2023 (see Figure 1).[2]

[1] Wood Mackenzie, “United States grid-scale energy storage outlook 2024”, July 1, 2024, https://www.woodmac.com/reports/power-markets-us-grid-scale-energy-storage-outlook-2024-150289219/.

[2] European Market Outlook for Battery Storage 2025-2029 - SolarPower Europe.

FIGURE 1. HISTORIC AND PROJECTED GROWTH OF BESS ENERGY STORAGE CAPACITY 2019–2033



Source for US: Wood Mackenzie, "US Utility-Scale Energy Storage Outlook H2 2024," February 2025, https://www.woodmac.com/reports/power-markets-us-utility-scale-energy-storage-outlook-h2-2024-150351455/.
Source for EU: SolarPower Europe, *"European Market Outlook for Battery Storage 2025–2029,"* May 2025, https://www.solarpowereurope.org/insights/outlooks/european-market-outlook-for-battery-storage-2025-2029/detail.

As BESSs become more widespread and their operational role on the power system grows, it will be crucial to ensure that they are secure against cybersecurity risks. As the electric grid faces growing cyber threats, BESSs represent a unique and underleveraged asset in strengthening grid resilience – not because they are legacy infrastructure, but precisely because they are not. Unlike legacy generation assets, which are often costly, complex, and slow to modernize due to their scale and age, BESSs offer a flexible and modern platform that can be *secure by design*.

While most large-scale power system assets rely on cloud-connected controllers and remote management, BESS control systems are currently also reliant on international supply chains. This makes it difficult to authenticate their cybersecurity credentials. Combined with other indicators, this appears to be leading to an increase in the perceived value of cyber threats targeting BESS systems for cyberattacks while they are still in an early stage of deployment. Given the expected growth of BESSs in the coming years, proactive measures by policymakers as well as owners, developers, operators, and maintainers (ODOMs) to protect additions to the BESS installed base are quite timely. [3]

This white paper examines the emerging cybersecurity risks associated with utility-scale battery energy storage systems. Specifically, it aims to:

- Assess the nature of cyber threats facing BESS ODOMs, which are also relevant to many other stakeholders, including financial institutions;
- Review evolving regulatory and policy frameworks aimed at mitigating these threats; and
- Explore actionable strategies that ODOMs can adopt to enhance the cybersecurity posture of their systems.

While cybersecurity across the broader electric power sector is an essential and rapidly evolving field, this paper narrows its focus to utility-scale BESSs – typically 20 MW (80 MWh, if the system is 4-hour duration) or larger – which have become critical nodes in modern grid infrastructure. We do not address the broader subject of utility grid cybersecurity, a vast and important topic, and we also do not address cybersecurity issues specific to small-scale distributed energy resources, such as smaller behind-the-meter (BTM) batteries that may be installed by homeowners or businesses, though these assets would be vulnerable to many of the same pathways that could be used to interfere with a utility-scale system.

Finally, this white paper is focused on remotely-triggered cybersecurity threats, not physical threats to BESSs from kinetic attacks. It also does not address policies for vetting and overseeing personnel with physical access to BESSs, which can be a pathway for malicious actors to cause damage or loss to a single BESS facility or a larger grid disruption. These issues are important elements of fully protecting any piece of critical infrastructure but are beyond the scope of this paper.

[3] There is already a large installed base of BESSs and other inverter-based resources that may have unaddressed cyber vulnerabilities (see Section II). While this white paper takes a forward-looking view on reducing cyber risks, the existence of potential legacy weaknesses increases the importance of reducing additions to the current threat level, especially as the installed base of BESSs scales substantially.

B. Components of a Modern BESS

FIGURE 2. COMPONENTS OF A MODERN BATTERY ENERGY STORAGE SYSTEM (DC BLOCK STRUCTURE). BURGUNDY COMPONENTS HAVE THE HIGHEST LEVEL OF CRITICALITY OF CYBER AND PHYSICAL THREATS. YELLOW COMPONENTS HAVE A MEDIUM LEVEL OF CRITICALITY.

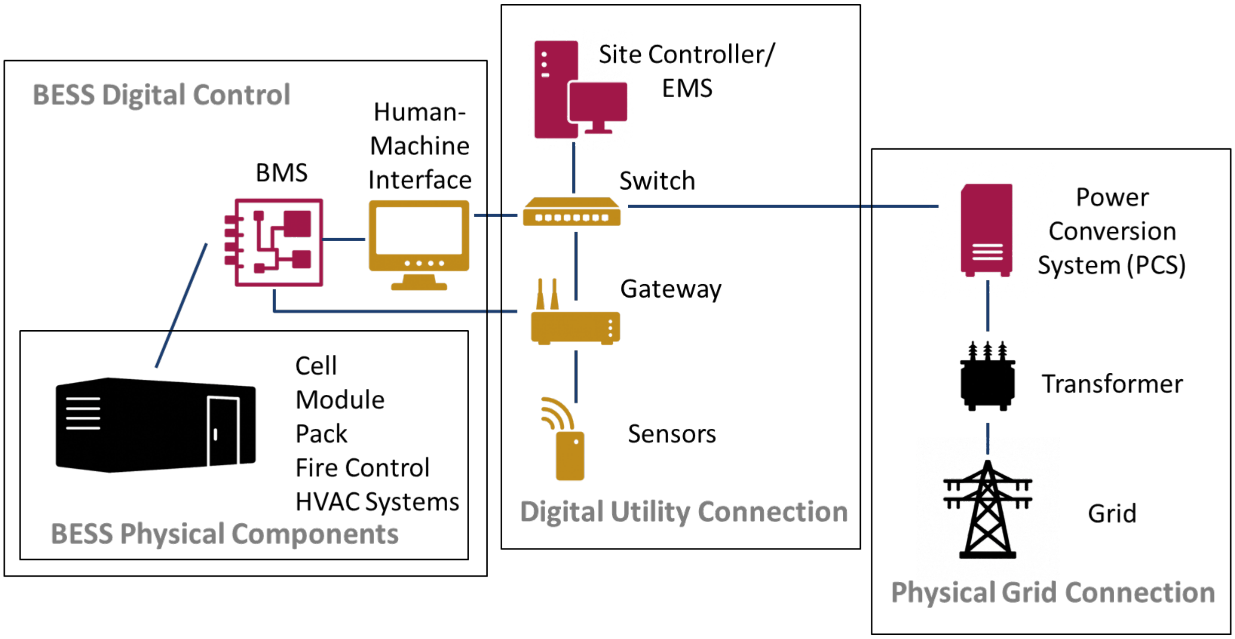
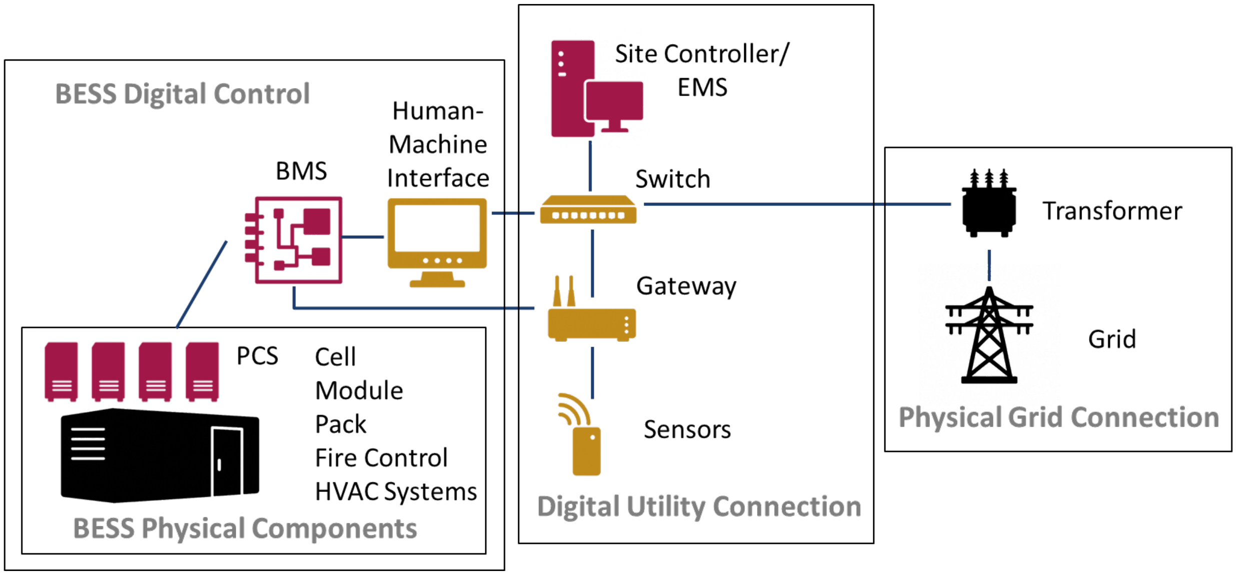


FIGURE 3. COMPONENTS OF A MODERN BATTERY ENERGY STORAGE SYSTEM (AC BLOCK STRUCTURE).



Source: Adapted from Center for Securing Digital Energy Technology, Idaho National Laboratory.

Modern-day utility-scale BESSs have one of two relatively standard component architectures, a DC block structure or an AC block structure. Figures 2 and 3 show simplified BESSs with each of the two structures, respectively.

Both structures contain the same four categories of components: cell modules and packs, which store the power; charging and discharging circuitry; power conversion systems to allow power flow to and from users and/or the grid; and communications and control systems for all parts of the system.

In both types of systems, the physical infrastructure surrounding the entire system includes HVAC equipment to maintain safe climatic conditions in the BESS, fire protection systems, and other physical protection elements (bottom left of Figures 2 and 3). All of these elements are essential for the function of a BESS; the elements that are digitally controlled (or "smart"), such as the control systems, are the portions that are vulnerable to cyber intrusions. In Figures 2 and 3, the components colored in burgundy have the greatest vulnerability to cyber intrusions, followed by yellow components. The black components generally do not have sensors or logic, so they are not at risk of a cyber intrusion.

One of the two main designs, a DC Block Structure, is illustrated in Figure 2. The core of all types of BESS systems (lower left of figure) is a group of battery cells built into modules and packs and surrounded by cooling and fire control systems. This hardware typically comes with monitoring and some control capability, but all communication to access these functions typically occurs via the battery management system (BMS).

The BMS is a combined hardware and software package designed to manage and monitor a rechargeable battery system and is the deepest point within the system where remote access is possible. The BMS is often supplied by the cell manufacturer, who often uses its communication portal to send firmware and software updates. OEMs are including increasing amounts of intelligence (in the form of AI and algorithms) in BMS and other control levels to improve the operation of batteries, which increases the complexity of 3rd party validation due to the complex and proprietary nature of such software.

As shown in the figure, the BMS is the first part of a portion that controls the power activities of the BESS. The BESS typically connected to both remote and onsite control dashboards, shown in the figure at the Human-Machine Interface (HMI). These components link to an Energy Management System (EMS), which instructs the BESS to charge or discharge based on instructions from the grid operator, asset operator, and/or its own economic optimization algorithms.[4]

Several additional components in the center of the figure serve as the gateway to secure communication and control with power system operators. These operators must maintain the ability to control charging and discharging of the BESS as well as connection/disconnection under emergency conditions. All elements in this portion of the BESS may be from domestic or foreign vendors, contain substantial amounts of software, and may be remotely accessible.

The final parts of a BESS (in the right side of the figure) physically manage the flow of electricity to and from the BESS. In a DC block structure such as Figure 2, BESS energy flows from the physical system in the bottom left through the switches and the power conversion system (PCS), which is the locus of local physical control of BESS DC energy. The PCS includes a central inverter, which changes the battery from DC into AC suitable for the main power grid. The transformer following the inverter changes the AC voltage to grid levels and is typically the boundary between the BESS and the grid.

A BESS with an AC block structure (Figure 3) is somewhat similar to the DC structure just described, with a few important differences. In an AC structure, the DC power stored in each battery module is converted to AC by smaller inverters (power conversion systems (PCSs)) located near the modules. Then, as in the DC block structure, the charging or discharging power is managed by the BESS Digital Control portion of the system (top left section of the figure), connected and controlled via the Digital Utility Connection portion of the system (center section of the figure), and physically connected to the grid via a transformer (right section of the figure).

These two figures illustrate that BESS systems contain several large components that combine extremely large amounts of internal software with communication capabilities. Many of these components, including PCSs and BMSs, are not unique to BESS systems and are often sourced from foreign manufacturers that build in remote access functionality to allow for monitoring and software updates. The many points of remote access enable systems to be efficiently monitored, controlled, and maintained remotely, but also create cybersecurity vulnerabilities.

[4] Utilities also use a system referred to as an “Energy Management System” in their control centers to control multiple power plants on their system. Although this is analogous to the EMS that controls one or several BESSs, it is part of the utility system and distinct from the EMS within a BESS.

C. Classifying Threat Actors – Evolving US and European Descriptions

Cyberthreat actors fall on a spectrum between fully-state-sponsored and largely independent. In the context of national security, a common criterion for policy action is the country in which the equipment manufacturer or service provider is domiciled. One important early example was the Bipartisan Infrastructure Law (Nov. 2021), which defined Foreign Entity of Concern (FEOC) as an entity "owned by, controlled by, or subject to the jurisdiction or direction of a government of a foreign country that is a covered nation." Subsequent legislation, such as the Inflation Reduction Act (August 2022), incorporated this definition to limit battery components and critical minerals sourced from FEOCs in electric vehicles that elect the Section 30D Clean Vehicle Credit.

The recently-enacted 2025 "One Big Beautiful Bill Act" (OBBBA) defines "Prohibited Foreign Entities" (PFEs) as either "Specified Foreign Entities" (SFEs) or "Foreign-influenced Entities" (FIEs). Briefly, PFEs are companies over whom control in some form by China, Russia, North Korea, and/or Iran is large enough (as explained below) to limit the availability of tax credits. The tests for whether a project is sufficiently controlled by a PFE include computing the fraction of project materials supplied by PFEs, analysis of a potential PFE's ownership or financial support by one of the four named countries and ensuring that licenses and contracts do not give PFEs effective control over a project.[5]

As mentioned, material sourcing restrictions related to PFEs were also broadly expanded in the OBBBA, which placed restrictions on a variety of technologies seeking federal tax credits, including battery storage. A 2024 Executive Order on limiting access to personal and governmental databases directed the Attorney General to apply the order to any "country of concern," defined as a nation that:

1. Has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons; and

[5] See Key Provisions of the One Big Beautiful Bill Act | Covington & Burling LLP and Keith Martin, et al, Working Through The FEOC Maze | Norton Rose Fulbright - July 2025.

2. Poses a significant risk of exploiting government-related data or bulk US sensitive personal data to the detriment of the national security of the US or security and safety of US persons.[6]

The final rule implementing the Order identified China, Cuba, Iran, North Korea, Russia, and Venezuela as countries of concern.[7] Similarly, the US Department of Commerce issued another executive-order-based rule in December 2024 designed to secure all US IT and communications from cyber and other national security threats. This rule used the term “foreign adversaries” to classify nations whose technology companies would be covered by the rule and classified the same six countries as adversaries.[8] A connected-vehicle rule was also issued in January 2025.[9]

There are no similar rules that apply specifically to control equipment in BESSs, but there have been legislative proposals that single out BESSs, such as the newly proposed Decoupling from Foreign Adversarial Battery Dependence Act passed by the US House of Representatives on March 10, 2025. Despite its title, the language of the Act primarily bars six specific Chinese BESS OEMs from receiving appropriated US funds but does not contain a new definition of foreign adversaries.

In the European Union, similar reservations concerning “high-risk providers” have driven a parallel policy trajectory around telecommunication infrastructure. The EU’s Coordinated Risk Assessment on Cybersecurity in 5G Networks established a precedent for scrutinizing the geopolitical exposure of vendors based on non-technical vulnerabilities. Key risk scenarios included state interference via pressure on suppliers under jurisdictional control of foreign governments, particularly where democratic safeguards or bilateral data protection agreements are absent.[10] These assessments culminated in several EU member states banning high-risk providers, including Huawei and ZTE from national 5G infrastructure. The EU’s methodology explicitly considers a supplier’s corporate structure, ownership ties to third-

[6] Joseph R. Biden, Jr., Executive Order on Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, February 28, 2024, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[7] 28 CFR pt. 202.601. https://www.ecfr.gov/current/title-28/chapter-I/part-202/subpart-F/section-202.601

[8] 15 CFR 791.4. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-E/part-791/subpart-A/section-791.4

[9] Final CVs Press Release 1.13.25.pdf.

[10] NIS Cooperation Group, “Cybersecurity of 5G networks EU Toolbox of risk mitigating measures,” CG Publication 1/2020, 23 *Policy and Legislation*, January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

country governments, and the legislative environment of their home country, including the ability of those states to exert coercive influence.

This framework is now extending beyond telecommunications. Under Article 22 of the NIS-2 Directive, the European Commission has initiated coordinated risk assessments for additional critical sectors, including solar PV and wind supply chains. These developments highlight the EU’s move toward a consistent doctrine of "tech sovereignty" and the potential for similar assessments to be applied to battery energy storage systems (BESSs) and other grid-edge technologies in the near future.

II. Cybersecurity Challenges and Risks for BESS Systems – Threat Landscape and Impacts

A. General Considerations

While regulatory bodies have been concerned with threats to electric sector infrastructure for nearly twenty years, recent geopolitical tensions have highlighted the industry’s rapidly evolving threat landscape. Russia's invasion of Ukraine in February 2022 marked the onset of an aggressive combination of kinetic and cyberattacks on critical infrastructure, featuring advanced malware attacks on electric power operations and a surge of cyberattacks by ideologically-driven hacktivists. The conflict between Israel and Hamas later that year echoed elements of this pattern, with a proliferation in the number of actors targeting critical energy infrastructure and cyber operations playing the role of strategic or tactical complements to physical assaults. These events suggest a new norm: critical infrastructure (including all facets of electric power) is increasingly at risk due to geopolitical conflict as well as cybercrime.

Threat models for the electric sector have also become increasingly complex as small-scale generation, grid-edge technology, and BESSs are leveraged to enhance power delivery efficiency. While these global efforts to overhaul existing infrastructure have undoubtedly bolstered grid operations, the large-scale deployment of interconnected and homogenous power systems raises security concerns. Specifically, BESSs provide electric sector entities with a scalable solution to reliability concerns stemming from fluctuating power demands.

However, these systems also leverage capabilities that enable vendor remote access and cloud-based applications for monitoring and maintenance, allowing systems to be deployed in facilities without on-site operators. The distributed nature of these digital systems expands the potential for cyberattacks as threat groups have demonstrated an increasing propensity to exploit remote connectivity into operational environments. In 2024, 20% of all incidents responded to by Dragos involved an exploitation of remote access, including VPN exploits, remote access applications, and remote desktop protocol (RDP) from corporate networks.

B. Cyberthreats To BESS Installations

The rapid adoption of BESSs must consider latent threat actors interested in exploiting the immediate impact battery storage has on grid stability. Adversaries have repeatedly demonstrated their ability to evolve, leveraging unforeseen technological vulnerabilities for malicious intent. For asset owners, the coming years will necessitate a proactive, anticipatory approach to cybersecurity to ensure a secure and sustainable energy future.

The ability of adversaries to damage critical infrastructure via cyberattacks was exemplified by the 2010 Stuxnet attack on an Iranian nuclear facility. Stuxnet was a complex, purpose-built malware capable of causing centrifuges controlled by infected programmable logic controllers (PLC) to alternate between operational extremes in quick succession. The malware also masked operational values to prevent detection and impair recovery processes. These functionalities resulted in physical damage to site centrifuges and sowed doubt among Iranian engineers regarding the efficacy of their instrumentation.

Dragos currently tracks 18 threat groups that are actively targeting the electric sector, have impacted organizations in the electric sector, or have demonstrated the capability to impact electric operations. A threat group is defined by the capabilities they have, the infrastructure they use, and the victims that they target. The groups that Dragos tracks are specifically focused on industrial operations. The capabilities they have include their tactics (what they do), techniques (how they do it) and procedures (the steps they take and the tooling they use) (i.e., TTPs).

This is an increase from 11 active threat groups in 2021. While the threat groups tracked by Dragos – particularly VOLTZITE and XENOTIME – have historically targeted traditional energy infrastructure, they have demonstrated a desire to expand their capabilities by increasing supply chain-based reconnaissance efforts. This strategic shift indicates that adversaries are motivated to expand their breadth of attack, making the decentralized, rapidly scaling nature of BESS deployments a potential target set.

The increase in adversaries targeting OT environments is due in large part to the increasingly homogenous nature of industrial deployments. Historically, asset owners designed highly custom facilities, which often included equipment procured from various vendors and original equipment manufacturers (OEMs) and bespoke protocols. However, modern facilities have become increasingly standardized by leveraging a single OEM for all major system components. This approach has enabled asset owners to reduce cost and complexity when scaling operations. However, the standardization of industrial environments has inadvertently reduced the sophistication required for adversaries to successfully target OT assets. Furthermore, adversaries are now capable of targeting a more diverse target pool via ICS-specific malware.

As an example, CHERNOVITE'S PIPEDREAM was discovered in 2022 and is the seventh known industrial control system (ICS)-specific malware. PIPEDREAM is a modular ICS attack framework that an adversary could leverage to cause disruption, degradation, and possibly destruction, depending on targets and the environment. PIPEDREAM can execute 38% of known ICS attack techniques and 83% of known ICS attack tactics. Moreover, PIPEDREAM can manipulate a variety of industrial control programmable logic controllers (PLC) and industrial software and can attack ubiquitous industrial technologies including CODESYS, Modbus, and Open Platform Communications Unified Architecture (OPC UA). Prior to the discovery of PIPEDREAM, ICS-capable malware was typically developed for a specific target. However, the modular nature of PIPEDREAM further indicates that threats are evolving their capability to impact distributed infrastructure.

In addition to the development of ICS capable malware, Dragos has observed threat groups increasingly leveraging strategic campaigns to enumerate and disrupt electric sector entities. Specifically, VOLTZITE (broadly known as Volt Typhoon) has targeted US-based electric companies with clear objectives to identify vulnerabilities within the country's critical infrastructure that can be exploited via destructive or disruptive cyberattacks. This group specifically aims to exploit the native functionality of control systems to achieve malicious objectives, a strategy referred to as "living off the land (LOTL)," to avoid detection. LOTL techniques were demonstrated during the 2015 cyberattack on Ukrainian electric distribution systems when ELECTRUM used legitimate commands to open circuit breakers via remote terminal units (RTUs). The ability to remotely open circuit breakers is critical to maintaining safe and reliable grid operations but can result in major power outages when used nefariously.

Additionally, VOLTZITE largely gains initial access by exploiting vulnerabilities in internet-facing VPN appliances or firewalls. This is particularly relevant to BESS systems, which routinely contain these elements. The US Cybersecurity and Infrastructure Security Administration (CISA) assesses with high confidence that VOLTZITE continues to develop and execute long term, strategic operations seeking to disrupt critical infrastructure and induce public panic via cyber means.[11] VOLTZITE is particularly concerning because of its objective to disrupt grid stability, capacity to exploit remote access solutions, and affiliation with the PRC (which manufactures many integrated systems that serve the global market.[12] While this group has been most active in North American infrastructure, it raises security concerns globally. Scanning activity of similar infrastructure has been seen worldwide and many joint advisories by security services globally have warned of the risks this group poses.

Testimony before the Congressional US-China Economic and Security Review Commission by Patrick Miller, CEO of Ampyx Cyber and one of the original contributors to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) security regulations for the electric power sector, notes that groups like Volt Typhoon have already demonstrated the ability to exploit vulnerabilities by maintaining persistent access to critical infrastructure while blending into normal network activity.[13] Additional testimony by Rob Joyce, former National Security Agency (NSA) Director of Cybersecurity, confirms that Chinese cyber operations now target control systems in power infrastructure with the strategic intent to cause disruption during a geopolitical crisis.[14]

While state-sponsored adversaries are particularly concerning to BESS asset owners, ransomware continues to impact organizations across industries. Ransomware compromises accounted for the majority of Dragos incident response cases impacting industrial organizations, with 25% resulting in a complete shutdown of operations and 75% causing at least some disruption to operations. While criminal groups have developed ICS-aware ransomware capable of terminating physical processes (e.g., EKANS), most incidents involve

[11] Harry Krejsa, “SUN SHIELD: How Clean Tech & America’s Energy Expansion Can Stop Chinese Cyber Threats,” Carnegie Mellon Institute for Strategy and Technology, January 2025, https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html.

[12] As noted in Section 1, manufactured components that are not digitally controllable are not the direct focus of the cyberattacks that are the focus of this white paper.

[13] US-China Economic and Security Review Commission, “Testimony of Patrick Miller Before the U.S.-China Economic and Security Review Commission,” April 2025, https://www.uscc.gov/sites/default/files/2025-04/Patrick_Miller_Testimony.pdf.

[14] Rob Joyce, “Testimony Before the House Select Committee on the Chinese Communist Party,” March 5, 2025, https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf.

traditional ransomware variants (e.g., LockBit, RansomHub, and Black Basta) compromising OT hosted on Microsoft Windows operating system-based assets.[15] Very recently, Nova Scotia Power was the target of a ransomware attack that resulted in the release of information on more than 200,000 of its customers.[16]

Additionally, organizations have become increasingly reliant on interdomain dataflows to drive business decisions and inform operational output. For instance, energy market, billing, and communications systems are typically hosted on enterprise or out-of-band (OOB) networks, yet have a direct impact on operational practices. Centralizing these technologies has increased organizational agility while decreasing capital and resource expenditures. However, the more exposed nature of enterprise and OOB networks has inadvertently increased risks to operations stemming from non-OT attacks. Asset owners should be aware of the risks associated with interdomain dependencies, as BESSs are particularly reliant on corporate and cloud infrastructure.

C. The Threats Posed by Foreign-Sourced Components

Many BESS assets rely on third-party systems and system components developed across a complex global supply chain that often includes equipment produced by FEOCs. According to the DOE, about 70% of PCSs approved for sale in California (the US's largest battery storage market) are from Chinese manufacturers, and only 4% are from US manufacturers.[17] In many cases, the contracts governing these components limit the ability of operators to inspect or monitor them. In the absence of policies to strengthen domestic manufacturing in Europe, the dependency on Chinese content and full integrated Chinese battery solutions is expected to be significantly higher in Europe. Even if a component is not sourced from a country with FEOCs, FEOCs may still exploit third parties to gain access. The SolarWinds hack (discussed further in the next subsection) is a prime example of how adversaries can infiltrate networks by compromising third-party vendors.[18] Therefore, strong cybersecurity controls and supply chain

[15] Dragos, Inc., "EKANS Ransomware and ICS Operations," The Dragos Blog, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[16] Nova Scotia Power customers handed 'to-do list' after ransomware attack | CBC News. Accessed May 28, 2025.

[17] US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Battery Energy Storage System Report*, November 1, 2024, https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf.

[18] Venminder Experts, *"SolarWinds Data Hack Is a Reminder Why Third-Party Risk Management Is Important,"* January 18, 2021, https://www.venminder.com/blog/solarwinds-hack-third-party-risk-importance.

risk management must be implemented regardless of component's country of origin. Additional controls should then be layered depending on the assessed risk.

This embedded software risk leaves asset owners with reduced visibility into who controls the code running on their infrastructure. In addition, developers and operators rely on OEMs for ongoing technical support, performance optimization, and firmware updates throughout the lifespan of BESS assets. Enabling access to these functions for some OEMs may open vectors for exploitation. This is particularly alarming, as vulnerabilities in these components can directly impact the security and functionality of the dependent products. While a vendor-manufactured product may be up to date with its own security patches, it could still include third-party components with unaddressed vulnerabilities. In such cases, the vendor might implement temporary mitigations to reduce the risk, but addressing the ultimate vulnerabilities in the components would largely depend on a third-party provided solution.

Evaluating BESS supply chain risks can be particularly challenging for BESS asset owners, as many system suppliers do not disclose which components are provided by third parties in an industry heavily influenced by FEOCs. For instance, battery management systems (BMSs) are directly connected to the BESS energy management system (EMS) and power conversion systems (PCSs). Collectively, these components manage the system's ability to charge and discharge in a safe and controlled manner. Despite this interdependent and critical function, manufacturers of these components (and sub-components) are often not disclosed to asset owners.[19] Without such disclosure, proactive mitigation measures such as those outlined in Section IV are not possible.

While software bill of materials (SBOM) and hardware bill of materials (HBOM) may alleviate some of these challenges, FEOCs often circumvent detection using proxy countries or companies for distribution.[20] This is typically facilitated by having significant assembly or manufacturing performed in a non-sanctioned country. In 2022, US Customs and Border Control found that China was transshipping several products containing printed circuit boards

[19] EPRI, *Insights from EPRI's Battery Energy Storage Systems (BESS) Failure Incident Database: Analysis of Failure Root Cause*, 2024 White Paper, May 2024, https://restservice.epri.com/publicdownload/000000003002030360/0/Product and US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Battery Energy Storage System Report*, November 1, 2024, https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf.

[20] US Department of Commerce, Department of Commerce Issues Final Determination of Circumvention Inquiries of Solar Cells and Modules from China, Press Release, August 18, 2023, https://www.commerce.gov/news/press-releases/2023/08/department-commerce-issues-final-determination-circumvention-inquiries.

(PCBs) through Mexico in order to qualify for preferential treatment under the United States-Mexico-Canada Agreement, thereby avoiding duties levied on Chinese PCBs under Section 301 of the Trade Act of 1974.[21] Similarly, the Russian and Iranian governments have historically sought to avoid sanctions by transferring oil via proxy countries.

D. Specific Pathways for Cyberattacks, and the Importance of the Supply Chain

Asset owners rely heavily on original equipment manufacturers (OEMs), vendors, and integrators for the acquisition, maintenance, and operation of critical systems and components. This means that organizations must understand contractual requirements and restrictions outlined in procurement documentation and service level agreements (SLAs) to scope and manage supply chain risk effectively.

Procurement documentation often requires third parties to attest that their technology meets certain technical specifications and was built using secure development practices. While this documentation is essential in managing legal and compliance risks, SLAs define roles and responsibilities related to maintaining and operating assets throughout their lifecycle. Unlike support contracts for traditional enterprise assets, SLAs commonly prevent asset owners from applying cybersecurity controls without the consent of relevant third parties. This practice aims to limit unintentional impacts to system functionality but often results in ambiguously defined or overly restrictive guidance for basic cybersecurity practice. For instance, vendors may reserve the right to approve and apply security patches that address known vulnerabilities.

This decision-making process relies on the vendor's approach to cybersecurity rather than that of the asset owner. A vendor's unwillingness to implement proper measures may therefore require the asset owner or operator to invest in additional mitigating security controls to reduce their risk to an acceptable level. Therefore, it is vital for owner operators to choose a vendor that will partner pro-actively in implementing 3rd party security controls for the full lifecycle of the asset as well as demonstrating ownership of the mitigations that rely on their ownership, such as software vulnerability resolution and obsolescence management.

While contractual requirements may indirectly impact an organization's cybersecurity posture, the implementation of commercially available hardware and software poses a more immediate

[21] US Department of Customs and Border Protection, Ruling H327583, November 15, 2022, https://rulings.cbp.gov/ruling/h327583.

concern. As previously noted, rogue communications devices were identified in Chinese manufactured solar power inverters and batteries. These devices were not disclosed in product documentation, including HBOMs. This discovery demonstrates that adversaries are actively exploiting challenges asset owners face when verifying the component list and functionality of procured technologies.

It is worth noting that power inverters do not typically store or transmit proprietary or sensitive information but are critical in maintaining reliable operations. This indicates that rogue communication devices were most likely installed to disrupt the ability of individual asset owners to generate solar power and possibly to attempt to initiate large-scale grid events. In addition to unauthorized system components, asset owners must consider risks associated with counterfeit hardware and software.

In 2024, a US citizen was sentenced to prison for trafficking fraudulent and counterfeit Cisco networking equipment. The operation involved installing pirated Cisco software and unauthorized system components – leveraged to circumvent standard methods of validating authenticity – on low-quality and outdated devices procured in China and Hong Kong. The modified devices were sold to industrial organizations, hospitals, and the US military. The consequences of these kinds of counterfeiting are more than just fraud; the product is unlikely to deliver the same capability and to be as safe. In many cases, counterfeit networking equipment was discovered to be such only when a user has attempted to address a vulnerability only to find the true vendor patch cannot be installed.

Adversaries have also increased supply chain attacks targeting widely deployed software. The Havex malware is a Remote Access Trojan (RAT) that communicates with a Command and Control (C2) server to establish persistent access within industrial environments. Unlike previous ICS malware, Havex was deployed using supply chain and watering hole attacks[22] that targeted over 2,000 ICS vendor websites. This resulted in asset owners unknowingly downloading the Havex malware[23] which subsequently scanned their industrial networks to identify connected assets in support of the adversary's reconnaissance efforts.

Similarly, the supply chain compromise campaign leveraging SolarWinds Orion software to distribute malware sought to gain access, move laterally, and steal data from victim

[22] A **watering hole attack** is a type of cyberattack in which threat actors compromise a legitimate website that is known to be frequented by a specific group or organization they are targeting. The goal is to infect visitors to the site with malware or collect sensitive information without arousing suspicion.

[23] Dragos, Inc., "The Evolution of Cyber Attacks on Electric Operations," Dragos Blog, https://www.dragos.com/blog/industry-news/the-evolution-of-cyber-attacks-on-electric-operations/.

environments.[24] The SolarWinds breach demonstrated an evolution in supply chain attacks by compromising the vendor's infrastructure to embed malware directly into legitimate software updates. This allowed the adversary to avoid common methods used to detect corrupted software packages, including hash validation.

E. Magnitude of Potential Harm

The consequences of a successful cyberattack on a grid-scale BESS can be both financially devastating and systemically disruptive. At the individual asset level, forced outages for maintenance or cybersecurity remediation can lead to significant revenue losses. Using the US ERCOT system as an example, we estimate that these losses could range from $400,000 to $1.2 million per month for a single 100 MW (4-hour duration, 400 MWh) battery system. Similar magnitudes of revenue loss could be expected in European markets such as Great Britain, Germany, Italy, or Poland. These losses, while substantial, are modest compared to the capital losses that could result from permanent damage to a BESS asset due to malicious cyber-induced failures, which could be over an order of magnitude greater.[25]

More critically, cyberattacks on BESS resources can pose systemic risks to the grid and result in widespread societal harm. Disruptive actions, such as the injection of harmful harmonics or the misuse of inverter controls, could trigger local or regional outages. In ERCOT, the average "value of lost load" (a proxy for the costs and impacts experienced by customers due to an outage) during a 16-hour outage exceeds $13,000 per MWh.[26] A scenario in which 100,000 customers lose access to 3,000 MWh of electricity during such an event would result in an estimated $39 million in economic losses within a single day.

These risks are magnified by current supply chain constraints. Many critical components, including inverters, BMSs, and control chips, are sourced internationally, often from

[24] Ben Miller, "Responding to the SolarWinds Software Compromise in Industrial Environments," Dragos Blog, https://www.dragos.com/blog/industry-news/responding-to-solarwinds-compromise-in-industrial-environments/.

[25] To manage the financial risk taken on by ODOMs, at least one insurance company has begun writing policies specific the BESS cyber risks. Kenneth Araullo, "McGill and Partners launch cyber coverage for battery energy storage systems; New product addresses physical damage, business interruption, and regulatory risks," Renaissance News, June 18, 2025, https://www.insurancebusinessmag.com/reinsurance/news/breaking-news/mcgill-and-partners-launch-cyber-coverage-for-battery-energy-storage-systems-539549.aspx.

[26] Charles Gibbons, Sanem Sergici, with support from PlanBeyond, *Value of Lost Load Study for the ERCOT Region,* Final Report, Before the Public Utility Commission of Texas, August 19, 2024, https://www.brattle.com/wp-content/uploads/2024/09/Value-of-Lost-Load-Study-for-the-ERCOT-Region.pdf.

geopolitically sensitive regions. Should a cyberattack render key components inoperable, restoring service may be significantly delayed. Lead times for certain components, including transformers, have stretched from typical 12-month cycles to as long as 32 to 36 months in some cases. These supply constraints can significantly extend outage durations, increasing both financial losses and reliability concerns.

Finally, the risks posed if there is a successful cyberattack on BESSs that triggers larger regional grid problems could rise to become broad threats to energy and national security. The importance of grid reliability to national security is well understood, though often underestimated. Reliable electricity supplies are essential to every military and defense function, from basic logistics and communications to advanced digital warfare. More generally, the broad-scale targeting of power grids and other critical infrastructures has become an element of modern warfare. Foreign adversaries successfully targeted Ukraine's power grid in 2015 and 2016, and Israel's water system in 2020, along with many other intrusions into power grids, with security implications that have gone unreported.[27,28]

In addition to attacks that disable power directly to the military, large power outages cause enormous economic damage, weaken civil society, and reduce a country's overall ability to respond to external threats. In response to the Reuters report that US experts had found unexpected communication devices inside PRC-sourced inverters, former National Security Agency Director Mike Rogers said:

> *"We know that China believes there is value in placing at least some elements of our core infrastructure at risk of destruction or disruption. I think that the Chinese are, in part, hoping that the widespread use of inverters limits the options that the West has to deal with the security issue."*[29]

Beyond their immediate security implications, large-scale blackouts also take a large economic and social toll. The 2025 Iberian Peninsula blackout, although explicitly not tied to actual or potential cybersecurity, provides a jarring example of the severe impact that a major blackout

[27] SMPnet | From Grid to Nation: The Convergence of Cybersecurity, National Security, and Power Grids.

[28] Earlier this year the three Baltic states, after a yearlong preparation and investments of around 1.5 bn (Baltic States' synchronization with the continental grid | DIIS) severed their connection to the Russian grid and connected to the continental European grid, strengthening their energy security and reducing dependence on Russia for the operation of their power system.

[29] Rogue communication devices found in Chinese solar power inverters | Reuters.

could have on safety and the economy. This 9-hour blackout of Spain and Portugal was estimated to cost between €2.25 and €4.5 billion, [30] stranded 35,000 transit passengers, and led to at least five deaths.[31]

III. Emerging Trends in the US and Europe

As part of the research for this paper, the Brattle/Dragos team interviewed 9 leading industry experts and former federal officials on emerging trends in cybersecurity policies, regulations, and standards applicable to large-scale batteries. To ensure candid reflections, these interviews took place under Chatham House rules, so no observations in this section are attributable to any individual panelist. The panelists included two cybersecurity directors at two leading large-scale storage manufacturers, two former senior federal cybersecurity officials, US national lab experts, and others.

The experts broadly agreed that increased supply chain scrutiny is necessary and that the current system of voluntary standards is likely not adequate to ensure BESS cybersecurity within a secure power system. None of the experts interviewed foresaw a cost-effective outcome that would involve completely onshoring the supply chain. However, multiple experts from both industry and government were supportive of policies that would disallow the use of sensitive components manufactured by countries of concern or effectively isolate those components from threat actors.

The interviewees were not in agreement on the likely mechanisms by which such policies would be implemented but outlined several possible legislative and regulatory paths that could be implemented at either the federal or state levels.

[30] Spain, Portugal switch back on, seek answers after biggest ever blackout | Reuters, 4.29.25.

[31] Spain and Portugal investigate cause of huge power blackout | AP News.

A. The United States

1. Growing Distrust of Foreign Entities of Concern (FEOCs)

Amid escalating concerns over national security, there has been a notable increase in scrutiny of technology and communications assets sourced from Foreign Entities of Concern (FEOCs).[32]

During the first Trump administration, these concerns led to sweeping policy measures aimed at limiting the influence of Chinese technology suppliers in critical infrastructure. In 2019, the addition of Huawei and other Chinese firms to the Department of Commerce's Entity List signaled an effort to restrict the integration of foreign-sourced digital and communications technologies.[33] Executive Order 13920, issued in May 2020, prohibited federal agencies and utilities from acquiring equipment from foreign adversaries that posed risks to the security of the bulk power system.[34]

The Biden administration largely maintained and expanded this posture of caution toward FEOCs, reinforcing efforts to secure critical energy infrastructure against cyber and supply chain threats. Executive Order 14017, issued in February 2021, launched a comprehensive review of supply chains for key sectors, including energy storage, with a focus on reducing dependence on adversarial nations.[35] This agenda was further bolstered by the CHIPS and Science Act of 2022, which directed substantial investment toward reshoring semiconductor manufacturing and strengthening domestic production of advanced technologies critical to clean energy systems, including BESS control components.[36] In parallel, the Department of Energy and the Cybersecurity and Infrastructure Security Agency (CISA) promoted "secure by design" principles for industrial control systems, encouraging vendors and operators to prioritize cybersecurity

[32] As an example, in May 2025, a group of 17 GOP lawmakers signed an open letter urging the Commerce Department to ban the sale of TP-Link routers, which are manufactured in China and have been identified as facilitating cyberattacks in the US. https://www.cotton.senate.gov/imo/media/doc/tplinkfinal.pdf.

[33] US Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities to the Entity List (Final Rule)," May 16, 2019, https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019.

[34] J. Scott Maberry, et al., "Securing the U.S. Bulk Power System: An Assessment of Executive Order 13920," May 8, 2020, https://www.energylawinfo.com/2020/05/bulk-power-system/#more-2042.

[35] Joseph R. Biden Jr., "Executive Order 14017—America's Supply Chains," February 24, 2021, https://www.presidency.ucsb.edu/documents/executive-order-14017-americas-supply-chains.

[36] US Congress, "Telecommunications Security Fund," in H.R. 4346—117th Congress (2021–2022): CHIPS and Science Act, https://www.congress.gov/bill/117th-congress/house-bill/4346.

features from the outset rather than as afterthoughts.[37] Together, these measures intensified pressure on developers and utilities to scrutinize their sourcing and integration practices.

The Biden administration even took steps to prohibit connected technology procurement from certain countries when the Bureau of Industry and Security (BIS) issued a final rule in January 2025 that restricted the import or sale of Chinese and Russian connected vehicle technologies (and completed vehicles that included those technologies). According to the BIS, it "determined these transactions pose national security risks, as companies from these countries may be compelled to share data or allow remote access to connected vehicles in the United States." [38] While that final rule is not directly relevant to battery storage, President Trump's America First Trade Policy memorandum directed the Department of Commerce to determine if these controls should be expanded to account for additional connected products.[39]

The experts we interviewed broadly agreed that a heightened security posture toward China is a necessary and prudent response to the evolving geopolitical and cybersecurity landscape. They emphasized that, given the critical role of BESS assets in grid stability and decarbonization goals, safeguarding these systems from potential foreign interference is essential. Looking ahead, many expect that the Trump administration, Congress, and some states will pursue additional policies aimed at further restricting the procurement of BESS software, control systems, and related smart technologies from Chinese entities. While the precise mechanisms and scope of these future actions remain uncertain, there is a shared expectation that the policy environment will continue to prioritize supply chain security and reduce reliance on adversarial component sources in the energy sector.

2. Changing Federal Role in Cybersecurity Space

Protecting the electric grid or other critical infrastructure from state-sponsored cybersecurity threat actors is one of few areas that enjoys enduring bipartisan support in US politics. As long ago as 2013, the US Federal Energy Regulatory Commission approved the first Critical Infrastructure Protection Standards promulgated by the North American Electric Reliability Council (NERC). While tariffs and trade restrictions have been used to address supply chain

[37] Cybersecurity and Infrastructure Security Agency, "Secure-by-Design," October 25, 2023, https://www.cisa.gov/resources-tools/resources/secure-by-design.

[38] One recent example of this type of restriction is the rule announced on Jan. 14, 2025 restricting information-connected vehicles manufactured in Russia and China. See, bis.gov/node/22645#:~:text=Overview,Authorizations for low-risk transactions.

[39] America First Trade Policy – The White House.

dependencies on adversarial nations, these measures do not directly address software, firmware, or hardware vulnerabilities embedded deep within BESS supply chains. For this reason, other policies are under consideration and have been enacted to address these specific risks directly.

Presidents Trump and Biden both signed Executive Orders[40] to bolster the security of critical infrastructure and their administrations published regulations[41] designed to protect Americans from the impact of foreign technologies. In Congress, several bills, including the "Decoupling from Foreign Adversarial Battery Dependence Act," and "The Federal Contractor Cybersecurity Vulnerability Reduction Act," aim to address cybersecurity vulnerabilities for entities that serve US military or other federal facilities. Members of Congress from both the Republican and Democratic parties have also sought to restrict the PRC or PRC-aligned entities from benefitting

[40] White House, *"Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"* May 2017, https://www.govinfo.gov/content/pkg/DCPD-201700317/pdf/DCPD-201700317.pdf,

White House, *"Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain,"* May 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain,

White House, *"Executive Order 13920: Securing the United States Bulk-Power System,"* May 2020, https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system,

White House, *"Executive Order 14028: Improving the Nation's Cybersecurity,"* May 2021, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity ,

White House, *"Executive Order 14017: America's Supply Chains,"* February 2021, https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains, and

White House, *"Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity,"* January 2025, https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity.

[41] Internal Revenue Service and Treasury, "Final Regulations: Sections 25E and 30D (Clean Vehicle Credit), including FEOC restrictions," May 6, 2024, https://www.federalregister.gov/documents/2024/05/06/2024-09094/clean-vehicle-credits-under-sections-25e-and-30d-transfer-of-credits-critical-minerals-and-battery,

Bureau of Industry and Security, *"Final Rule: Securing the Information and Communications Technology and Services Supply Chain—Connected Vehicles,"* January 14, 2025, https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats and

Biden, "State and Local Government Cybersecurity Act of 2021", https://flashpoint.io/blog/biden-signs-two-cyber-bills-into-law,
Trump, *"Secure and Trusted Communications Networks Act of 2019,"* March 12, 2020, https://www.congress.gov/bill/116th-congress/house-bill/4998,

and Trump, *"NIST Small Business Cybersecurity Act,"* August 15, 2018, https://www.sbc.senate.gov/public/index.cfm/2018/8/president-trump-signs-risch-s-small-business-cybersecurity-legislation-into-law.

from federal tax credits for energy deployment and manufacturing[42], most recently with the wide-ranging FEOC sourcing restrictions included in the One Big Beautiful Bill Act. NERC is continuing to develop added cyber protection standards, such as the rules implementing FERC Order 901 for inverter-based resources.[43] In addition, US national laboratories have conducted substantial cybersecurity research and published guidelines such as the Idaho National Labs' digital infrastructure guidance.[44]

3. States Stepping Up as Cybersecurity Regulators

In addition to federal actions, state governments are increasingly stepping into the cybersecurity field with their own regulatory and institutional innovations. California has played one of the leading roles with legislation such as AB 2813, which created the California Cybersecurity Integration Center (Cal-CSIC) to monitor, analyze, and coordinate cyber threat responses across the state's agencies and critical infrastructure sectors.[45] Texas has followed suit with SB 475, which established the Electric Grid Security Council. This council provides cybersecurity guidance to the energy industry, supports educational programs, and works directly with utility stakeholders to reduce physical and cyber risks.[46]

States are also leveraging legislative tools to curtail foreign influence and improve procurement standards. Texas's Lone Star Infrastructure Protection Act explicitly prohibits businesses and government entities from entering into agreements that grant FEOCs direct or remote access to critical infrastructure.[47] Texas has also established the "Texas Cyber Command", funded with

[42] John R. Moolenaar, "NO GOTION Act," November 2, 2023, https://www.congress.gov/bill/118th-congress/house-bill/6175,

Carol D. Miller, "End Chinese Dominance of Electric Vehicles in America Act," April 15, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7980,

Sherrod Brown et al., "American Tax Dollars for American Solar Manufacturing Act," July 31, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/4873 and

Nancy Mace, "Federal Cybersecurity Vulnerability Reduction Act," August 22, 2023, https://www.congress.gov/bill/118th-congress/house-bill/5255.

[43] See North American Reliability Council, Reliability Standards Under Development, June 23, 2024.

[44] Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance. October 2024.

[45] California State Assembly, "AB 2813 – Government Investment Act," April 18, 2018, https://agov.assembly.ca.gov/sites/agov.assembly.ca.gov/files/AB%202813.pdf.

[46] Texas Senate, "SB 475 – Relating to an advisory body on the security of the electric grid ," March 27, 2019, https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00475S.htm.

[47] Texas Senate, "SB 2116: Relating to prohibiting contracts or other agreements with certain foreign-owned companies in connection with critical infrastructure in this state," 87th Legislature, Regular Session, April 1, 2021, https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SB02116I.pdf.

$135M through 2027 to centralize threat intelligence, incident response, and digital forensics.[48] Arizona also has a "Cyber Command", established in 2021 as part of the Arizona Department of Homeland Security.[49] Through Arizona's HB 2736, they have also proposed establishing a seven-year data encryption and cybersecurity pilot program.[50] Georgia's SB 346 takes a similar approach by preventing Chinese-owned or affiliated companies from bidding on state contracts.[51] Meanwhile, national advocacy groups like the American Legislative Exchange Council (ALEC) are promoting model policies that prohibit the use of state funds to purchase technology from providers linked to adversarial foreign governments.[52]

In parallel, several states are exploring forward-looking procurement rules aimed at addressing future vulnerabilities. These include potentially augmenting NERC Critical Infrastructure Protection (CIP) standards to apply to smaller BESS installations and the incorporation of standards such as UL 2941 at the component level. Still, these efforts face a structural challenge: implementing rules for future systems without acknowledging vulnerabilities in currently deployed assets can limit the practical impact of these policies.[53]

4. The Expanding Role of Industry and Voluntary Standards

Amid this fragmented regulatory environment, the private sector and industry-led initiatives are taking a more prominent role in defining cybersecurity expectations. There is growing demand for independent, third-party assurance of cybersecurity practices, including deeper examinations of hardware and software bills of materials (HBOM/SBOM). By probing more

[48] Texas Legislature, *"House Bill 150: Relating to the Creation of the Texas Cybersecurity Command,"* enrolled June 2025, https://legiscan.com/TX/bill/HB150/2025.

[49] Arizona Department of Homeland Security, "Cyber Command," July, 2021, https://azdohs.gov/cyber.

[50] Arizona Legislature, "HB 2736: Relating to Cybersecurity and Data Encryption Pilot Program," 57th Legislature, 1st Regular Session, 2025, https://legiscan.com/AZ/text/HB2736/2025.

[51] Georgia Senate, "SB 346: Relating to prohibiting companies owned or operated by China from bidding on or submitting proposals for state contracts," 2021–2022 Regular Session, March 2, 2021, https://www.legis.ga.gov/api/legislation/document/20212022/203470.

[52] American Legislative Exchange Council, "An Act Restraining State and Local Governmental Use of Mobile or Online Software Applications and Electronic Devices Under Control of a Foreign Adversary," December 31, 2024, https://alec.org/model-policy/an-act-restraining-state-and-local-governmental-use-of-mobile-or-online-software-applications-and-electronic-devices-under-control-of-a-foreign-adversary/.

[53] The effectiveness of these regulations may depend on the structure of utility markets. All segments of vertically integrated utilities are primarily overseen by state public utility commissions (PUCs), while the distribution portion of utilities in restructured states remains subject to PUC regulation but other portions of the states' power systems must navigate oversight and coordination through Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs). However, all portions of the industry operating at bulk power levels are subject to certain federal requirements such as the Critical Infrastructure Protection (CIP) standards.

deeply into the origins and structure of their supply chains, companies aim to mitigate risks and demonstrate trustworthiness in a competitive market. For example, many utility tenders now include requirements for cybersecurity protection in both private and state-owned procedures, including during the procurement process.

Nonetheless, congressional testimony from both Idaho National Lab's Emma Stewart and Cybersecurity executive Patrick Miller emphasized the need to move beyond voluntary frameworks toward more structured deployment of secure-by-design principles.[54] Stewart has advocated for prescriptive standards that include pre-operational inspection, firmware verification, and contractual transparency as baseline requirements. Both she and Joyce have argued that industry standards alone or individual company bans will not deter highly capable threat actors with state backing. Prescriptive cybersecurity standards have the potential to level the playing field by ensuring that all stakeholders, regardless of market size or geography, meet a minimum threshold of security. [55]

There may be value in offering incentives to battery owners who exceed minimum cybersecurity standards.[56] This approach parallels the treatment of cybersecurity investments by regulated distribution utilities, which, as of 2024, are allowed to rate base such expenses, effectively enabling them to increase profits through these investments. In contrast, merchant generators, including battery owners, do not operate under the same regulated return structures, leading them to view cybersecurity primarily as a cost center rather than a value-generating asset. Recognizing this disparity, the National Security Telecommunications Advisory Committee (NSTAC) issued a report in March 2024 recommending the use of financial incentives, such as tax deductions and grants, to help close the gap between basic compliance and the level of cybersecurity required to address national security risks effectively.[57] These incentives could be modeled on successful precedents, such as the investment tax credit (ITC) for solar energy or the Leadership in Energy and Environmental Design (LEED) tax credit for green buildings.

[54] See footnote 7 above and the testimony of Patrick C. Miller, CEO of Ampyx Cyber, U.S.-China Economic and Security Review Commission, April 24, 2025.

[55] Raising the minimum standard for BESS cybersecurity may have the added benefit of simplifying financing for projects by reducing perceived risk and creating clearer expectations for investors and insurers.

[56] Enhancing cyber resilience in electricity systems – Analysis - IEA.

[57] NSTAC Report to The President.

B. Europe

1. The Role of EU-Wide Directives in Energy Cybersecurity

In contrast to the United States, where federalism and ideological resistance to centralized regulation often complicate national policy implementation, the European Union has taken a more unified, if not always cohesive, approach to cybersecurity governance. The European regulatory environment is structured around EU-wide directives and regulations that require member states to transpose and enforce rules domestically. While this framework theoretically offers a coordinated path to continent-wide cybersecurity for energy infrastructure, in practice, national differences in implementation, enforcement, and foreign policy orientations introduce significant fragmentation.

At the core of the EU's cybersecurity framework is the Network and Information Security (NIS) directive, recently updated and expanded as NIS2, and the newer EU Cyber Resilience Act. The NIS directives represent the EU's effort to improve cyber resilience across critical infrastructure sectors, including energy. Unlike prescriptive regulatory regimes such as NERC CIP in the US, the NIS and NIS2 directives emphasize a risk-based approach with limited direct government oversight. [58] Owners and operators of critical infrastructure – including utility-scale battery storage systems – are required to assess threats, take appropriate mitigation steps, and demonstrate that their controls are "defendable" in the event of a breach. The burden of risk management, and its legal consequences, rests squarely on the asset owner, with limited direct government oversight.

NIS2 significantly expands the scope of cybersecurity obligations. Where NIS applied only to systems above a certain size threshold (typically 2 GW), NIS2 brings smaller systems and a broader range of digital infrastructure into its purview.[59] This reflects the EU's recognition that even modestly sized systems, when integrated into an interconnected grid, can pose substantial risks. As implementation proceeds across EU member states, energy asset owners must navigate national variations in how these risk-based mandates are interpreted and enforced.

The Cyber Resilience Act (CRA) of 2024 is a new EU-wide law that requires member nations to create cyber surveillance authorities for all EU manufacturers of products with digital elements

[58] International Cyber Threat Task Force, "What do you need to know about NIS2?" September 30, 2024, https://www.int-comp.org/insight/what-do-you-need-to-know-about-nis2/.

[59] Infosecurity Magazine, "NIS2 Directive: Everything EU Organizations Need to Know," November 14, 2024, https://www.infosecurity-magazine.com/blogs/nis2-everything-eu-orgs-need-to/.

(hardware or software), certify that every product offered for sale in the EU meets cyber protection standards, and that manufacturers take responsibility for protection over the full product life cycle.

The CRA, which goes into full effect in 2027, will apply to the full stack of manufacturers and vendors of BESS equipment throughout the EU.[60] In addition to this law, the EU Energy directorate has also announced a specific review of cybersecurity risks in the solar value chain, which will necessarily include components routinely included in BESSs.[61] Finally, the EU has initiated a consultation to update its 2019 EU Cybersecurity Act. This consultation is intended to update the mandate of the EU cybersecurity agency and improve and streamline cybersecurity certification processes, among other goals.[62]

2. Challenges of Harmonization Across a Fragmented Policy Landscape

Despite the ambition of EU-wide regulation, achieving consistent cybersecurity outcomes across the continent remains a formidable challenge. Member states differ sharply in their strategic orientations and willingness to disentangle their energy sectors from foreign dependencies, particularly with regard to Chinese suppliers. Hungary, for example, has maintained close ties to China and has resisted efforts to sever digital infrastructure partnerships.[63] Conversely, Lithuania has implemented a ban on Chinese communication access to its wind and solar infrastructure, reflecting a broader European concern about foreign control of critical systems.[64] In Germany, regulatory mandates that required solar “clipping” (a form of generation curtailment) sparked fears that Chinese OEMs could exert direct influence

[60] See Cyber Resilience Act | Shaping Europe’s digital future.

[61] The inquiry is announced in this speech by EU Energy Commissioner Dan Jorgenson on March 26, 2025. See SolarPower Summit.

[62] See Commission opens consultation on revising EU Cybersecurity Act | Shaping Europe’s digital future April 11, 2025.

[63] South China Morning Post, “China scouts Hungary to power battery production and sell to wider, warier EU,” May 10, 2024, https://www.scmp.com/economy/china-economy/article/3262232/china-scouts-hungary-power-ev-battery-production-and-sell-wider-warier-eu.

[64] ESS News, “Lithuania bans Chinese remote access to energy storage, solar, wind devices,” November 20, 2024, https://www.ess-news.com/2024/11/20/lithuania-bans-chinese-remote-access-to-energy-storage-solar-wind-devices/.

over domestic distributed energy resources by improperly triggering this "clipping" when it would be harmful to the system.[65]

These divergent national approaches create a dangerous mismatch. The EU power grid is deeply interdependent, meaning that the effects of cybersecurity vulnerabilities in one member state can cascade across borders. As such, inconsistent national cybersecurity policies create system-wide exposure. The European Commission has acknowledged this challenge and is placing increasing emphasis on harmonization.[66] However, the complex, multi-layered nature of EU policymaking (where regulations must be proposed, negotiated, and then translated into national law) impedes rapid and consistent policy implementation.

3. Industrial Policy, Chinese Influence, and US Pressure

European policymakers are attempting to integrate cybersecurity into broader economic and industrial strategies. The Net Zero Industry Act, for instance, positions cybersecurity not just as a defensive priority, but as an enabler of clean energy manufacturing and digital infrastructure deployment. However, Europe's deep reliance on Chinese-made components and software remains a significant concern, particularly in grid infrastructure and energy storage systems.[67] This dependency is under growing scrutiny – not just from within the EU but also from US officials, who are pressuring allied nations to limit procurement from Chinese vendors and align with transatlantic supply chain security priorities.

Despite these pressures, the EU's regulatory response remains uneven. While NIS2 and related initiatives establish a common floor for cybersecurity practices, the lack of detailed, enforceable technical controls leaves substantial discretion to individual member states and operators. This patchwork approach stands in stark contrast to the EU's approach to cyber-protection of EU 5G networks, which was a relatively unified approach,[68] as well as to jurisdictions like Australia,

[65] Clean Energy Wire, "Solar PV hardware opens door to Chinese interference in German power supply – security agency," January 20, 2025, https://www.cleanenergywire.org/news/solar-pv-hardware-opens-door-chinese-interference-german-power-supply-security-agency.

[66] European Commission, "A Competitiveness Compass for the EU," COM(2025) 30 final, January 29, 2025, https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en.

[67] In 2023, components from China made up about one-third of the EU's imports of low-voltage boards and panels, which includes programmable logic controllers.

[68] Shoring cybersecurity safeguards in BESS and the wider energy sector could build on previous experience around 5G cybersecurity. Recognizing the importance of cybersecurity for 5G networks, the European Commission in 2019 initiated a coordinated approach to address security risks, supported by the European Council and ENISA. EU Member States conducted national risk assessments, culminating in the EU Coordinated

Continued on next page

where frameworks such as the Australian Energy Sector Cybersecurity Framework (AESCF) provide more centralized guidance.[69]

Risk Assessment report. This identified key threats, vulnerabilities, and risks, including those posed by high-risk suppliers. The EU's resulting 5G cybersecurity toolbox highlighted the need to mitigate risks associated with supplier dependency, state interference, and software vulnerabilities. This underscores the importance of reassessing policies and implementing robust measures to ensure the security, integrity, and technological sovereignty of 5G networks across the EU. See European Commission, *"Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures,"* European Commission Digital Strategy, 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[69] Australian Energy Market Operator (AEMO), "AESCSF Framework and Resources," 2025, https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.

IV. Steps that Owners, Developers, Operators, and Maintainers Can Take to Reduce Risk

By taking a proactive approach to cybersecurity, asset owners and operators have the opportunity to reduce risk while also saving time and money. Addressing well-understood threats during the design and construction phases allows firms to implement effective controls with greater efficiency and lower cost. Although new threats will continue to emerge, requiring flexibility and ongoing adaptation, many proven solutions are already available and can be integrated early to avoid the higher complexity and expense of retroactive fixes. The following sections highlight several specific measures ODOMs can take now to improve system security.

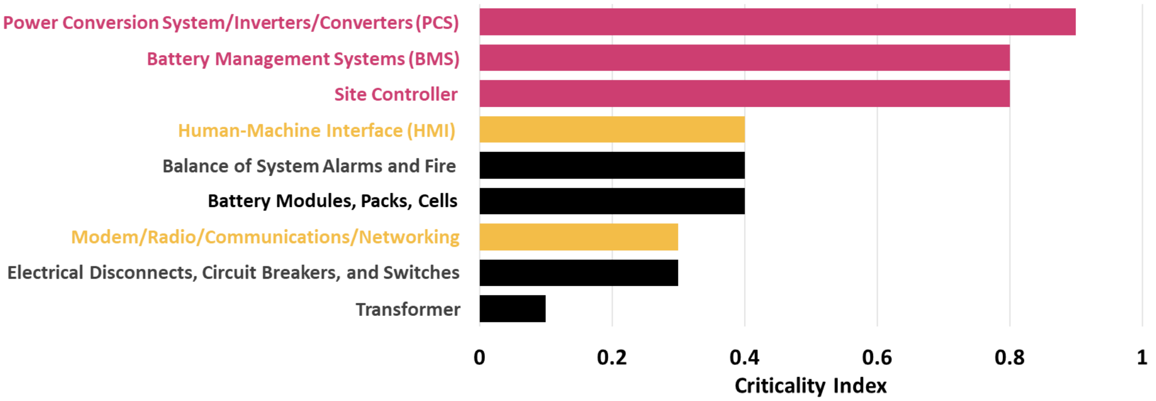
A. HBOMs and SBOMs

Effective cybersecurity risk management in BESS requires a component-level understanding of operational criticality and network exposure. SBOM and HBOM analyses provide the visibility needed to assess and mitigate risks tied to functionality, communications pathways, and integration with broader energy infrastructure. At a minimum, an assessment of any digital component that can affect the reliability or integrity of the system should be part of SBOM and HBOM analyses. Mechanical and purely electrical components would not require this level of scrutiny when addressing cyber risks, but similar approaches may be required to ensure the quality of components.

The US Idaho National Laboratory evaluated BESS components for their cyber-physical consequence potential and assessed that the PCS, BMS, and EMS must be top priorities for SBOM and HBOM review due to their central role in safe and secure energy flow. Figure 4 below, adapted from the Idaho National Laboratory, demonstrates the essential nature of smart components like inverters, BMS, and PCS and the need to evaluate their cybersecurity risks.[70]

[70] Idaho National Laboratory, "BESSIE: Battery & Energy Storage Supply Chain Analysis, Mitigation Deployment, and Tools," March 2024, https://inl.gov/content/uploads/2024/03/BESSIE_supply-chain-battery-report.pdf.

FIGURE 4. CRITICALITY OF BESS COMPONENTS TO CYBER, PHYSICAL, AND SAFETY CONSEQUENCE OUTCOMES



Source: Idaho National Laboratory, "BESSIE: Battery & Energy Storage Supply Chain Analysis, Mitigation Deployment, and Tools," March 2024, https://inl.gov/content/uploads/2024/03/BESSIE_supply-chain-battery-report.pdf.

Note: INL analysts applied a "Cyber-Informed, Consequence-Driven Engineering" approach to develop total consequence scores across the listed BESS components by utilizing cyber and physical impacts from component malfunction. Components are colored in consistency with Figures 2 and 3, showing high levels of criticality in burgundy, medium levels of criticality in yellow, and low levels of criticality in black. Due to the INL's addition of physical impacts in evaluating criticality in Figure 4, components "Battery Modules, Packs and Cells" and "Balance of System Alarms and Fire" have a slightly higher criticality than components in yellow.

To manage the issues that may arise from software subcomponents, one must first know what these components are. A software bill of materials is the best way to demonstrate the full inventory. The SBOM should be built during development and should include a complete listing of all third-party applications, libraries, SDKs, and binaries. ODOMs can use SBOMs to run automated scans to identify known CVEs in software components to reduce cyber risk from exploitable software vulnerabilities and check to see if third-party components come from trustworthy sources. Tooling for the retrospective creation of SBOM can also be used to validate the declared content in the vendor-provided SBOM, ensuring further integrity of the supply chain.

Verifying the build of assets at a component level is complicated. This is especially the case when equipment can pass through multiple hands before the asset moves into the custody and management of the owner. Attempting to verify the build of every component is extremely complex. Therefore, establishing trust and second line controls to verify is critical. The vendor should be able to demonstrate a detailed hardware bill of materials and software bill of materials and demonstrate the controls they have in place to verify that what is delivered matches. This can reduce the risk of counterfeit parts or hardware trojans.

Asset owners should leverage HBOMs and SBOMs to verify that all components are produced by trusted third parties and that procured hardware and software meet defined functional and security requirements. Additionally, SBOMs can be leveraged to identify potentially unnecessary software packages that may inadvertently increase a BESS attack surface. Asset owners should identify SBOMs for atypical or uncommon software packages and coordinate with their vendors or integrators to determine their necessity. At a minimum, an assessment of any digital component that can affect the reliability or integrity of the system should be part of these assessments and should all be included in the HBOM.

Counterfeiting of industrial equipment has been a significant issue that proper HBOM and SBOM processes should prevent. Fake, substandard equipment masquerading as having been made by Cisco and Yokogawa are prime examples of how counterfeiting can take place and result in low quality or vulnerable assets ending up in critical facilities. Establishing trust in all vendors and sub-vendors is vital to ensure the authentic sourcing of all items.

A mature BESS manufacturer will understand the potential challenges associated with different countries of origin and look to manage these risks by sourcing higher risk subcomponents from safe countries and trusted, auditable, suppliers. This is particularly the case for the cyber elements of a system.

B. Defensible Architecture

Connectivity into BESS environments is critical, and each BESS will have some standard requirements and some specific to its implementation. It is most likely that the OEM and customers will both want remote access and at least one party will require some operational control over the asset. While monitoring an asset is important, the loss of condition monitoring should not affect the safe operation of the system. It is also important to design a BESS system so that, should operational communications be lost, it remains in a safe state.

Adversaries will use remote communication in several ways. Adversaries often attempt to exploit remote connectivity to gain access to and impact target systems. Therefore, asset owners must be aware of all methods of accessing BESS and connected systems and have the capability to establish segmentation within operational environments. Implementing robust, maintained, and monitored firewalls is a critical element for developing a properly segmented environment, which can impede an adversary’s ability to access or pivot within critical networks.

Communications within any BESS are vital to ensure that all components work well together: remote monitoring is critical to manage the asset and remote control allows the system to deliver or consume energy on demand. However, many battery storage system providers oversimplify the architecture, leaving networks with “flat” sites, whereby all assets within a network can communicate with each other directly regardless of their function. This can mean that a single vulnerability or misconfiguration can expose all equipment to attack. Internal segmentation and zoning of assets can slow the progress of even the most determined adversary should the perimeter be breached and prevent operational impacts.

Defining the perimeter itself is vital, and as a primary control should be tightly managed and monitored. Any credentials used to access this perimeter should be regularly updated and audited, as this is a route commonly used by determined attackers to gain access. Any party accessing the OT networks should be constrained by additional controls to limit their activities to the specific needs of their role. Recognizing that some roles require a privileged level of access, there will always be need for further controls and visibility. Threat actors, whether determined criminals or malicious insiders, can use the highest level of privilege to move within the systems as designed. This makes monitoring of all network traffic for threats and behaviors critical.

C. Secure Remote Access (SRA)

Given the previously described need, remote access is unavoidable, and with the vulnerable and critical nature of assets, SRA should be a priority. Threat actors look to use and exploit these routes, so solutions such as session-based VPN should be avoided. Robust role-based access control and control of the capabilities available to the user should be limited to their operational need. Activities should be logged and access levels reviewed. There should be no shared account usage, and the use of Multi-Factor Authentication (MFA) should be used to prevent sharing. The use of dedicated engineering workstations can provide a further layer of defense when using remote access.

D. Network Visibility and Monitoring

Given the way adversaries operate with controls (living off the land), it is important to monitor the communications within operational systems. This includes the operational communications between assets as well as those between zones. The BESS vendors should provide the ability for customers to implement this kind of monitoring by default using their own tooling or provide it as a component.

E. Software Maintenance and Support

Contractual commitments for software support can be difficult to sustain over the lifespan of a long-lived asset such as a BESS connected to the electrical power grid. A BESS with a 20-year life may contain components that become obsolete well before the end of the asset's life, especially given the shorter IT lifecycle in which elements such as PCs lose vendor support only a few years after deployment. To maintain security integrity throughout the asset's life, asset owners must ensure that all parties in the supply chain establish and adhere to appropriate contractual arrangements that define patching responsibilities, address obsolescence, and specify how potential cyber risks will be managed.

ODOMs should look for demonstrable engagement from their technology supplier in managing declared issues through ethical disclosure processes for managing vulnerabilities, especially in cases that demonstrate the support of vulnerabilities in older assets. ODOMs should evaluate suppliers' previous experience providing long-term maintenance to BESS assets, the extent to which they leverage local and/or in-house service teams, and their familiarity with the software and controls used in the BESS.

When considering a BESS solution and reviewing the cybersecurity controls and mitigations, ODOMs should look to vendors that manage the integration of all major software solutions; not rely on a chain of third-party vendors. This gives them full control of the software management lifecycle, ensuring a full understanding of the software bill of materials, and greater ownership of long-term software maintenance and updates.

F. Proactive Measures vs. Retrospective Measures

When adopting the measures chronicled above, it is important to keep in mind that proactive management of cybersecurity risks is preferable to after-the-fact fixes. The cost of retrofitting security capabilities is often two-to-three times more expensive than implementation during the initial build or having the capabilities built into the product. As an example, enabling network changes for visibility can have little or no cost if they are part of an initial design and configuration. In contrast, retrofit network modifications can cost $10,000–100,000 per location just to enable visibility. Adding network segmentation or next-generation firewalls can further increase this cost.

There have been a number of cases of extraordinary expense based on policy change. For example, in the UK, large telecommunications companies have begun complex multimillion pound projects to remove their dependency on equipment from suppliers such as Huawei.[71] Similar equipment removal decisions have been adopted in the German telecommunications market.[72] There have also been reports of utilities removing equipment provided by Chinese vendors from high-criticality environments.[73] These instances highlight the need for the critical infrastructure industries, including BESS, to adopt evergreen control systems that are more easily modernized and upgraded over time as standards shift or new policies emerge.

Verifying the origin of hardware is a complex task, but hardware is at least physical and visible. Software, however, is more complex and with many applications being built using existing code, drivers, or libraries. Building a detailed picture of these software sub-components is critical to understanding the potential dependencies and vulnerabilities that might exist within a system. A software bill of materials (SBOM) can provide assurance of the software supply chain, as these are most accurate when produced during the software development. However, retrospective generation of an SBOM can be $1,000–20,000 per asset, depending on the level of detail and expected accuracy – and it often requires reverse engineering of a third-party's intellectual property. These costs would not address any vulnerabilities discovered, and should these not be addressable via an update, could run into costs of more than $100,000 and may result in the need for complete asset replacement.

Retrospective replacement of major physical system components due to a loss of support or trust from a vendor could result in a big impact. While proportional to the scale of the facility, it is expected that replacing a component, such as inverters, can result in major re-engineering and testing. Additionally, the cost of supply can range from $1 million to $10 million. Given the nature of modern OT devices, it is unlikely that third party software could be provisioned on hardware provided by another manufacturer, in particular for firmware-based devices which rely greatly on their original manufacturer for support.

[71] UK Department for Digital, Culture, Media & Sport, "Huawei legal notices issued," October 13, 2022, https://www.gov.uk/government/news/huawei-legal-notices-issued.

[72] Federal Ministry of the Interior, "Greater security and technological sovereignty for the German 5G mobile network: The Federal Government concludes contracts with telecommunications companies," July 11, 2024, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2024/07/5g-en.html.

[73] Reuters, "Britain's National Grid drops China-based supplier over cyber security fears," December 17, 2023, https://www.reuters.com/technology/cybersecurity/britains-national-grid-drops-china-based-supplier-over-cyber-security-fears-ft-2023-12-17/.

Implementing controls in retrospect is complex and costly. Cybersecurity controls are best implemented when thoroughly tested, but doing this in a realistic environment rather than during design or factory acceptance testing can lead to costly extended outages or inconclusive testing due to concerns of introducing emulated threats in a production system. Device and system penetration testing can show where weakness exists in a configuration. These often expose new and existing vulnerabilities in software sub-components. Often, these sub-component applications are not declared or obfuscated.

While it can be difficult to predict the future behavior of a supplier, it is important to understand how they approach cyber vulnerabilities and what processes they have in place for communicating and resolving them. In late 2017, researchers from Kaspersky discovered a vulnerability in a relay product and followed an ethical disclosure process with ICS CERT (succeeded by CISA).[74] By January 2018, ICS CERT was forced to disclose this vulnerability after having had no response from the relay vendor. This demonstrated a lack of robust vulnerability management processes with the vendor, and while an update was released after customer pressure, confidence in their ability to manage this critical process was significantly damaged.

Vulnerabilities are inevitable, so the approach to managing them is critical. Robust procedures to prevent their introduction should be of primary concern for anyone looking to buy a long-term asset, but it is also important to understand a technology provider's process for managing discovered vulnerabilities. It is important to have a demonstrable understanding of the product's HBOM and transparency with the end owner support and long-term assurance around the cybersecurity of a BESS.

G. Summary

- Proactively integrating cybersecurity during design and construction is significantly more cost-effective than retrofitting later.
- HBOMs and SBOMs are essential tools for identifying risks, verifying component authenticity, and managing software vulnerabilities.
- Critical components like PCS, BMS, and EMS require prioritized scrutiny due to their impact on system reliability and safety.

[74] Kaspersky ICS CERT: "Vulnerability in Nari PCS-9611 relays," January 2018, https://ics-cert.kaspersky.com/publications/blog/2018/01/29/nari/.

- Trust in vendors and their supply chains is key to preventing counterfeit or insecure hardware and software.
- Long-term software support agreements are vital to manage patching, obsolescence, and vulnerability disclosures.
- Secure system architecture must include segmentation, firewalls, and strong perimeter controls to reduce exposure.
- Remote access should be tightly controlled with role-based permissions, MFA, logging, and dedicated workstations.
- Continuous network monitoring helps to detect adversarial activity and maintain visibility across BESS communications.

V. Conclusion

Battery energy storage systems are rapidly becoming a large and essential part of American, European, and other global power grids. They provide capacity, energy, resilience, and other reliability services to steadily expanding power systems with ever-larger amounts of variable renewable electric generation. By the end of the decade or sooner, BESS capacity in both the US and the EU is expected to surpass 400 GWh – more than four times 2024 levels and roughly equal (in capacity terms) to the EU's current nuclear fleet.[75] As a result, ensuring that this capacity remains cybersecure is an integral part of the larger challenge of maintaining overall power system security in a changing geopolitical environment.

A review of the threat landscape demonstrates that, for the first time, BESSs and their key components are becoming the focus of threat actors targeting the overall utility sector, including the 18 specific threat actor groups tracked by Dragos. At present, about half of all BESS components are sourced from foreign nations with security concerns. Many modern BESSs are designed to allow remote access to the BESS by these OEMs; this access creates multiple intrusion paths for threat actors. In addition, other digital components used within the BESS or introduced for functions such as servicing can introduce vulnerabilities. Press reports have already indicated that US experts have identified at least one instance of an unauthorized communication device in a key energy conversion element.[76] This energy conversion element is used in BESS systems, so there is a risk of this type of unauthorized communication occurring in BESS systems.

The potential harm from BESS cyber-intrusion extends beyond the owners and operators of BESS facilities to their regional grid, their regional economy, and potentially the national security arena itself. For owners and operators, revenues lost from a single month-long outage could be in the range of $400,000–1.2 million for a single 100 MW (4-hour duration, 400 MWh) BESS facility, excluding the costs of remediation and repair and reputation capital losses, both of which may exceed revenue losses. In extreme cases, BESS cyberattacks could destabilize

[75] The EU currently has 98 MWe of nuclear generation, according to the World Nuclear Association.

[76] Reuters, "'Ghost in the machine': Rogue communication devices found in Chinese solar power inverters," May 14, 2025, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.

their regional grid and trigger blackouts with enormous economic losses, immediate threats to health and safety, and possible national security implications.

Recognizing these threats, national and subnational authorities are adopting or proposing increased cybersecurity requirements that impact developers, owners, operators and maintainers of BESSs. The US is already limiting the use of some BESS components sourced from FEOCs from federally-supported and defense department projects, while the European Union has adopted both a cybersecurity directive and a cybersecurity certification law applying to BESS systems and components. Though exact policy pathways for additional legislative or regulatory restrictions are not entirely certain yet, the expert panel we interviewed uniformly agreed that cybersecurity requirements will (and should) be strengthened for operational technologies, including BESSs, in both the US and Europe.

To stay ahead of these developments, ODOMs should monitor the evolving cybersecurity landscape and ensure that cybersecurity protections are designed and built into their installations from the start and maintained throughout the asset's lifetime. Useful measures that these BESS participants can adopt include:

- Requiring verified HBOMs and SBOMs for OEMs and other vendors and relying on controlled software development whenever possible;
- Creating a defensible architecture with proper segmentation or zoning of assets and safe shutdown modes;
- Best-in-class secure remote access provisions, such as role-based access controls;
- Monitoring all network connections between and within operating sections of the facility; and
- Making cybersecurity a core tenet guiding their people, practices, and supply chains.

For these and other measures, building in cyber protection from the start, as suggested by the Idaho National Laboratory's Secure by Design framework, is likely to be much less costly than retrofit solutions.[77] Using a proactive approach to security, BESS ODOMs can greatly reduce the risks and damage from costly cyberattacks. With this protection, they can better ensure that energy storage systems remain safe and secure contributors to the essential economic, social, and national security services provided by electric power systems around the world.

[77] Idaho National Laboratory, *"A National Secure-by-Design Strategy,"* April 2023, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65687.pdf.

Authors

Peter Fox-Penner is a Brattle Principal based in Washington, DC. Specializing in the markets, policies, regulation, and transformation of the electricity industry, he advises US energy companies, grid operators, and government agencies. He has testified on energy-related matters in more than 100 proceedings before federal and state courts, the Federal Energy Regulatory Commission, arbitrations, and public service commissions. He has served as a regulatory and strategic advisor to boards and executives and is the author of numerous books and articles.

PFoxP@brattle.com

Phil Tonkin is Field Chief Technology Officer at Dragos, Inc., where he uses his experience in the energy sector to provide technical insight and strategic guidance in securing industrial operations. His career has included roles in electricity transmission, distribution, and generation; gas transmission, distribution, and storage; and IT. Prior to joining Dragos, he led the OT security program at one of the world's largest investor-owned utilities for five years.

PTonkin@dragos.com

Justin Pascale is a Principal Industrial Consultant at Dragos, Inc., where he helps asset owners and business leaders better understand and enhance their cybersecurity capabilities. He believes in working with customers to identify tailored cybersecurity solutions that align with and support business objectives and operational practices.

JPascale@dragos.com

Noah Rauschkolb is an Energy Associate at Brattle, based in San Francisco. He supports clients on technical and economic analysis of emerging technologies, including battery energy storage, distributed energy resources (DERs), and load flexibility. He holds a Ph.D. in Mechanical Engineering from Columbia University.

Noah.Rauschkolb@brattle.com

Purvaansh Lohiya is a Senior Energy Analyst at Brattle, based in San Francisco. He supports Brattle experts in matters of energy litigation, decarbonization, transmission and utility planning. He holds a B.Sc. in Chemical Engineering from University of California, Berkeley.

Purvaansh.Lohiya@brattle.com