Testimony of Dr. Paul N. Stockton[1]

Senior Fellow, Johns Hopkins University Applied Physics Laboratory

Before the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

"Examining Emerging Threats to Electric Energy Infrastructure Mission of Affordable and Reliable Energy for America"

July 18, 2023

Chair Rodgers, Ranking Member Pallone, Chair Griffith, Ranking Member Castor, and members of the Subcommittee, thank you for the honor of testifying before you today.

Threats to America's electric energy infrastructure are intensifying and increasingly diverse. Two factors are driving these trends, one that is obvious and another that gets less attention than it merits. We typically focus on the increasingly sophisticated attack capabilities that China and other potential adversaries can employ against our electric system. I look forward to discussing those capabilities with you today, including cyber, physical and electromagnetic threats.

[1] Nothing in my testimony necessarily reflects the positions of the Department of Energy, the Department of Defense, or any other Federal agency.

A second factor is also changing the threat landscape. The US grid is undergoing a fundamental transformation, driven by the nationwide deployment of solar and wind generation assets, battery energy storage systems, and advanced power electronics to control them. This transformation is creating new opportunities for adversaries to attack our electric system. Yet, if we can strengthen the protection of these new electric system components, we may be able to adopt innovative resilience strategies that offer immense benefits for national security. We can also focus those strategies to directly counter the objectives that China is likely to seek if it attacks America's electric system.

INVERTER-BASED RESOURCES: NEW ATTACK SURFACES AND RESILIENCE OPPORTUNITIES

Solar, wind, and battery energy storage systems are inverter-based resources (IBR): they rely on inverters and other power electronics to deliver the electricity they generate to the grid.[2] The North American Electric Reliability Corporation (NERC) states that "inverter-based resources are now found everywhere across the bulk power system (BPS) in North America and are the most significant driver of grid transformation today."[3]

[2] Inverters are electronic devices that convert direct current (DC) electricity, which is what solar panels generate, to alternating current (AC) electricity, which the electrical grid uses. Grid-connected wind generation assets and battery energy storage systems typically require inverters as well. Department of Energy (DOE), *Solar Integration: Inverters and Grid Services Basics*, https://www.energy.gov/eere/solar/solar-integration-inverters-and-grid-services-basics; DOE, *Solar Power Electronic Devices*, https://www.energy.gov/eere/solar/solar-power-electronic-devices; Section II of this paper examines inverter functions and vulnerabilities in greater detail.

[3] North American Electric Reliability Corporation (NERC), *An Introduction to Inverter-Based Resources on the Bulk Power System*, June 2023, 1, https://www.nerc.com/pa/Documents/2023_NERC_Guide_Inverter-Based-Resources.pdf. NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system

IBRs have provided reliable, much-needed power during the 2023 heat domes and other extreme events. Yet, they are also prone to catastrophic failures that can put the grid at risk. NERC has found that multiple large-scale disturbances of the bulk power system have occurred due to "systemic deficiencies" in the inverters for solar generation resources. These problems pose "a significant risk to BPS reliability" and could potentially cause "widespread outages."[4]

IBR vulnerabilities also provide China with new opportunities to create such blackouts. In a detailed and insightful study issued by the Department of Energy, the Department highlighted a variety of ways in which adversaries can attack inverter-based resources as a means to disrupt local power distribution systems. In particular, the Department has determined that distributed energy resources (DERs) - that is, solar and other inverter-based resources that are tied to distribution systems - are creating new attack surfaces, and that "malicious actors are positioned well to enter DER energy systems."[5] These threats go beyond local distribution systems, however. As inverter-based resources are increasingly tied to the high-voltage transmission infrastructure that provides the backbone of America's grid, the systemic deficiencies of IBRs will pose growing risks to the US electric system as a whole.

awareness; and educates, trains, and certifies industry personnel. NERC, *About NERC*, https://www.nerc.com/AboutNERC/Pages/default.aspx

[4] NERC, *Industry Recommendation: Inverter Based Resource Performance Issues*, March 14, 2023, 1, 6-7, https://www.nerc.com/pa/rrm/bpsa/AlertsDL/NERCAlertR-2023-03-14-01Level Inverter-BasedResourcePerformanceIssues.pdf

[5] DOE, *Cybersecurity Considerations for Distributed Energy Resources on the US Electric Grid*, October 2022, 16, https://www.energy.gov/sites/default/files/2022-10/CybersecurityConsiderationsforDistributedEnergyResourcesontheU.S.ElectricGrid.pdf.

Today, the severity of this threat is limited by the relatively small portion of US electricity that solar and wind generation provides. Solar photovoltaic and wind systems combined provided only 13.6 percent of the electricity generated in 2022.[6] However, those levels are projected to quickly increase. According to DOE's Lawrence Berkley National Laboratory, the combined solar and wind capacity now actively seeking grid interconnections (~1,250 GW) approximately equals the installed capacity of the entire U.S. power plant fleet.[7]

DOE also projects rapid growth in DER generation. Approximately 90 gigawatts (GW) of DER were deployed across the grid in 2022, half of which are rooftop solar installations that now total over 3 million systems. DOE expects those deployments to quadruple by 2025 to approximately 380 GW.[8] Changes in federal and state renewable energy targets, constraints on transmission system availability and expansion, supply chain problems, and other factors could limit the expansion of solar and wind generation in the coming decade. Nevertheless, strategies to secure the grid of the future must account for massive increases in IBRs and the new attack surfaces they will create.

These strategies should also account for the emerging capabilities that inverters and other power electronics will offer – for good and ill. Efforts are underway to enable IBRs to help operators

[6] In 2022, solar photovoltaic systems provided 3.2% of total US generation; wind provided 10.2%. US Energy Information Administration (USEIA), *What is U.S. Electricity Generation by Generation Source*, https://www.eia.gov/tools/faqs/faq.php?id=427&t=3

[7] Lawrence Berkely Laboratory, *Grid Connection Requests Grow by 40% in 2022 as Clean Energy Surges, Despite Backlogs and Uncertainties*, April 4, 2023, https://emp.lbl.gov/news/grid-connection-requests-grow-40-2022-clean. For a similarly robust projection of solar growth and a survey of factors that will affect it, see DOE, *Solar Futures Study*, September 2021, https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf

[8] DOE, *DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid*, October 6, 2022, https://www.energy.gov/eere/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy

maintain the grid's reliability, including by controlling frequencies and voltages when disturbances occur. Indeed, as inverter-based resources provide an increasing share of US power, their ability to provide such reliability services will become vital. Battery energy storage system (BESS), which also rely on inverters, will be especially important for future reliability because they can help grid operators deal with the intermittency of solar and wind-provided power and provide additional frequency and voltage support when needed.

But these capabilities also entail risks. As DOE warns, adversaries can seek to access and manipulate advanced IBR capabilities, and use them to create potentially catastrophic disruptions.[9] The very measures we take to enhance the reliability of an IBR-heavy grid may inadvertently jeopardize the grid's cyber resilience. I will speak shortly about these risks and propose options to make the future grid both reliable and survivable.

In addition, grid strategies should capitalize on the novel security benefits that nationwide deployment of IBRs could provide. If we can secure solar, wind, and battery storage systems from adversary disruption and exploitation, we may be able to adopt new grid protection and emergency response strategies that help prevent China or other adversaries from achieving their objectives. We can also explicitly structure our implementation of these new strategies to strengthen deterrence by resilience, and (in combination with credible threats of responding to enemy attacks)

[9] DOE, Cybersecurity Considerations. Specific threat scenarios involving exploitation of advanced IBR capabilities at the distribution level (i.e., DERs) are examined on pp. 21-28

help convince Xi Jinping that the benefits of striking the US grid are dwarfed by the costs China would incur.[10]

Opportunities to improve resilience are emerging at multiple levels of the electric system, including nationwide, regional, and device-level initiatives.

- As millions of solar, wind, energy storage, and control systems are deployed throughout the US, we may be able to shift towards a decentralized grid architecture that is more difficult to disrupt than today's version, which relies on a small number of critical, high-value assets that adversaries can selectively target.

- At a regional scale, where individual transmission operators (TOPs), balancing authorities, and reliability coordinators help operate the BPS, dispersed generation can also enable new strategies to limit the impact of grid instabilities and cascading blackouts. Microgrids already enable the creation of "power islands" that can segment from the grid in emergencies to sustain service to military bases and other customers within them. Now, building on existing TOP remedial action schemes, dispersed generation may enable these operators and their partners to create much larger (and, ideally, more stable) emergency islands that can power the multiple, interdependent infrastructure systems on which national security, public safety, and the grid itself depend.[11]

[10] Deterrence by resilience is defined in DOD's *2022 National Defense Strategy of the United States of America*, October 27, 2022, 8, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[11] NERC defines a remedial action scheme (RAS) as "a scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and Mvar), tripping load, or reconfiguring a System(s)." Section V of this study examines how TOPs can build

- At the device level, the future deployment of grid-forming inverters, advanced controls for battery energy storage systems (BESS), and other emerging technologies may enable TOPs to conduct power restoration using decentralized assets that will be more difficult for adversaries to target and disrupt.[12] These restoration opportunities could have special strategic value if China or other adversaries conduct sustained, multi-week grid attacks during regional conflicts with the United States.

None of these resilience strategies will be viable unless we can defend solar, wind, and battery systems from adversary exploitation and disruption. In the next portion of my testimony, I will offer specific recommendations to prioritize the protection of such assets. Before doing so, however, it will first be helpful to examine the threat implications of a further challenge to grid reliability and resilience: the rise of electric vehicles (EVs), "smart" buildings, and other highly controllable sources of demand for power. Electric system operators must constantly maintain the balance between total generation and the consumption of electricity, or load.[13] Such balancing operations are crucial to maintain or restore grid reliability when disturbances occur - including, potentially, cyber-induced disruptions.

on their existing RAS to enable pre-planning and operation of strategic power islands. NERC, *Glossary of Terms*, updated March 8, 2023, 26, https://www.nerc.com/pa/Stand/Glossary of Terms/Glossary_of_Terms.pdf

[12] For a definition of grid-forming inverters and summary of their potential power restoration roles, see NERC, *White Paper: Grid Forming Controls*, December 2021, iv, 16, https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Grid_Forming_Technology.pdfhttps://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Grid_Forming_Technology.pdf

[13] Load is defined as "An end-use device or customer that receives power from the electric system." NERC, Glossary, 18.

Grid operators often respond to imbalances by conducting demand-side management operations. For example, they can conduct load shedding, and temporarily halt or reduce the flow of power to selected areas or customers. With the rapidly growing deployment of EVs and their charging stations, as well as other loads that can be controlled via the internet, options are now emerging for emergency demand-side management on a massive scale. These same capabilities are opening the door to unprecedented opportunities to manipulate demand for power, and exacerbate rather than remedy grid instabilities.

PRIORITIZING AND IMPLEMENTING GRID RESILIENCE INITIATIVES

With the emergence of so many new attack surfaces, developing and implementing grid resilience strategies will entail an additional challenge: prioritizing our cybersecurity efforts. DOE offers a starting point to do so. The Department recommends that cyber resilience initiatives concentrate on potential threats "where cyber manipulation could result in unacceptable consequences."[14] That recommendation offers a valuable starting point to focus our resilience initiatives. In addition, I propose that we prioritize our efforts to prevent Chinese leaders from accomplishing their goals in attacking the grid.

US intelligence assessments and DOD's 2022 National Defense Strategy suggest that China will have two especially prominent goals in disrupting US infrastructure. First Chinese leaders will seek to undermine the will of the US public to defend our allies abroad. Jeopardizing public safety

[14] DOE, *National Cyber-Informed Engineering Strategy*, June 2022, 12. For comprehensive recommendations on creating consequence-based resilience strategies, see Idaho National Laboratory, *Consequence-Driven Cyber-Informed Engineering*, https://inl.gov/cce/, and Andrew Bochman and Sarah Freeman, *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering* (Boca Raton, FL: CRC Press, 2021)

by halting the flow of power to water systems, hospitals, and other electricity-dependent "lifeline" facilities offers a highly leveraged means to achieve that goal, and coerce US leaders into backing down in confrontations over Taiwan or other regional conflicts. US grid strategies should help prevent Chinese leaders from accomplishing such objectives. In particular, as inverter-based resources become ubiquitous, we should prioritize efforts to secure them so they can help protect (and, if necessary, rapidly restore) power to facilities and functions essential for saving American lives.

Chinese leaders may also conduct much more limited strikes that might entail reduced escalatory dangers, but still help them prevail in regional conflicts. Senior US officials and military officers warn that Beijing may launch narrowly targeted attacks on the grid to disrupt the domestic operations necessary to support military power projection during an intensifying confrontation over Taiwan or some other regional contingency.[15] Grid security strategies for the IBR-heavy grid must also help strengthen resilience against such "fort to port" attacks and other efforts to impede US preparations at home for warfighting abroad.

The prerequisite for achieving both goals: as the US transitions from a relatively small number of large-scale generators to a highly decentralized system, we need to prevent those dispersed resources and their control systems from having *common mode failures* that would enable Beijing to manipulate or disrupt them at whatever scale Chinese leaders desire – from key US ports of debarkation to comprehensive, nationwide strikes.[16]

[15] Glen D. VanHerck and Jacqueline D. Van Ovost, "Fighting to get to the Fight," *Military Times*, May 31, 2022, https://www.militarytimes.com/opinion/commentary/2022/05/31/fighting-to-get-to-the-fight/

[16] Common failure modes are defined here has vulnerabilities shared by widely deployed hardware, firmware, software, or support services (such as cloud data storage) that adversaries can exploit to cause the widespread,

Members of the Committee, I believe that we need device-level security requirements for inverters and other grid components that pose special risks of exploitation for catastrophic or more targeted attacks. I also recommend that we develop measures to secure the grid against large-scale load manipulation, and leverage America's rapidly increasing battery storage capabilities to help protect and rapidly restore power to the facilities that Chinese leaders seek to hold at risk.

Many such initiatives will require new regulatory strategies. As you know, the BPS has mandatory, enforceable cybersecurity standards that strengthen its resilience against attack. No equivalent standards exist for distribution-level utilites, which are regulated by states and which are incorporating rapidly expanding solar generation assets and control systems. Moreover, energy aggregators and other non-utility operators play increasingly important roles in managing and marketing these distribution-level power flows. These new entrants typically have far less cybersecurity experience and expertise than their utility counterparts.

I recommend that we develop a holistic regulatory strategy that includes all of the assets and participants needed to prevent high-consequence events, including demand-side attacks. I also recommend that we establish mandatory, enforceable cybersecurity standards for *all* grid components that China might exploit to conduct attacks that would jeopardize public safety or national security, regardless of whether those components are deployed on distribution systems or the BPS.

simultaneous disruption or mis-operation of such assets. The nuclear power industry uses an equivalent term, common cause failure, to describe a similar phenomenon: the "loss of function to multiple structures, systems, or components due to a shared root cause." Nuclear Regulatory Commission, *Common Cause Failure Definition*, September 14, 2017, https://www.nrc.gov/docs/ML1725/ML17257A412.pdf

Members of the Committee, thank you again for the honor of testifying, and I look forward to any questions or comments you might have.

MAJOR POINTS OF STOCKTON TESTIMONY

- Threats to America's electric energy infrastructure are intensifying and increasingly diverse. These trends reflect the increasingly sophisticated attack capabilities that China and other potential adversaries can employ against our electric system. The transformation of the US grid is also creating new opportunities for adversaries to attack our electric system.
- The grid is rapidly incorporating solar, wind, and battery energy storage systems on a nationwide basis. These assets are inverter-based resources (IBR): they rely on inverters and other power electronics to deliver the electricity they generate to the grid. IBR vulnerabilities provide China with new opportunities to disrupt the grid, and these risks will grow as IBR penetration increases.
- If we can strengthen the protection of IBRs, we may be able to adopt new resilience strategies that leverage their highly dispersed deployment. Such strategies could offer immense benefits for national security. In addition, we can focus strategies to directly counter the objectives that China is likely to seek if it attacks America's electric system.