



**Congressional
Research Service**

Informing the legislative debate since 1914

Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience

May 17, 2024

Congressional Research Service

<https://crsreports.congress.gov>

R48067



R48067

May 17, 2024

Brian E. Humphreys
Analyst in Science and
Technology Policy

Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience

Russia has conducted a deliberate campaign to destroy Ukrainian electricity infrastructure as part of its larger war effort against Ukraine. This campaign dates to the initiation of hostilities in 2014, but intensified in October 2022 after a broader Russian invasion, begun on February 24, 2022, stalled. Ukrainian authorities were able to prevent wholesale collapse of the grid and maintain critical services—albeit with curtailments and interruptions. Ukraine’s defense of critical infrastructure against sustained cyber and physical attacks provides real-world insights into Russian capabilities and tactics, and highlights potential vulnerabilities of U.S. electricity production and supply against persistent threats.

Russia launched several cyberattacks that caused limited short-duration service interruptions in some cases. Physical attacks had more strategic impact, bringing the Ukrainian grid to the brink of collapse as rolling blackouts became commonplace in late 2022, before moderating in early 2023. The overwhelming majority of Russian strikes against Ukrainian infrastructure targeted transmission facilities—as opposed to power stations—and focused on substations and hard-to-replace large power transformers (LPTs) used to step voltage up or down for long-distance transmission and local distribution, with the apparent aim of isolating and destabilizing major sections of the grid. Other strikes targeted industrial producers of replacement grid equipment, as well as assets used to transfer electricity between the Ukrainian and European grids.

However, Ukrainian electricity infrastructure has thus far proved resilient. Some observers credit Ukrainian resilience against cyberattacks to grid operators’ familiarity with Russian tactics, vigilant cyber hygiene, skilled use of manual override controls in the absence of full visibility over control systems, and technical assistance from the United States and other countries. Likewise, resilience against physical attacks was aided by pre-invasion investments in transmission system modernization, stockpiling of spare equipment, and scenario modeling, which increased grid operators’ threat awareness and adaptive capacities. Wartime improvisation—such as the use of Starlink stations to fill communications gaps during grid emergencies—also played a role. Some broader structural problems, such as the low energy efficiency of Ukrainian infrastructure, and massive out-migration of would-be ratepayers, were partially addressed through emergency measures. However, reforms of inefficient and politicized market and regulatory structures were largely deferred.

Ukrainian experiences have highlighted complex interdependencies among society, governance, the economy, and infrastructure systems. The extent to which U.S. policymakers, federal agencies, or industry partners have contemplated these interdependencies, or prepared for sustained grid operations with degraded capabilities in an environment of continuing attrition of assets, is not clear. Exercise and grid-modeling scenarios often present grid emergencies as discrete and anomalous events starting from a baseline of full operational functionality—including operable communications—rather than from a degraded state due to previous hazard events, and they generally do not model societal and economic interfaces with infrastructure systems. Existing federal programs for energy efficiency, low-income ratepayer support, and disaster assistance may mitigate societal and economic vulnerabilities to some extent by expanding and stabilizing the ratepayer base and utility finances, and reducing stress on the grid, but such benefits are largely incidental to other program goals, such as social welfare, environmental protection, and job creation.

Recent congresses have enacted major legislation to fund investments in expansion, modernization, and hardening of transmission infrastructure to enhance resilience. For example, the Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) directs the Department of Energy (DOE) to provide grid resilience grants to eligible entities based on “greatest community benefit” in reducing disruptions to service. However, the electricity sector still lacks consensus resilience metrics to inform such assessments, according to some experts. The IIJA also requires DOE to assess stockpiling options for LPTs, and to provide an update of related industry efforts. A 2023

Government Accountability Office report found that DOE had not “identified actionable objectives, or time frames” to complete these tasks.

Potential options for Congress include instituting stockpiling programs, creating industrial production incentives, establishing supply chain security requirements, overseeing national exercise programs, and supporting development of consensus resilience metrics. The interdependencies between electricity market design and regulation, the financial solvency of ratepayers and utilities, and grid security and resilience during complex crises could be considerations for Congress when authorizing, funding, or exercising oversight of relevant programs for social welfare, job creation, disaster recovery, or environmental protection.

Contents

Introduction	1
Background: The Ukrainian Grid	1
Ukrainian Pre-Invasion Generation Capacity	2
Ukrainian Pre-Invasion Transmission Network	2
Russian Infrastructure Attacks.....	3
Cyber Effects.....	4
Physical Effects	6
Economic Effects	8
Ukrainian Resilience to Infrastructure Attacks.....	8
Cyber Resilience	9
Physical Resilience.....	10
Economic Resilience.....	14
Lessons Learned: Implications for U.S. Grid Resilience	14
Potential Gaps in U.S. Preparedness	16
Russian Capabilities and Limitations	16
Potential Attrition Risks to the U.S. Electricity Sector and Mitigation Considerations	17
Industrial Base Capacity, Supply Chain Security, and Stockpiling.....	17
Economic Resilience	19
Disaster Assistance.....	20
Affordability, Access, and Social Welfare.....	21
Efficiency, Jobs, and the Environment.....	22
Generation	23
Transmission	24
Energy Management Systems and Cybersecurity	25
Issues for Congress.....	27

Contacts

Author Information.....	29
-------------------------	----

Introduction

Russia has conducted a deliberate campaign to destroy Ukrainian electricity infrastructure as part of its larger war effort against Ukraine. This campaign dates to the initiation of hostilities in 2014, but intensified in October 2022 after a broader Russian invasion, begun on February 24, 2022, stalled.¹ Hundreds of missile and drone attacks—apparently informed by expert Russian analysis of Ukrainian electricity infrastructure systems—struck generating plants, substations, and large power transformers (LPTs). Damage or disruption from cyberattacks also presented a significant threat, although strategic effects were comparatively limited. Ukrainian authorities were able to prevent wholesale collapse of the grid and maintain critical services—albeit with curtailments and interruptions—through a combination of adaptation, foreign aid, and pre-war preparation.

The Ukrainian case presents a singular example of defense against sustained critical infrastructure attacks conducted by a capable adversary in cyber and physical realms. By necessity, Ukraine has defended and operated its electric grid in a degraded state over a period of years against steady—sometimes rapid—attrition of key assets. The United States, by contrast, has comparatively little experience in addressing persistent attritional threats to its grid—either manmade or natural. The Ukrainian experience exposes linkages between regulatory, social, environmental, and economic policy on one hand, and—on the other—technical and operational aspects of grid security and resilience that are often not readily apparent during steady-state periods or short-term emergencies.

This report provides analysis of the Ukrainian experience and its potential implications for U.S. critical infrastructure security and resilience. The analysis is twofold. First, the report considers how actual—as opposed to hypothetical—adversary threats were manifested in Ukraine, and what factors affected critical outcomes. Second, it considers how these outcomes may usefully frame issues of U.S. strategic energy security—the nation's ability to sustain national critical energy production and supply functions against natural or manmade hazards with minimal disruption. It examines how these issues intersect with several areas of longstanding congressional policy interest in the U.S. electricity sector: private sector investment; affordability, access, and social welfare; consumer protection; energy efficiency and the environment; disaster assistance; and job creation and “re-shoring” of industrial production.² It concludes with a discussion of legislative and oversight options for Congress.

Background: The Ukrainian Grid

Ukraine gained independence in 1991 after the collapse of the Soviet Union, inheriting a vertically-integrated and state-owned electricity monopoly.³ Although the Ukrainian grid provided universal access to electricity, it was considered inefficient—among the most energy-

¹ For more, see CRS Report R47068, *Russia's War in Ukraine: Military and Intelligence Aspects*, by Andrew S. Bowen.

² The definition of strategic energy security used in this report is adapted from National Renewable Energy Laboratory (NREL), “Strategic Energy Security,” <https://www.nrel.gov/security-resilience/strategic-energy-security.html>; and Cybersecurity and Infrastructure Security Agency (CISA), “National Critical Functions,” <https://www.cisa.gov/topics/risk-management/national-critical-functions>.

³ The World Bank Group, *Electricity Reform in Ukraine: The Impact of Weak Governance and Budget Crises*, Note No. 168, Washington, DC, December 1998, <https://openknowledge.worldbank.org/server/api/core/bitstreams/c3d477d8-b594-5891-b98a-7fe1ad2ac38a/content>.

intensive in the world⁴—and unsustainable in the context of an emerging market economy.⁵ A series of reforms over the ensuing decades led to partial privatization and market reforms that separated generation, transmission, and distribution segments in an effort to make them more competitive. Reform efforts to bring the sector into alignment with applicable European Union (EU) market design and risk management standards accelerated after Russia illegally annexed Crimea in 2014.⁶ However, the full suite of market reforms that may have addressed persistent underinvestment issues had not been enacted or implemented prior to the Russian invasion in 2022.⁷

Ukrainian Pre-Invasion Generation Capacity

Ukraine had 59 gigawatts (GW) of installed generation capacity in 2021, but a substantial share of this capacity was unavailable due to age and maintenance issues, even prior to the 2022 invasion.⁸ Nonetheless, Ukraine possessed major nuclear, thermal, and hydroelectric power plants, as well as an expanding portfolio of renewable energy-based generation capacity.⁹ Data provided to the International Energy Agency (IEA) by Ukrenergo, the state grid operator, showed that 2022 daily generation peaked on January 27 at 21.3 GW—in line with generation levels of the previous several years.¹⁰ Generation levels were sufficient to meet demand.¹¹

Ukrainian Pre-Invasion Transmission Network

The national transmission network and interconnections with neighboring countries are operated by Ukrenergo, the state grid operator. Until the 2022 invasion, the network was synchronized with Russia's grid—the Soviet legacy system, which also included other former Soviet republics.¹² Synchronization of generators within a larger system usually provides greater

⁴ DOE defines energy intensity as “the quantity of energy required per unit output or activity.” See DOE, “Overview of Energy Intensity Indicators,” <https://www.energy.gov/eere/analysis/overview-energy-intensity-indicators>. According to the International Energy Agency (IEA), Ukraine's energy intensity in 2018 was twice the world average. See IEA, “Ukraine Energy Profile, Demand,” <https://www.iea.org/reports/ukraine-energy-profile>.

⁵ Ibid.

⁶ Ibid., p. 11. For an overview of EU market design and risk management policy, see European Commission: Electricity Market Design, https://energy.ec.europa.eu/topics/markets-and-consumers/market-legislation/electricity-market-design_en.

⁷ Ibid., p. 4. According to the article, “The main promises of reform—depoliticization of electricity price setting and attraction of investment and know-how to the power industry—remain unfulfilled.” For additional discussion of Ukrainian sector characteristics and reform initiatives, see International Energy Agency (IEA), *Ukraine Energy Profile*, Paris, 2021, <https://iea.blob.core.windows.net/assets/ac51678f-5069-4495-9551-87040cb0c99d/UkraineEnergyProfile.pdf>.

⁸ EIA: Ukraine, Electricity, <https://www.eia.gov/international/data/country/UKR/electricity/electricity-capacity>. For discussion of pre-existing maintenance issues, see CMS, Expert Guide to Electricity Law and Regulation: Ukraine, “Generation,” <https://cms.law/en/int/expert-guides/cms-expert-guide-to-electricity/ukraine>. According to a June 2023 UNDP June report, Ukraine had 37.6 GW of generation capacity available at the beginning of 2022. See U.N. Development Program, *Towards a Green Energy Transition in Ukraine*, New York, NY, June 2023, p. 10, <https://www.undp.org/ukraine/publications/towards-green-transition-energy-sector-ukraine>.

⁹ Much of the renewable energy generation capacity fell under Russian control after the illegal annexation of Crimea.

¹⁰ IEA, “Data Explorer: Electricity Demand and Generation in Ukraine,” <https://www.iea.org/data-and-statistics/data-tools/ukraine-real-time-electricity-data-explorer>. Data provided by Ukrenergo.

¹¹ Robert Bacon, *Learning from Power Sector Reform: The Case of Ukraine*, The World Bank, Washington, DC, August 2021, p. 4.

¹² Synchronization is the process of matching the frequency and phase of a generator with all other generators on a common interconnection, which is necessary for grid stability. See “Energy KnowledgeBase: Synchronization,” <https://energyknowledgebase.com/topics/synchronization.asp>.

stability and redundancy compared with smaller networks because grid operators have greater ability to smooth out instantaneous fluctuations in supply and demand.

Ukrainian grid operations were complicated by the Russian seizure of Crimea and its generation assets in 2014, which made Ukraine even more dependent on Russian-controlled generation facilities that powered the legacy interconnection for load balancing.¹³ In addition, insufficient transmission capacity “[limited] the output of some nuclear plants,” which represented a large share of Ukraine’s power generation capacity.¹⁴ In sum, the Ukrainian grid faced several complex challenges on the eve of the invasion: high energy intensity, limited grid flexibility, transmission constraints, Russian seizure of generation assets in Crimea and eastern Ukraine, and reliance on a hostile power—Russia—for grid stability.

Some observers believe that Russia timed the February 2022 invasion to coincide with a planned Ukrainian test synchronization of its grid with the European grid. During the test, Ukraine disconnected from Russian power stations that had provided additional stability to its grid. This may have left it more vulnerable to further disruption and—at the same time—hampered Ukrainian response to the invasion.¹⁵

Russian Infrastructure Attacks

The Russian full-scale invasion began on February 24, 2022, causing major disruptions to the electricity sector. Daily demand rapidly declined by roughly 40% from pre-invasion levels, mostly due to wartime disruptions to the Ukrainian economy and dislocation of millions of electricity consumers.¹⁶ Russian capture of Ukrainian territory, followed by wholesale destruction of generation, transmission, and distribution systems beginning in October 2022, led to deficits in available generation capacity.¹⁷

A United Nations Development Program (UNDP) assessment conducted with the cooperation of Ukrainian authorities found that available generation capacity declined 51% between early 2022 and April 2023 due to loss of power plants.¹⁸ Damage to generation, transmission, and distribution networks forced imposition of rolling blackouts. The average Ukrainian household

¹³ IEA, “Data Explorer,” p. 27; and Eliza Batchelder et al., *Ukraine’s Potential Energy*, Center for Strategic and International Studies (CSIS), Washington, DC, 2023; see “Modernizing the Grid” section, <https://features.csis.org/ukraines-potential-energy/>. Load-balancing refers to grid operations to balance supply and demand for electricity on a nearly instantaneous basis to maintain grid stability.

¹⁴ Ibid.

¹⁵ For example, see Murray Brewster, “Power Play: How Russia Missed Its Window to Crash Ukraine’s Electrical Grid by Stealth,” *CBC News*, November 3, 2022, <https://www.cbc.ca/news/politics/russia-ukraine-kyiv-electricity-grid-1.6638410>; and Global Resilience Institute at Northwestern University, “GRRN Resilience Lecture Series: Ukraine’s Electric Grid During the Russian Invasion,” <https://globalresilience.northeastern.edu/grm-resilience-lecture-series-ukraines-electric-grid-during-the-russian-invasion/>.

¹⁶ IEA, “Data Explorer.”

¹⁷ According to a March 2023 World Bank and United Nations Development Program report, 10 GW of Ukrainian installed capacity remained under control of Russian forces as of 2023, and was not supplying the Ukrainian grid. See United Nations Development Program (UNDP) and The World Bank, *Ukraine Energy Damage Assessment*, Executive Summary, New York, NY, March 2023, p. 4.

¹⁸ UNDP, *Towards a Green Transition of the Energy Sector in Ukraine: Update on the Energy Damage Assessment*, New York, NY, June 2023, p. 6, <https://www.undp.org/ukraine/publications/towards-green-transition-energy-sector-ukraine>.

had to endure five cumulative weeks without electricity from October 10 to the end of December 2022, according to estimates based on Ukrenergo data.¹⁹

Russian infrastructure attacks against Ukraine included both cyber and physical components. Expert assessments of the level and quality of coordination between these lines of effort are mixed.²⁰ Both types of attacks targeted generation facilities and critical power substations in order to cause physical destruction of hard-to-replace assets, seeking maximum disruption of electricity supply to Ukrainian consumers. Through such means, Russia apparently attempted to break apart the unified Ukrainian grid into smaller “islands” of isolated power production and distribution that would be less stable and more vulnerable to follow-on attacks.

Cyber Effects

Russian cyberattacks on the Ukrainian grid predate the onset of full-scale war in February 2022. Russia carried out two widely-publicized attacks against Ukraine in 2015 and 2016, both of which the United States government attributed to the GRU—Russia’s military intelligence directorate.²¹

The 2015 cyberattack targeted regional power distribution companies. The attack deployed malware, called BlackEnergy, to the companies through spear-phished emails and malicious Microsoft Word files.²² Some affected companies’ computers were made inoperable in this attack. The BlackEnergy malware also spread to industrial control systems (ICS) of the companies that were connected to the internet, degrading the companies’ abilities to monitor and control their power delivery operations.²³ ICS energy management systems (in Ukraine and elsewhere) generally include Supervisory Control and Data Acquisition (SCADA) functions, telecommunications, and “real-time reliability support tools,” which are used to “monitor, control, and optimize” grid operations.²⁴ Loss, disruption, or exploitation of these energy management systems presents risk to grid visibility and flexibility, making them a potential target of cyberattacks.²⁵

According to the Department of Homeland Security’s Cybersecurity and Information Security Agency (CISA), “During the cyber-attacks [on Ukraine], malicious remote operation of the breakers was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via

¹⁹ UNDP, *Towards a Green Transition of the Energy Sector in Ukraine*, Update on the Energy Damage Assessment, June 2023, p. 11, <https://www.undp.org/ukraine/publications/towards-green-transition-energy-sector-ukraine>.

²⁰ See Jon Bateman, *Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, pp. 14-22, Washington, DC, 2022, <https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657>.

²¹ Cybersecurity and Infrastructure Security Agency, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,” Advisory AA22-110A, May 9, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>. Also, see *ibid.* Also, CRS InFocus 11718, *Russian Cyber Units*, February 2, 2022, by Andrew S. Bowen; and CRS Report R46616, *Russian Military Intelligence: Background and Issues for Congress*, by Andrew S. Bowen.

²² Cybersecurity and Infrastructure Security Agency, “Ongoing Sophisticated Malware Campaign Compromising ICS (Updated E),” ICS-Alert-14-281-01E, July 22, 2021, <https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e>.

²³ *Ibid.*

²⁴ North American Electric Reliability Corporation, *Risks and Mitigations for Losing EMS Functions Reference Document*, Version 2, March 3, 2020, p. 1, https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Risks_and_Mitigations_for_Losing_EMS_Functions_v2.pdf.

²⁵ Grid flexibility is a power system’s capacity to dynamically balance power supply with demand across a wide area using networked systems of electricity generation, transmission, and distribution. Grid visibility refers to system operator ability to ascertain the state of the grid and its various components at any given time.

virtual private network (VPN) connections.”²⁶ The credentials for operational technology (OT) systems were acquired illicitly. In addition, malware was deployed to erase files needed for system restoration. Approximately 225,000 customers were impacted, although outages were relatively brief—measured in hours.

The 2016 attack—conducted by the same GRU actors—built on tactics and techniques developed for the 2015 attack.²⁷ The attack encoded ICS manipulations within software rather than relying on hackers’ manual interactions with ICS—a change that made the attack more scalable, according to experts.²⁸ Malware was also used to stymie recovery attempts by preventing “legitimate communications with field equipment,” while a simultaneous denial-of-service attack targeted digital protective relays designed to shield essential grid equipment from electric faults.²⁹ Post-event analyses identified GRU programming errors that contributed to failure of the attack, but noted that essential remote monitoring systems were successfully taken offline during the latter phase of the attack.³⁰ Although no major outages were reported, Ukrainian grid operators had to manually close breakers at affected substations to restore electricity without full visibility of essential systems, putting grid equipment at risk.

In April 2022, the GRU attempted a third attack based upon a further development of the malware and tactics used in the 2016 attack. The attack targeted a regional Ukrainian utility and affected nine substations. However, the attack was quickly detected and neutralized by Ukrainian authorities, according to media reports.³¹ In July 2022, DTEK Group—a private sector energy provider—reported another Russian cyberattack on its IT infrastructure that coincided with a missile attack on one of its power stations, but did not provide details on tactics and techniques used or effects of the attack on critical infrastructure functions.³² Senior CISA officials have assessed that Russia has continued to mount cyberattacks on Ukrainian infrastructure during the full-scale war.³³ Russian attacks have also targeted the European grid on a continuing basis, according to media reports.³⁴

²⁶ CISA, “Cyber-Attack Against Ukrainian Critical Infrastructure,” <https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01>.

²⁷ Cybersecurity and Infrastructure Security Agency, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,” Advisory AA22-110A, May 9, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.

²⁸ Joe Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*, Dragos Inc., August 15, 2019, p. 3.

²⁹ Cybersecurity and Infrastructure Security Agency, “CrashOverride Malware,” website, July 20, 2021, <https://www.cisa.gov/uscert/ncas/alerts/TA17-163A>.

³⁰ Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event*, pp. 2-5.

³¹ Andy Greenberg, “Russia’s Sandworm Hackers Attempted a Third Blackout in Ukraine,” *Wired*, April 12, 2022, <https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>.

³² DTEK, “Enemy Launches Hacker Attacks on the Power System,” press release, July 1, 2022, <https://dtek.com/en/media-center/news/vslid-za-raketnimi-udarami-po-tes-vorog-zavdae-khakerskikh-udariv-po-energosislemi/>. For analysis of DTEK claims, see Bateman, *Russia’s Wartime Cyber Operations in Ukraine*, pp. 15-16.

³³ See Washington Post Live interview with Brandon Wales, CISA Executive Director, “Investing in America’s Cyber Infrastructure, Resilience and Workforce,” October 12, 2023, <https://www.washingtonpost.com/washington-post-live/2023/10/12/investing-americas-cyber-infrastructure-resilience-workforce/>.

³⁴ Victor Jack, “Europe’s Grid Is Under a Cyberattack Deluge, Industry Warns,” *Politico*, November 27, 2023, pp. <https://subscriber.politicopro.com/article/2023/11/europes-grid-is-under-a-cyberattack-deluge-industry-warns-00128694>.

Physical Effects

As was the case with cyberattacks, physical attacks on Ukrainian energy sector predated full-scale war in 2022.³⁵ The attacks primarily targeted power plants and long-distance transmission equipment, focusing on LPTs and assets with long-lead manufacture times. These attacks presaged the wider-scale attacks in 2022 and afterwards that affected the entire country. Damage from physical attacks was severe, bringing the Ukrainian grid to the brink of collapse as rolling blackouts became commonplace in late 2022, before moderating in early 2023.

On balance, physical attacks against electricity infrastructure proved much more destructive in terms of costs and service disruptions than the cyberattacks were.³⁶ The acute crisis period extended for roughly three months between October 2022 and January 2023, peaking in late November 2022.³⁷ A CRS analysis of open-source data aggregated by ACAPS, an international nonprofit, identified nearly 600 attacks on electricity infrastructure assets during the year following the February 24, 2022, invasion—the overwhelming majority targeting transmission and distribution assets.³⁸

A U.N. Development Program assessment reported that “41 out of 94 crucial high-voltage transforming substations located in government-controlled territories have been damaged or destroyed by missiles or drones.”³⁹ On the generation side, up to 60% of Ukrainian generation capacity was struck during the bombing campaign, according to some reports,⁴⁰ and available generation capacity fell from 37.6 GW to 13.6 GW between February 24 and December 31, 2022, before rising to 18.3 GW in April 2023.⁴¹ Total damage to the sector was estimated at more than \$9.1 billion by researchers at the Kyiv School of Economics.⁴² Major industrial enterprises with intact production lines were forced to curtail production due to electricity shortages, causing additional economic damage.⁴³

³⁵ Sophie Lambroschini, “How Do Ukrainian Networks Resist? Sources and Limits of Critical Infrastructure Resilience,” *PONARS Eurasia*, December 12, 2022, <https://www.ponarseurasia.org/how-do-ukrainian-networks-resist-sources-and-limits-of-critical-infrastructure-resilience/>.

³⁶ For a discussion of the comparative effectiveness of cyber versus physical attacks, see Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine*.

³⁷ See Marcus Walker and Yaroslav Trofimov, “Russia Tried to Freeze Ukraine. Here's How It Survived the Winter,” *Wall Street Journal*, March 20, 2023, <https://www.wsj.com/articles/how-ukraine-survived-russias-mission-to-turn-off-the-lights-winter-is-over-and-were-still-here-8668c5f5?st=5addrxt391g4oht>.

³⁸ See ACAPS, “Data/Ukraine/Ukraine-Damages,” <https://www.acaps.org/en/data#dataset-19>. CRS selected a date range between February 24, 2022, and February 24, 2023. The infrastructure type variable was filtered to include three categories: power plant; nuclear plant; and electricity distribution system. The total recorded attacks on each infrastructure type were as follows: [conventional] power plant (15); nuclear units (4); and electricity supply system (566).

³⁹ See the UN Development Program and the World Bank, *The Ukraine Energy Damage Assessment Report: Executive Summary*, March 2023, p. 4, https://ukraine.un.org/sites/default/files/2023-04/UNDP_Ukraine_Energy_ExecutiveSummary_eng.pdf.

⁴⁰ Suriya Evans-Pritchard Jayanti, *Ukraine's Energy Sector Survives Winter*, The Atlantic Council, April 11, 2023, <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-energy-sector-survives-winter/>.

⁴¹ See the U.N. Development Program and the World Bank, *The Ukraine Energy Damage Assessment Report: Executive Summary*, March 2023, p. 4; and the U.N. Development Program and the World Bank: *Update on the Energy Damage Assessment*, New York, NY, June 2023, p. 6.

⁴² International Energy Charter, Cooperation for Restoring the Ukrainian Infrastructure Project Task Force, *Ukrainian Energy Sector Evaluation and Damage Assessment-IV*, Brussels, Belgium, 2023, p. 3.

⁴³ Ian Lovett, “Russia Expands Shelling of Kherson, as Power Shortages Drag On in Kyiv,” *The Wall Street Journal*, November 25, 2022, <https://www.wsj.com/articles/russia-expands-shelling-on-kherson-as-power-shortages-drag-on-in-kyiv-11669370547>.

An advisor to the Ukrainian government described attacks on transformer substations as “painful” in an October 2022 media interview. Even though generation capacity remained sufficient, “the ability to transport electricity to consumers is gone.”⁴⁴ As the attacks progressed, availability of generation capacity became a greater concern. In addition, attacks on natural gas pipelines and facilities contributed indirectly to decreases in natural gas-powered electricity generation.⁴⁵

Russian targeting of electricity infrastructure apparently sought to hamper adaptation and recovery efforts. Some strikes targeted Ukrainian legacy equipment manufacturers, taking advantage of a unique vulnerability of the Ukrainian system—its reliance on Soviet-era equipment supported by a declining user and manufacturing base. In addition, Russian strikes targeted specially adapted LPTs that enabled a small-but-growing electricity trade between Ukraine and neighboring European countries.⁴⁶

Russia also conducted extensive attacks on communication facilities. Communications are essential for grid restoration operations after major disruptions, and for maintaining steady state operations in any electricity grid. According to the International Telecommunications Union, the first six months of full-scale war produced \$1.79 billion in damage to Ukrainian communications infrastructure. Energoatom—Ukraine’s nuclear power authority—and Ukrenergo operate their own extensive fiber-optic communications networks for relay protection, emergency automation, communications between facilities, and other uses.⁴⁷ The extent of damage to these grid-specific systems versus public service provider infrastructure used for telephony and commercial internet functions is not clear. However, grid operators in many countries—including the United States—rely on both specialized and commercial communications to varying degrees.

Data from spring 2023 suggested a trend towards moderation—and even elimination—of supply shortages due to diminishing Russian military capacity and emergency restoration efforts aided by provision of globally-sourced equipment to Ukraine. In an April 2023 report, the Institute for the Study of War—a Washington, DC, think tank that has provided regular assessments of the Russian military campaign since the full-scale invasion—stated that the Russian infrastructure campaign had culminated in strategic failure as it did not force Ukraine to negotiate for peace.⁴⁸ October 2023 media reports indicated that Russia was in the early stages of a renewed infrastructure campaign expected to extend into winter.⁴⁹ Observers at the time voiced concerns

⁴⁴ From Ivan Borysenko, “How Can Ukraine Get Through Winter With its Power Grid Intact—Expert Interview,” *New Voice of Ukraine*, October 19, 2022, <https://english.nv.ua/amp/how-can-ukraine-get-through-winter-interview-50277948.html>.

⁴⁵ International Energy Charter, Cooperation for Restoring the Ukrainian Infrastructure Project Task Force, *Ukrainian Energy Sector Evaluation and Damage Assessment-IV*, Brussels, Belgium, 2023, p. 4.

⁴⁶ “European Companies Asked to Urgently Donate Spare Parts to Repair Ukraine’s Power Grid,” *EuroNews*, November 2, 2022, <https://www.euronews.com/2022/11/29/european-companies-asked-to-urgently-donate-spare-parts-to-repair-ukraines-power-grid>. Ukraine began commercial electricity export to EU countries in June 2022, exporting \$542.5 million worth of electricity before Russian attacks forced cessation of exports. Ukraine began importing small volumes of electricity from the European Network of Transmission System Operators (ENTSO-E) in January 2023. See *ibid.*, p. 15.

⁴⁷ “Ukrenergo Launched a Large-Scale Telecommunications Network Reconstruction Project,” *Kosatka Media*, December 2019, <https://kosatka.media/en/category/elektroenergiya/news/ukrenergo-nachalo-masshtabnyy-proekt-po-rekonstrukcii-telekommunikacionnoy-seti>; and International Telecommunications Union, *Interim Assessment on Damages to Telecommunications Infrastructure and Resilience of the ICT Ecosystem in Ukraine*, Geneva, December 2022, p. 21, [https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine -2022-12-22_FINAL.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf).

⁴⁸ Karolina Hird, et al., *Russian Offensive Campaign Assessment*, Institute for the Study of War, Washington, DC, April 8, 2023, <https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-8-2023>.

⁴⁹ David L. Stern, “In Ukraine, Russia’s Winter Attacks on Infrastructure Have Started,” *Washington Post*, October 10, 2023, <https://www.washingtonpost.com/world/2023/10/10/winter-ukraine-russia-infrastructure-attacks/>.

that Ukraine lacked reserve capacity in case of future Russian strikes in winter 2023-2024.⁵⁰ After renewed Russian missile attacks on hydroelectric and other energy facilities in early 2024, Ukrainian leaders told congressional leaders that replenishment of stocks of U.S. supplied air defense systems and missiles was urgently needed to protect electricity infrastructure.⁵¹

Economic Effects

Even prior to 2022, the Ukrainian electricity sector had structural economic flaws characteristic of many post-Soviet states: excessive non-payments and customer arrears; extensive price controls and cross-subsidization; high levels of bad debt; inefficiency; and underinvestment in the infrastructure base. According to critics, the existing system was riven with opaque ownership structures, with many hybrid business entities mixing state and private-sector ownership. As such, the regulatory framework tended to safeguard political and economic privileges of connected individuals at the expense of overall sector performance, according to observers.⁵²

War damage and population displacements have badly eroded the industrial base and national economy of Ukraine, exacerbating preexisting financial problems and forcing emergency measures that could delay reforms.⁵³ According to an estimate by the National Bank of Ukraine, nearly 90% of energy companies will not be able to service their debts due to physical destruction of assets and loss of their ratepayer bases.⁵⁴ The total loss of steel works destroyed in Mariupol by Russian forces and disruption of associated supply chains lowered demand for electricity—simultaneously easing pressure on the stressed national grid and depriving utilities of many major industrial customers. Even where industrial infrastructure remained intact, electricity shortages forced production stops in some cases. Surveys reported decreases in business confidence in industrial, trade, and services sectors.⁵⁵

Ukrainian Resilience to Infrastructure Attacks

Hostilities in Ukraine continue as of this writing. However, Ukrainian electricity infrastructure functions have thus far proved resilient in the face of persistent attacks. The following three subsections consider factors that played a role in ensuring resilience of cyber, physical, and economic infrastructure of electricity production and supply to end-users. Continuing challenges are also discussed.

⁵⁰ Andrian Prokip, “How Will Ukraine’s Energy Sector Fare in the Upcoming Winter?,” *The Wilson Center*, September 5, 2023, <https://www.wilsoncenter.org/blog-post/how-will-ukraines-energy-sector-fare-upcoming-winter>.

⁵¹ Isabelle Khurshudyan, Anastacia Galouchka, and Francesca Ebel, “Russia Strikes Power Plants in Heavy Blow to Ukrainian Electric Grid,” *Washington Post*, March 29, 2024, <https://www.washingtonpost.com/world/2024/03/29/ukraine-russia-airstrikes-energy-war/>. For an overview of Russian missile attack capabilities and Ukrainian defenses, see Ian Williams, *Putin’s Missile War: Russia’s Strike Campaign in Ukraine*, Center for Strategic and International Studies, *A Report of the CSIS Missile Defense Project*, Washington, DC, May 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230505_Williams_Putin_Missile.pdf.

⁵² The World Bank Group, *Electricity Reform in Ukraine*.

⁵³ Damage to industrial base, see ACAPS, *Ukraine: Impact of Conflict on the Ukrainian Economy: Implications for Humanitarian Needs*, Geneva, February 13, 2023, p. 2.

⁵⁴ International Energy Charter, *Ukrainian Energy Sector Evaluation and Damage Assessment-IV*, p. 8.

⁵⁵ *Ibid.*

Cyber Resilience

A potential appeal of cyberattacks from the attacker perspective is their presumed capacity to generate widespread impacts anonymously over unlimited distance at the relatively modest cost of developing and deploying malicious computer code. However, Russia did not demonstrate a capability to rapidly—or anonymously—deploy highly effective cyberattacks targeting critical infrastructure systems during the winter 2022-2023 infrastructure campaign.⁵⁶ In general, cyberattacks—either before or after the invasion—did not succeed in their apparent goal of permanently damaging critical systems and assets in the electricity sector to cause a widespread grid collapse.

Observers attribute these results to a combination of factors: (1) the timely actions of Ukrainian grid operators using manual override controls as described above; (2) increasing Ukrainian familiarity with, and awareness of, Russian threats; (3) errors by Russian attackers who may have lacked a full understanding of electric grid topologies, associated OT systems, and the electrical engineering necessary to manipulate ICS successfully; (4) a measure of luck aided by the inherent difficulties of designing and executing successful cyberattacks on complex ICS installations; and (5) technical assistance (including intelligence sharing) and financial support from Western and other foreign governments to Ukraine.⁵⁷

Following the April 2022 cyberattack, Viktor Zhora, the head of Ukraine's Computer Emergency Response Team (CERT), said, "We have been dealing with an opponent that has been constantly training us, drilling us. Since 2014 we've been under constant aggression, and our expertise is unique in how to rebuff this aggression. We're stronger. We're more prepared."⁵⁸

Ukrainian authorities have also benefited from support from allied governments and private sector entities. For example, Microsoft reported that it had provided more than \$400 million in technology assistance to Ukraine as of November 2022, including cybersecurity services.⁵⁹ In June 2022, CISA and its Ukrainian counterpart signed a memorandum of understanding (MOU) to expand the existing relationships for information sharing and best practices, critical infrastructure security technical exchanges, and cybersecurity training and joint exercises.⁶⁰ The

⁵⁶ See Bateman, *Russia's Wartime Cyber Operations in Ukraine*. Also, Mueller et al., *Cyber Operations During the Russo Ukrainian War: From Strange Patterns to Alternative Futures*, CSIS, Washington, DC, July 2023, <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>.

⁵⁷ For an example of U.S. military technical assistance, see U.S. Senate Committee on the Armed Services, Transcript, Hearing to Receive Testimony on the Posture of United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2023 and the Future Years Defense Program, pp. 51-53, April 5, 2022, Washington, DC, https://www.armed-services.senate.gov/imo/media/doc/22-21_04-05-2022.pdf. For information on intelligence sharing, see David Vergun, "Partnering with Ukraine on Cybersecurity Paid Off, Leaders Say," DOD News, December 3, 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/>; and Nick Beecroft, *Evaluating the International Support to Ukrainian Cyber Defense*, Carnegie Endowment for International Peace, Washington, DC, November 3, 2022, <https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322>.

⁵⁸ Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, April 12, 2022, <https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>.

⁵⁹ Brad Smith, "Extending our Vital Technology Support for Ukraine," *Microsoft on the Issues*, November 3, 2022, <https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/>.

⁶⁰ CISA, "United States and Ukraine Expand Cooperation on Cybersecurity," press release, July 27, 2022, <https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity>.

Department of Energy (DOE) has also supported cybersecurity work during this period as part of a broader assistance program for the Ukrainian energy sector.⁶¹

Technical analysis of Russian cyberattacks has uncovered errors in design and execution that betray weaknesses in tradecraft and relevant engineering knowledge.⁶² In general, OT systems represent a more variegated target to attackers than corporate IT systems. Russian hackers apparently struggled to fully understand interfaces between cyber and physical systems specific to their targets despite extensive clandestine reconnaissance of Ukrainian systems and some knowledge of electricity infrastructure, according to experts.⁶³

Emerging research suggests that cyberattacks targeting ICS face inherent limitations when used as an instrument of war or subversion.⁶⁴ Attacks against infrastructure OT systems often require extensive reconnaissance and industry-specific knowledge to successfully execute.⁶⁵ Hasty work by the adversary may lead to mistakes that heighten the chance of discovery by defenders, or—as in the case of the 2016 Russian cyberattack on the Ukrainian grid—contain errors typical of software that has not been properly tested to guarantee functionality. Likewise, anonymity—a key aspect of subversion—may be compromised, as was the case in the Russian attacks on Ukraine. Finally, more “virulent” malware designed to spread in networked systems may infect attacker systems or systems of third countries that possess means to retaliate.⁶⁶ Some experts note that Russia is trying to develop more modular and standardized malware that can be more rapidly and widely deployed to target ICS.⁶⁷

Physical Resilience

The Ukrainian grid proved vulnerable to physical attacks conducted at scale by Russian forces. Lengthy and often unscheduled outages covering large areas disrupted industrial production and other critical infrastructure functions during the winter months of 2022-2023. However, system resilience was sufficient to forestall a complete or otherwise unrecoverable collapse of the grid. Ukrainian authorities restored critical functions of power supply across most of the country as Russian military resources were exhausted or redirected to other priorities.

Several factors may have contributed to Ukrainian success in limiting the time and scope of the acute crisis, and ensuring a relatively rapid recovery of critical power supply functions.

⁶¹ U.S. Department of State, “Energy Security Support to Ukraine,” press release, November 29, 2022, <https://www.state.gov/energy-security-support-to-ukraine/>.

⁶² Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event*.

⁶³ Ibid.

⁶⁴ For example, Lennart Maschmeyer, “The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,” *International Security*, vol. 46, no. 2 (Fall 2021); and Erica D. Borghard, and Shawn W. Lonergan, “Cyber Operations as Imperfect Tools of Escalation,” *Strategic Studies Quarterly* 13, no. 3 (2019), <https://www.jstor.org/stable/26760131>.

⁶⁵ See Bateman, *Russia's Wartime Cyber Operations in Ukraine*.

⁶⁶ Maschmeyer, “The Subversive Trilemma.” One example of unintended effects with potential geopolitical ramifications is the Russian attack on the Viasat satellite communications network in Ukraine an hour before the 2022 invasion—one of the few known effective cyberattacks on Ukrainian critical infrastructure during the war. The resulting loss of communications functions affected the operation of German wind turbines hundreds of miles away. See Patrick Howell O’Neill, “Russia Hacked and American Satellite Company One Hour Before the Ukraine Invasion,” *MIT Technology Review*, May 10, 2022, <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

⁶⁷ Dragos: ELECTRUM Threat Group Operations, <https://www.dragos.com/threat/electrum/>.

- Stockpiling and sparing: Ukraine stockpiled spare equipment and constructed reserve control facilities before the invasion, according to the head of Ukrenergo.⁶⁸
- Excess generation and transmission capacity from Soviet legacy infrastructure: Availability of excess capacity—a cost liability in peacetime—may have facilitated preservation of grid functions. According to Ukrainian officials quoted in the *Wall Street Journal*, “The energy system had a major strength inherited from Soviet times, say energy officials: Capacity was far higher than needed. Ukraine once housed a large part of the Soviet Union’s industrial base. As a result, all parts of the grid had backups built in, and every city could receive electricity by various routes.”⁶⁹
- Transmission capacity improvements: Ukraine began preparing for integration with the European grid in 2017 by refurbishing parts of its domestic grid. Old equipment was replaced, power lines were refurbished, and new lines were installed.⁷⁰ The ability to reroute available supply over multiple pathways helped keep the grid running.
- Interconnection with the European grid: With the onset of full-scale war, Ukraine accelerated integration with the European power grid—the crisis apparently prompting European system operators to achieve consensus and accept risks to their own national grids that might have been unacceptable in peacetime.⁷¹ Although initial Ukrainian interconnection transmission capacity was fairly modest, import capacity had increased to 700 MW—roughly the capacity of a single coal-fired power plant—by February 2023, with export capacity reaching 400 MW during the same period. Russian attacks forced cessation of electricity exports to Europe in October 2022. However, these resumed in April 2023, with capacity expected to increase gradually thereafter according to ENTSO-E.⁷² As of February 2024, the Ukrainian export capacity limit to Europe was 550 MW.⁷³ The diminished domestic consumer base increased reliance on export sales as a

⁶⁸ Robert Walton, “After Months of Russian Attacks, Ukraine’s Grid Resumes Electricity Exports to EU. How Did It Survive,” *Utility Dive*, April 12, 2023, <https://www.utilitydive.com/news/after-months-of-russian-attacks-ukraines-grid-resumes-electricity-exports/647359/>.

⁶⁹ Walker and Trofimov, “Russia Tried to Freeze Ukraine.” This runs counter to the IEA assessment quoted in this report (see “Ukrainian Pre-Invasion Transmission Network”).

⁷⁰ Borysenko, “How Can Ukraine Get Through Winter.”

⁷¹ Anna Blaustein, “How Ukraine Unplugged from Russia and Joined Europe’s Power Grid with Unprecedented Speed,” *Scientific American*, March 22, 2022, <https://www.scientificamerican.com/article/how-ukraine-unplugged-from-russia-and-joined-europes-power-grid-with-unprecedented-speed/>; and Gregory Barber, “The Race to Rescue Ukraine’s Power Grid from Russia,” *Wired*, March 10, 2022, <https://www.wired.com/story/the-race-to-rescue-ukraines-power-grid-from-russia/>.

⁷² ENTSO-E, “Further Increase in the Trade Capacity with the Ukraine/Moldova Power System,” press release, April 19, 2023, <https://www.entsoe.eu/news/2023/04/19/further-increase-in-the-trade-capacity-with-the-ukraine-moldova-power-system/>; and ENTSO-E, “ENTSO-E Announces Further Support to Ukraine Through a New Agreement on Emergency Energy Assistance and Increased Electricity Trading Capacity,” press release, March 29, 2023, <https://www.entsoe.eu/news/2023/03/29/press-release-entso-e-announces-further-support-to-ukraine-through-a-new-agreement-on-emergency-energy-assistance-and-increased-electricity-trading-capacity/>.

⁷³ ENTSO-E, “Further Increase in the Trade Capacity with the Ukraine/Moldova Power System,” press release, February 28, 2024, <https://www.entsoe.eu/news/2024/02/28/further-increase-in-the-trade-capacity-with-the-ukraine-moldova-power-system/>.

source of funding. Ukrainian experts said that revenue from sales to Europe will be used to fund ongoing repairs to the grid.⁷⁴

- Adaptation, improvisation, and operational learning: Exposure to Russian attacks over nearly a decade apparently informed planning efforts in advance of the infrastructure campaign in late 2022. Ukrenergo modeled “how the power grid would work at different levels of destruction,” according to its chief executive. This experience and planning apparently informed recovery operations.⁷⁵ Ukrenergo also claimed installation times of LPTs improved drastically, moving from 2-3 months typical in peacetime to 3-4 days during the campaign.⁷⁶
- Availability of emergency communications for grid management: On at least one occasion, the Starlink low-Earth orbit satellite constellation provided resilient communications that enabled restoration of electricity supply after attacks on ground-based communications infrastructure, according to a senior Ukrainian official.⁷⁷ Media reports imply numerous complex black start operations during the Russian campaign. Black start operations repower major grid interconnections after outages, and are regarded in the industry as being among the most complex grid operations. They require real-time assessments of grid assets, identification, and control of transmission pathways to repower generation facilities, and sequencing and coordination of complex procedures over a distributed network operated by numerous grid entities.⁷⁸
- Efficiency improvements: In 2023, EU sponsored a program to provide five LED lightbulbs in exchange for the same number of conventional bulbs from every Ukrainian household.⁷⁹ The EU Delegation to Ukraine predicted that the program will reduce electricity consumption by 7-10%, or 1 GW, during peak hours.
- Use of multinational expertise and emergency procurement assistance: The U.S. Department of Energy provided technical assistance through the National Laboratories based on a decade-long partnership with Ukrainian counterparts, which was used for planning grid synchronization with Europe and for making real-time damage assessments after Russian missile strikes.⁸⁰ The U.S. Department of State provided assistance with U.S. and international sourcing of

⁷⁴ Video: UATV English, “Ukraine Resumed Electricity Exports Amid Russian Shelling: Putin Can’t Break Ukraine’s Energy System,” <https://www.youtube.com/watch?v=hVollSRZjEk>. (See comments at 3:50 mark).

⁷⁵ Walton, “After Months of Russian Attacks, Ukraine’s Grid Resumes.”

⁷⁶ Bateman, *Russia’s Wartime Cyber Operations in Ukraine*.

⁷⁶ See Walker and Trofimov, “Russia Tried to Freeze Ukraine.”

⁷⁷ “Starlink Helped Restore Energy, Communications Infrastructure in Parts of Ukraine—Official,” *Reuters*, October 12, 2022, <https://www.reuters.com/world/starlink-helped-restore-energy-communications-infrastructure-parts-ukraine-2022-10-12/>.

⁷⁸ Walker and Trofimov, “Russia Tried to Freeze Ukraine.” For background on black start operations, see NREL: Black Start, <https://www.nrel.gov/grid/black-start.html>.

⁷⁹ According to DOE, Light-Emitting Diode (LED) bulbs use 75% less energy than equivalent incandescent bulbs. See DOE: LED Lighting, <https://www.energy.gov/energysaver/led-lighting>.

⁸⁰ See U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Energy, *Statement of Jason Fuller, Chief Energy Resilience Engineer, Electricity Sector, Pacific Northwest National Laboratory*, 118th Cong., 1st sess., March 23, 2023, p. 4, <https://www.congress.gov/118/meeting/house/115530/witnesses/HHRG-118-SY20-Wstate-FullerJ-20230323.pdf>.

- replacement equipment for the Ukrainian grid in partnership with other nations and international organizations.⁸¹
- Hardening of key assets: Authorities used physical barriers to protect critical elements of key substations against missile attack.⁸²
 - Dispersion: Installations of rooftop solar and residential battery storage systems increased during the bombing campaign due to a spike in consumer demand, providing limited service in some blacked-out areas, according to media reports.⁸³

Persistent resilience challenges remain. The condition of Ukraine's grid was still precarious going into the winter of 2023-2024, according to observers.⁸⁴ The ability to restore power following Russian attacks was largely due to operational measures rather than comprehensive repair of infrastructure.⁸⁵ Further, as of this writing, Ukraine remained largely reliant on foreign assistance, as domestic manufacturing capacity remained limited. Additional risk may result from Ukrainian reliance on a few centralized nuclear and hydroelectric facilities for large-scale generation—a pre-war feature of the Ukrainian grid that destruction or damage of fossil-fuel powered generation plants has exacerbated.

Availability of replacement LPTs in an emergency has long been a concern of infrastructure planners globally. Lead times and costs rose rapidly in 2022. Ukrenergo reported that LPTs were difficult to procure globally during the bombing campaign. “It’s obvious no one is ready,” the head of Ukrenergo said.⁸⁶ U.S. power executives interviewed by a trade publication in December 2022 said that procurement times for new distribution transformers were more than a year—up from three months in 2020, with average costs up two or threefold over the same period.⁸⁷ While the availability of LPTs used to step-up voltage for long-distance transmission has long been a concern to industry observers, the tight supply of transformers used for local distribution is a recent concern, according to the U.S. executives.

The Ukrainian government postwar recovery plan, published in July 2022, calls for several electricity-related resilience initiatives to close known gaps. The plan calls for expansion of the synchronized grid interconnection with ENTSO-E, and investing in “anti-missile security of assets in Ukraine [and] war-proof design” of energy assets. Additionally, it calls for rebuilding of major hydroelectric installations damaged during the war and major investments in other renewables. Ukrainian experts and government officials have advocated for increased use of renewables both for purposes of alignment with EU membership requirements and creating a more distributed and difficult-to-target generation network.⁸⁸ The recovery plan also foresees

⁸¹ U.S. Department of State, “Energy Security Support to Ukraine.” Also NREL, “Ukraine Fights to Build More Resilient, Renewable Energy System in Midst of War,” press release, July 27, 2023, <https://www.nrel.gov/news/features/2023/ukraine-fights-to-build-a-more-resilient-renewable-energy-system-in-the-midst-of-war.html>.

⁸² Walton, “After Months of Russian Attacks, Ukraine’s Grid Resumes.”

⁸³ Sara Schonhardt, “Ukrainians Shift to Renewable Power for Energy Security Amid War,” *E&E News*, March 1, 2023, <https://www.scientificamerican.com/article/ukrainians-shift-to-renewable-power-for-energy-security-amid-war/>.

⁸⁴ U.N. Development Program, *Towards a Green Energy Transition in Ukraine*.

⁸⁵ Anonymous, “As the War on the Power Sector Rages On, Tides Could be Turning in Favor of Ukraine,” *Power Grid International*, February 20, 2023, <https://www.power-grid.com/td/as-the-war-on-the-power-sector-rages-on-tides-could-be-turning-in-favor-of-ukraine/#gref>.

⁸⁶ Walton, “After Months of Russian Attacks, Ukraine’s Grid Resumes.”

⁸⁷ Robert Walton, “Utilities Sound Alarm Over Distribution Transformer Shortage as Procurement Times Surpass 1 Year and Costs Triple,” *Utility Dive*, December 19, 2022, <https://www.utilitydive.com/news/distribution-transformer-shortage-appa-casten/639059/>.

⁸⁸ Anonymous, “Tides Could Be Turning.”

major investment in more efficient housing stock to reduce the electricity sector's energy intensity, following expert recommendations.⁸⁹ Many of the residential buildings and enterprises in Ukraine date to the Soviet era and were not designed for energy efficiency.

Economic Resilience

The regulatory framework and market mechanisms that facilitate the production and sale of electricity in Ukraine were undergoing reforms at the time of the Russian invasion. Reforms anticipated eventual integration of the national electricity market with the European regional market, along with regulatory harmonization. The President of Ukraine declared martial law on February 24, 2022, which halted many pre-war market and regulatory reform initiatives. Subsequent legislative and regulatory changes prioritized security of supply and consumer access over market regulatory reforms. Measures included continuation of existing public-service obligations requiring utilities to provide electricity to consumers at a fixed price, and a suspension of household disconnection for non-payment and penalties for arrears.⁹⁰

The resulting shortfalls in revenue from consumer protection measures were partially covered by profits from electricity exports to ENTSO-E countries, although the amount of electricity traded has been relatively modest and subject to disruption from Russian attacks.⁹¹ Seizure of certain Russian-owned assets in the electricity industry has also provided some revenue.⁹² Nonetheless, these amounts did not cover losses. In 2022, the European Bank for Reconstruction and Development (EBRD) repurposed €147.3 million in existing loans to Ukrenergo to provide emergency liquidity. The funds were originally purposed for upgrading transmission infrastructure and for harmonization of operational and legal framework with European electricity networks.⁹³ The emergency liquidity provided for short-term needs, but at the expense of longer-term priorities for economic stabilization of the sector.

Lessons Learned: Implications for U.S. Grid Resilience

The Ukrainian wartime experience with grid resilience and restoration includes many extreme edge cases that have rarely, if ever, been encountered by the U.S. electricity sector. Further, the Ukrainian experience is prolonged, unfolding over nearly a decade against a persistent and determined adversary. For Ukrainian grid operators, return to unobstructed steady state operations is a practical impossibility during active hostilities. By necessity, Ukraine must continue— indefinitely, or until the cessation of hostilities—to maintain and continually re-establish critical functions of production, transmission, distribution, and sale of electricity with degraded resources in a persistent high-threat environment.

⁸⁹ Dixi Group, *Priorities for Ukraine's Post-War Energy Recovery: Summary of the Discussion*, Issue #2, https://dixigroup.org/wp-content/uploads/2022/11/supboard_2022_10_upd_clean-1.pdf.

⁹⁰ Task Force Cooperation for Restoring the Ukrainian Energy Infrastructure, *Key Legal Developments in Ukraine's Energy Sector*, I (February 24, 2022 to October 20, 2022), Kyiv, 2022, pp. 8-9, https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2022_10_26_Legal_developments_in_Ukraine_s_energy_sector.pdf.

⁹¹ *Ibid.*, p. 13.

⁹² *Ibid.*, p. 14.

⁹³ European Bank for Reconstruction and Development, "EBRD Supports Ukraine Electricity Company With €97.3 Million of Finance," press release, August 26, 2022, <https://www.ebrd.com/news/2022/ebd-supports-ukraine-electricity-company-with-973-million-of-finance.html>.

Ukrainian mitigation of attrition risks prior to the war, as well as subsequent response, recovery, and sustainment activities, highlighted the complex interrelationships and dependencies between society, governance, the economy, and physical or digital infrastructure systems. The Ukrainian electricity sector had several known vulnerabilities prior to the 2022 invasion—i.e., inefficient and highly centralized legacy systems and assets on the supply and demand side of the electricity sector; weaknesses in finance and governance; reliance on an outdated production base (partially controlled by a likely adversary) for replacement equipment; and the political risk of integration of its national grid with the Soviet-legacy grid controlled by Moscow.

Ukraine partially mitigated these risks through limited investments in grid efficiency and distributed energy resources, stockpiling programs, governance and market reforms, and preparation for synchronization and integration with the European grid. Additionally, during the more limited phase of conflict between 2014 and 2022, Ukraine gained experience in countering Russian cyber and physical attacks on the grid, and modeling possible future attack profiles in order to inform investments in response capabilities.

In general, resilience outcomes between sustained operations and system-wide collapse appear to have been decided on the margins in many cases. Pre-invasion Ukrainian resilience investments did not forestall wartime grid emergencies, but may have allowed authorities time and space for improvisation and adaptation to compensate for gaps and vulnerabilities as they were exposed by Russian attacks, ensuring the continued functioning of the system.

For example, synchronization with the European grid—however tentative—provided a source of grid stabilization and export earnings that helped preserve the physical and financial viability of the electricity sector that was burdened by payment arrears and inefficient ownership structures even before the war, giving Ukrainian authorities time to seek financial support and equipment donations from foreign partners. Pre-invasion stockpiling programs may have eased wartime demands for global sourcing of replacement equipment from pandemic-stressed supply chains. Likewise, pre-invasion investments in lowering the energy intensity of the grid did not fully resolve legacy issues, but may have been sufficient to provide time for the EU's LED bulb exchange initiative and private residential installations of solar and battery storage systems to make a meaningful reduction in load on the highly stressed national grid.

In sum, Russian attacks on the Ukrainian grid highlighted several characteristics that factored into grid resilience:

- financial, social, and economic health of supply and demand side entities (e.g., industrial, and residential electricity consumers),
- sector cybersecurity culture,
- sector preparedness (risk modeling, exercises, incident response assets),
- grid topology and geography (geographical placement of generation, transmission, and distribution assets as a component of risk exposure—i.e., proximity to allied or hostile states, or exposure to natural hazards),
- grid network structure (synchronization, interconnection of grid assets, and power transfer capacity between major national and regional interconnections),
- redundancy and resilience of critical systems for grid visibility and flexibility (communications, electronic energy management systems, power transformers),
- availability of critical replacement equipment and parts,
- grid energy intensity, and
- international partnerships.

The following sections discuss how these characteristics may relate to the U.S. context.

Potential Gaps in U.S. Preparedness

The extent to which U.S. federal agencies and industry partners have prepared to sustain grid operations against persistent threats for extended periods while suffering attrition of key grid assets is not clear.⁹⁴ Both real incidents and exercise scenarios have tended to be presented as discrete and anomalous events starting from a baseline of full or near-full functionality, rather than from a degraded state due to previous hazard events. For example, a major grid exercise conducted in the United States by the Electricity Information Sharing and Analysis Center (E-ISAC) in 2021 presented a scenario that included sophisticated cyber and physical attacks carried out by an unnamed hostile nation-state over a two-day period, with a return to unobstructed steady state operations within two weeks.⁹⁵ Further, according to experts many technical assessments of grid resilience may not adequately account for human behavior and decisionmaking, cascading effects of events over time, or interactions between social and engineered systems.⁹⁶

As the Ukrainian case illustrates, attritional conflicts involve hostile—and perhaps irrational—human decisionmaking and behavior, and may unfold over an extended period. Continuing attacks on infrastructure by a variety of conventional and unconventional means may incrementally degrade infrastructure via multiple failure modes to the point of collapse. Other phenomena, such as the increasing severity and incidence of weather events caused by climate change, space weather, or electromagnetic pulse attacks during a nuclear exchange, may also present attritional threats to the grid that defy simple analyses based on static probabilities.⁹⁷

Russian Capabilities and Limitations

The Russian infrastructure attacks on Ukraine over the course of nearly a decade provide information about Russian capabilities and limitations in both cyber and physical domains. When developing cyberattacks on the Ukrainian grid, Russian entities operated with advantages against a (presumptively) weaker defender that would not obtain in a conflict with the United States—

⁹⁴ For the purposes of this report, attrition may be defined as the progressive reduction in the number and function of critical infrastructure systems, assets, and networks over time due to hostile action or other causes.

⁹⁵ North American Electric Reliability Corporation (NERC) and Electricity Information and Analysis Center (E-ISAC), *GridEx VI: Lesson's Learned Report*, Atlanta, GA, April, 2022, <https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20VI%20Public%20Report.pdf>. Government and industry stakeholders conduct preparedness exercises that simulate effects of widespread electricity outages from a variety of causes. E-ISAC is hosted by the NERC, an industry non-profit that develops and enforces mandatory reliability standards for the bulk electricity system under auspices of the Federal Energy Regulatory Commission, an independent DOE agency. Major exercises are conducted by NERC, DOE, FEMA, Department of Defense (DOD: USCYBERCOM and National Guard/Reserves), and DOD's Defense Advanced Research Projects Agency. (Source: National Academies of Sciences, Engineering, and Medicine). The 2019 DOE Clear Path VII and FEMA Shaken Fury 2019 exercises presented the scenario of a major earthquake in the Mississippi River Valley region, affecting multiple infrastructure sectors over a nine-day period. The Federal Bureau of Investigation exercise 2015 workbook presented several scenarios of long-term power outages (1-12 months) resulting from a single catastrophic event. See George Baker III et al., *Triple Threat Power Grid Exercise*, InfraGard National EMP SIG TTX Planning Team, High-Impact Threats Workshop and Tabletop Exercises Examining Extreme Space Weather, EMP and Cyber Attacks, Washington, DC, 2015.

⁹⁶ Laura Leddy et al., *Measuring and Valuing Resilience: A Literature Review for the Power Sector*, NREL, Golden, CO, August 2023, p. 20, <https://www.nrel.gov/docs/fy23osti/87053.pdf>.

⁹⁷ See CRS Video WVB00557, *Policy Options to Address Energy Transition, National Security, and Climate Change*, by Brent D. Yacobucci, Corrie E. Clark, and Ashley J. Lawson; and CRS Report R47339, *Ensuring Electricity Infrastructure Resilience Against Deliberate Electromagnetic Threats*, by Brian E. Humphreys.

i.e., geographic proximity, experience with legacy systems, and a well-developed network of Russian-speaking collaborators—and yet were not able to generate or sustain desired effects. Nonetheless, the cyberattacks demonstrated techniques that may improve over time and be integrated with other types of attacks as a part of hybrid or open warfare in potential future conflicts.

Physical attacks proved to be much more effective, but were also subject to resource constraints—i.e., the availability of missiles capable of penetrating Ukrainian air defenses—and conflicting military priorities over the longer term.⁹⁸ Whether using cyber or physical methods, Russia timed attacks to exploit periods of vulnerability during major technical upgrades, and prioritized electricity transmission and distribution infrastructure—both within Ukraine, and between Ukraine and European markets—to limit grid flexibility and increase the probability of a general grid collapse. Events in Ukraine suggest that there are limits on the frequency, duration, and severity of both cyber and physical attacks. Even capable and well-resourced threat actors may fail to effectively combine cyber and physical capabilities against resilient systems.

Potential Attrition Risks to the U.S. Electricity Sector and Mitigation Considerations

Several possible parallels between the Ukrainian experience and management and attritional threats to the U.S. electricity sector can be drawn from the above analysis, despite significant differences in geography, governance, the economy, and technology. The subsections below consider possible sources of vulnerability and resilience in the U.S. electricity sector in the context of attrition. Further, the analysis below considers how other policy goals—such as the provision of social benefits to eligible recipients, or increasing domestic industrial production—may affect grid infrastructure vulnerability and resilience.

Industrial Base Capacity, Supply Chain Security, and Stockpiling

Some U.S. utilities assert that they face LPT and distribution transformer shortages due to a combination of historical supply constraints, the impacts of the 2019 novel coronavirus (COVID-19) pandemic, and severe weather events. Transformer supply challenges include access to emergency transformer reserves, domestic manufacturing capacity, and the availability of specialty steel. Further, long-term grid emergencies in the context of attritional conflict may take available domestic production assets offline that might otherwise be used to replace losses of grid equipment, or else disrupt international supply chains (see “Economic Effects” section).⁹⁹

In the past, interest among policymakers focused mostly on LPTs used in bulk power transmission. A 2014 Department of Energy (DOE) study found that the United States had “limited production capability to manufacture LPTs” and that “if several LPTs were to fail at the same time, it could be challenging to quickly replace them.”¹⁰⁰ DOE’s 2015 Quadrennial Energy Review (QER) concluded that, for LPTs, “the lack of off-the-shelf transformer options and

⁹⁸ Resource constraints may operate on both sides of the conflict, as seen in the March 2023 missile attack on a hydroelectric dam that temporarily left the Ukrainian city of Kharkiv in darkness.

⁹⁹ For more information on LPTs and grid resilience, see CRS Insight IN12048, *Electric Power Transformers: Supply Issues*, by Paul W. Parfomak.

¹⁰⁰ DOE: Office of Electricity Delivery and Energy Reliability, *Infrastructure Security and Energy Restoration*, April 2014 Update, Washington, DC, April 2014, p. 31, <https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf>.

industry practice of as-needed manufacturing is an ongoing concern” and recommended that DOE develop a critical LPT reserve of emergency spares.¹⁰¹

Over the past few years, concerns about transformer supplies have extended to smaller units used in local distribution networks. For example, an August 2022 survey by the American Public Power Association found that “production of distribution transformers is not meeting current demand” and that “many public power utilities are at a high risk of stocking out on transformers.”¹⁰² An Edison Electric Institute official stated at the time that supply constraints were even greater for smaller, distribution-level transformers than for LPTs. Some smaller utilities have reported that lead times for orders of distribution transformers grew from a few months in 2020 to well over a year in 2022, and that unit prices have increased by up to 400% or more.¹⁰³

In June 2022, President Biden issued a memorandum allowing DOE to use Defense Production Act (50 U.S.C. §§4501 et seq.) authority to increase domestic production of transformers, among other electrical equipment.¹⁰⁴ DOE states that it subsequently has held listening sessions with stakeholders and has published an associated Request for Information.¹⁰⁵ DOE also has joined with the Electricity Subsector Coordinating Council to establish a “Supply Chain Tiger Team” to identify supply chain challenges and potential solutions for grid components, including transformers.¹⁰⁶ The Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) required DOE to assess the potential development and storage of an inventory of LPTs and to provide an update of related industry efforts.¹⁰⁷ An August 2023 GAO report, “Electricity Grid: DOE Could Better Support Industry Efforts to Ensure Adequate Transformer Reserves,” noted these DOE initiatives, but found that DOE officials had not yet “identified actionable objectives, or time frames” to advance stated goals.¹⁰⁸ Some stakeholders voiced concerns that federal stockpiling might aggravate supply chain constraints.¹⁰⁹

Some legislative proposals in the 118th Congress would encourage domestic manufacturing of LPTs and other transmission system materials and equipment, prohibit use of certain equipment manufactured by potential U.S. adversaries, and limit agency rulemakings affecting LPT

¹⁰¹ The White House: Quadrennial Energy Review Task Force, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, Washington, DC, April 2015, p. 2-12, https://www.energy.gov/sites/prod/files/2015/07/f24/QUER%20Full%20Report_TS%26D%20April%202015_0.pdf.

¹⁰² Paul Ciampoli, “APPA Survey of Members Shows Distribution Transformer Production Not Meeting Demand,” *Public Power Association*, October 12, 2022, <https://www.publicpower.org/periodical/article/appa-survey-members-shows-distribution-transformer-production-not-meeting-demand>.

¹⁰³ “Transformer Shortages and Price Spikes,” *Jefferson County Public Utility District*, <https://www.jeffpud.org/transformer-shortages-price-spikes/>.

¹⁰⁴ Presidential Determination No. 2022-19, “Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as Amended, on Transformers and Electric Power Grid Components,” 87 *Federal Register* 35079, June 9, 2022.

¹⁰⁵ DOE Office of Policy, “DOE Actions to Unlock Transformer and Grid Component Production,” October 22, 2022, <https://www.energy.gov/policy/articles/doe-actions-unlock-transformer-and-grid-component-production>; and DOE Office of Manufacturing and Energy Supply Chains, “Defense Production Act: Request for Information.”

¹⁰⁶ Derrill Holly, “Tiger Team: Electric Co-op Leaders Join Effort to Ease Supply Chain Problems,” *NRECA*, <https://www.electric.coop/tiger-team-electric-co-op-leaders-join-effort-to-ease-supply-chain-problems>.

¹⁰⁷ See § 40103(d), 135 Stat. 429, 929 (2021). According to GAO, as of July 2023, DOE has not conducted the assessment or issued the report.

¹⁰⁸ U.S. Government Accountability Office, *Electricity Grid: DOE Could Better Support Industry Efforts to Ensure Adequate Transformer Reserves*, August 2023, <https://www.gao.gov/assets/gao-23-106180.pdf>.

¹⁰⁹ *Ibid.*, p. 14.

efficiency (which some believe would exacerbate current supply chain constraints).¹¹⁰ The Facilitating the Reshoring of Energy Grid Component Manufacturing Act of 2023 (S. 34) would establish a DOE loan program to expand domestic manufacturing of grain-oriented electrical steel, or GOES—a specialized alloy used in LPT manufacture, LPTs, distribution transformers, and other electric grid components. The Protect American Power Infrastructure Act (S. 1050) would prohibit certain transactions that involve using equipment used in bulk-power system substations, control rooms, or power generating stations to provide power for defense critical electric infrastructure in the United States if a foreign adversary owns or exercises influence over the equipment.

The Protecting America's Distribution Transformer Supply Chain Act (H.R. 4167) would prohibit DOE from revising existing energy conservation standards for distribution transformers in electric power systems for the next five years. Proponents of this prohibition argue that such rulemakings would disrupt domestic supply chains and increase manufacturing lead times for domestic distribution transformers.¹¹¹

Economic Resilience

In this report, economic resilience refers to the ability of grid entities to finance business operations that support maintenance—or recovery and restoration—of grid infrastructure during a major crisis. Background conditions in any given service area, such as geography, economic conditions, ratepayer vulnerability, market structure, and regulation may affect economic resilience. In Ukraine, Russian attacks deprived utilities of customers and diminished the economic viability of the remaining electricity customer base, even as political and economic considerations in Ukraine made arrears collections and rate increases impossible. The deteriorating situation was mitigated to a degree by foreign aid, payments from electricity exports to Europe, and electricity imports from Europe to make up shortfalls in domestic generation capacity (see “Economic Effects” section).

Comparable grid disruptions are rare in the United States, but parallels exist in certain cases in which multiple extreme weather events struck vulnerable communities one after the other. For example, in 2005 Hurricane Katrina struck New Orleans and surrounding areas on the Gulf Coast, causing an estimated \$125 billion in damage.¹¹² Utilities faced major flooding of substations used for electricity transmission and distribution, and loss of communication infrastructure. Response was further complicated by damage to employees' homes and the forced evacuation of the major area utility's corporate headquarters, degradation of law and order, disease threats, contractor bankruptcies, fuel shortages, and logistics complications.¹¹³ Hurricane Rita then struck the same area weeks later, damaging transmission systems (including thousands of transformers) and generation facilities.

¹¹⁰ Discussion of DOE proposed efficiency standards for distribution transformers is in CRS Insight IN12179, *DOE's Proposed Regulation on Electricity Distribution Transformers*, by Martin C. Offutt.

¹¹¹ See Representative Richard Hudson, “Hudson Introduces Legislation to Protect Energy Supply Chain,” press release, July 16, 2023, <https://hudson.house.gov/press-releases/hudson-introduces-legislation-to-protect-energy-supply-chain>. In a January 2023 rulemaking notice, DOE argued that consumer cost-savings, health benefits, and environmental benefits justified the proposed increase in efficiency standards. See DOE, “Energy Conservation Program: Energy Conservation Standards for Distribution Transformers,” 88 *Federal Register* 1728, January 11, 2023.

¹¹² Richard D. Knabb, Jamie R. Rhome, and Daniel P. Brown, *Tropical Cyclone Report: Hurricane Katrina, 23-30 August 2005*, National Hurricane Center, Update, January 4, 2023, p. 13, https://www.nhc.noaa.gov/data/tcr/AL122005_Katrina.pdf.

¹¹³ Danny Taylor, *Louisiana Hurricanes Katrina and Rita Restoration/Recovery Electric Operations*, Entergy, Baton Rouge, LA, p. 8, February 21, 2006, https://www.lsu.edu/ces/conferences/rui2006/rui2006_taylor.pdf.

Although power was restored to most customers in the New Orleans area within 14 days of Katrina's landfall, 123,000 customers waited weeks more for restoration.¹¹⁴ In some areas with widespread destruction of residential neighborhoods—generally those with high preexisting poverty rates—immediate restoration was not possible.¹¹⁵ The uninsured infrastructure losses, combined with lost load caused by property loss and out-migration totaling nearly half the city's pre-storm population, created pressure for rate increases to finance restoration and recovery work.¹¹⁶ Infusions of federal aid on the supply side of the market to assist utilities moderated—but did not eliminate—pricing pressures. Entergy, the area's major utility, issued long-term corporate bonds to finance restoration and recovery, passing costs to ratepayers on monthly bills as a storm recovery surcharge for nearly a decade.¹¹⁷

More recently, many utilities were affected by the widespread economic disruptions caused by the COVID-19 pandemic that began in early 2020. Many utilities, local governments, and state governments implemented policies to suspend disconnections for nonpayment, known as disconnection moratoriums—a situation with parallels to wartime measures adopted in Ukraine (see “Economic” section) that contributed to a sharp rise in utility bill arrearages that may affect industry investment in infrastructure.¹¹⁸ Moratoriums generally postpone, but do not forgive, payment of utility bills by ratepayers. Congress has not directly addressed shutoffs or utility revenues in enacted pandemic relief legislation. Implementation of provisions of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136) may have the effect of reducing cases of utility bill nonpayment. For more information on COVID-19 disruptions to the U.S. electricity sector, see CRS Report R47417, *Electric Utility Disconnections*, by Ashley J. Lawson and Claire Mills.

Disaster Assistance

FEMA and the Small Business Administration (SBA) both administer post-disaster relief programs, which may serve to stabilize communities and prevent out-migration. The Federal Emergency Management Agency (FEMA) may, under the Stafford Act, aid public works (including nonprofit electric cooperatives) damaged in natural disasters under the Public Assistance (PA) Program.¹¹⁹ For-profit investor-owned utilities may be eligible to apply tax exemptions and other accounting mechanisms to certain recovery costs.¹²⁰ In cases of terrorist

¹¹⁴ Ibid., p. 15.

¹¹⁵ Entergy projected that 87,000 customers—nearly half of Entergy New Orleans Inc.'s customers—would be “unable to take service without demolition or significant reconstruction.” See *ibid.*, p. 6. For discussion of demographic characteristics of affected areas, see Elizabeth Fussell, Narayan Sastry, and Mark VanLandingham, “Race, Socioeconomic Status, and Return Migration to New Orleans After Hurricane KatriOkna,” *Population and Environment*, vol. 31 (December 11, 2009), pp. 20-42.

¹¹⁶ Taylor, *Louisiana Hurricanes Katrina and Rita Restoration*, p. 19.

¹¹⁷ Mark Ballard, “Entergy Customers to See Lower Electricity Bills Now That 2005 Hurricane Debt Paid Off,” *The Advocate*, August 1, 2018, https://www.theadvocate.com/baton_rouge/news/politics/entergy-customers-to-see-lower-electricity-bills-now-that-2005-hurricane-debt-paid-off/article_375ab88e-95b1-11e8-bf8e-6786a2504162.html.

¹¹⁸ See CRS Report R47417, *Electric Utility Disconnections*, by Ashley J. Lawson and Claire Mills. According to the National Governors Association, gas and electric utilities accumulated \$32 billion in arrears by the end of 2020 with “as many as 20% of households behind on utility payments.” See National Governors Association, *Memorandum on State Utility Disconnection Moratoriums and Utility Affordability*, Washington, DC, June 14, 2021, <https://www.nga.org/publications/memorandum-on-state-utility-disconnection-moratoriums-and-utility-affordability/>.

¹¹⁹ For more on program history and authorities, see CRS Report R46749, *FEMA's Public Assistance Program: A Primer and Considerations for Congress*, by Erica A. Lee.

¹²⁰ Bridgette Bourge, NRECA, “Federal Emergency Management Agency (FEMA) Disaster Assistance: Help Keep (continued...)”

attack, the list of incidents that qualify for a major disaster declaration is specifically limited, and it is not clear whether a terror or military attack on the grid would meet the legal definition of a major disaster if the incident involved something other than a fire or explosion, such as small-arms fire, an electromagnetic pulse, or a cyberattack.¹²¹ Additionally, investor-owned utilities may apply for funds provided to states through the Department of Housing and Urban Development (HUD) Community Development Block Grant (CDBG) Program, which may fund urgent community development needs such as restoration of utilities after natural disasters. Emergency appropriations are often made as a series of temporary expansions of the CDBG program, tailored to specific situations and authorized through appropriations acts—a process that may require lengthy agency rulemaking to establish administrative procedures for disbursement.¹²²

Affordability, Access, and Social Welfare

Federal and state low-income ratepayer assistance programs may reduce out-of-pocket costs for qualified ratepayers during steady state operations, which may incidentally expand the addressable market and stabilize utilities' ratepayer bases. At the federal level, the Low-Income Home Energy Assistance Program (LIHEAP), administered by the Department of Health and Human Services (HHS), provides block grants to states to assist low-income ratepayers with home heating and cooling costs.¹²³ A 2015 CRS report found that 22% of eligible persons received LIHEAP assistance.¹²⁴ Regular funding peaked in 2010 at \$4.5 billion. Funding in 2022 was \$3.8 billion, or \$2.8 billion in 2010 dollars.¹²⁵ However, Congress made supplemental appropriations for FY2023 for an additional \$2.3 billion.¹²⁶ Several committees have held hearings on electricity prices and affordability. Additionally, prices and affordability have been prominent topics of debate in the context of major energy bills in the 117th and 118th Congresses.¹²⁷

Not-For-Profit Electric Cooperatives' Rates Reasonable When Disaster Strikes," June 2016, https://www.electric.coop/wp-content/uploads/2016/03/fast_fact_fema_june_14_2016_update_final.pdf.

¹²¹ For more information on post-disaster aid and acts of terrorism, see CRS Report R44801, *Stafford Act Assistance and Acts of Terrorism*, by Bruce R. Lindsay. For more information on electromagnetic pulse hazards to the grid, see CRS Report R47339, *Ensuring Electricity Infrastructure Resilience Against Deliberate Electromagnetic Threats*, by Brian E. Humphreys. For more information on physical threats to the grid, see CRS Insight IN12074, *Electric Grid Physical Security: Recent Developments*, by Paul W. Parfomak. Operators of designated critical electricity infrastructure may be authorized to implement cost-recovery measures under 16 U.S.C. §824o-1 in the event of an electromagnetic pulse attack, geomagnetic storm, or physical attack on designated critical electricity infrastructure if the President authorizes a grid security emergency.

¹²² For more information, see CRS Report R46475, *The Community Development Block Grant's Disaster Recovery (CDBG-DR) Component: Background and Issues*, by Joseph V. Jaroscak.

¹²³ For more information, see CRS Report RL31865, *LIHEAP: Program and Funding*, by Libby Perl.

¹²⁴ See CRS Report R44327, *Need-Tested Benefits: Estimated Eligibility and Benefit Receipt by Families and Individuals*, by Gene Falk et al., p. 39.

¹²⁵ See Department of Health and Human Services, "Low-Income Energy Programs Funding History 1977-2022," https://liheapch.acf.hhs.gov/Tribes/energyprogs_history.htm. Adjusted figures calculated by CRS with Bureau of Labor Statistics online calculator, at <https://data.bls.gov/cgi-bin/cpicalc.pl>.

¹²⁶ See Dear Colleague Letter, Dr. Lanikque Howard, Office of Community Services, Administration for Children and Families, February 22, 2023, <https://www.acf.hhs.gov/ocs/policy-guidance/liheap-dcl-second-liheap-supplemental-grant-funding-release-ffy-2023>.

¹²⁷ See "Electricity Affordability" section in CRS Report R47521, *Electricity: Overview and Issues for Congress*, by Ashley J. Lawson.

Efficiency, Jobs, and the Environment

In recent decades, several energy-efficiency programs have been instituted to provide social benefits, create jobs, and protect the environment, although these may also have incidental energy security and resilience impacts by lowering energy intensity and stress on the grid.¹²⁸ The Energy Independence and Security Act of 2007 (P.L. 110-140) mandated efficiency standards for lightbulbs under Title III, “Energy Savings Through Improved Standards for Appliance and Lighting.” The DOE considered consumer costs, energy savings, emission reductions, and health impacts during the agency rulemaking.¹²⁹ In Ukraine, distribution of more efficient lightbulbs was regarded as an emergency measure to reduce load on the national grid during wartime (see “Physical” section).

DOE’s Weatherization Assistance Program (WAP) aids low-income recipients through block grants awarded to states. The program is designed to lower beneficiaries’ monthly energy bills through increased efficiency. In fiscal year (FY) 2021, WAP received an allocation of \$310 million.¹³⁰ The Inflation Reduction Act of 2022 (IRA; P.L. 117-169) created two Home Energy Rebate programs, providing a total of \$8.5 billion in funding to reduce consumer energy costs and support job creation. Funds are provided to states to “develop, implement, and enhance residential energy efficiency and electrification programs in U.S. households,” in order to lower monthly consumer bills and support job creation.¹³¹ An additional \$225 million will be made available to eligible tribal nations for the same purpose.¹³²

In June 2022, the White House announced an interagency initiative to promote adoption of modernized building codes to improve climate resilience and reduce energy costs.¹³³ The initiative includes guidance to DOE, HUD, and FEMA to leverage efficiency and disaster assistance programs to support increased adoption.¹³⁴ In general, domestic building codes and standards are developed and maintained by non-governmental standards-developing organizations, and are adopted and enforced variously by locale.¹³⁵ The general inefficiency of housing stock in Ukraine contributed to high energy intensity, which was a strategic liability during the height of the grid infrastructure attacks (see “Physical” section). In the United States, the efficiency of domestic housing stock—although higher than in Ukraine—might similarly

¹²⁸ According to the U.S. Energy Information Administration (EIA), U.S. energy intensity has—on average—decreased by more than half since 1983. See EIA, “U.S. Energy Intensity Has Dropped by Half Since 1983, Varying Greatly by State,” August 3, 2021, <https://www.eia.gov/todayinenergy/detail.php?id=48976>.

¹²⁹ See DOE, “Energy Conservation Program: Definitions for General Service Lamps,” 87 *Federal Register* 27461-27482, July 8, 2022.

¹³⁰ See CRS Report R46418, *The Weatherization Assistance Program Formula*, by Corrie E. Clark and Lynn J. Cunningham.

¹³¹ DOE, “Biden Harris Administration Opens Applications for States and Territories to Implement \$8.5 Billion for Home Energy Rebates as Part of Investing in America Agenda,” <https://www.energy.gov/articles/biden-harris-administration-opens-applications-states-and-territories-implement-85-billion>. Also see CRS Report R47698, *Home Energy Rebates from the Inflation Reduction Act of 2022, P.L. 117-169: Frequently Asked Questions*, by Martin C. Offutt.

¹³² *Ibid.*

¹³³ White House, “Biden-Harris Administration Launches Initiative to Modernize Building Codes, Improve Climate Resilience, and Reduce Energy Costs,” press release, June 1, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/01/fact-sheet-biden-harris-administration-launches-initiative-to-modernize-building-codes-improve-climate-resilience-and-reduce-energy-costs/>.

¹³⁴ For example, FEMA, *Building Codes Strategy*, Washington, DC, March 2022, https://www.fema.gov/sites/default/files/documents/fema_building-codes-strategy.pdf.

¹³⁵ For more on building codes and standards, see CRS Report R47665, *Building Codes, Standards, and Regulations: Frequently Asked Questions*, coordinated by Linda R. Rowan.

factor into grid resilience in the face of a prolonged crisis with progressive degradation of grid infrastructure.

Generation

In the United States, authority to set generation capacity requirements resides with state regulatory agencies, which balance consumer needs for affordable electricity against resilience objectives. Ukraine inherited a Soviet-era grid with excess reserve generation capacity. Although costly in terms of economic efficiency, the excess capacity later proved useful in the context of an attritional war that targeted grid infrastructure extensively. In the United States' more decentralized system, state regulatory agencies' adoption of reserve margins for generation capacity is guided by considerations of resilience objectives, risk tolerance, and cost.¹³⁶ Electricity policies and willingness to pay for excess capacity—varying widely among regions—may affect quantity and quality of investments in new generation capacity and other risk mitigations.¹³⁷

For example, the power outages in Texas during a severe cold weather event (Winter Storm Uri) in February 2021 prompted some observers to raise concerns that the highly-decentralized energy-only market in Texas led to underinvestment in generation assets able to withstand rare, but extreme, weather conditions.¹³⁸ Tom Fanning, a utility CEO and co-chair of the Electricity Sector Coordinating Council—an industry-led body that represents the private sector in federal public-private partnerships for critical infrastructure security and resilience—asserted that economic incentives for market participants predominated as the main factor influencing industry investment behavior. “If the rules of the market don’t reward someone for resilience, they won’t get resilience,” he said.¹³⁹ Texas’ decentralized energy-only market operated on a lower reserve margin than most of the rest of the country in the years leading up to the outage event.¹⁴⁰ Reserve

¹³⁶ NERC defines reserve margins as “the difference between available capacity and peak demand, normalized by peak demand shown as a percentage to maintain reliable operation while meeting unforeseen increases in demand (e.g., extreme weather) and unexpected outages of existing capacity.” See NERC: M-1 Reserve Margin, <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.

¹³⁷ For more on the relationship between market and regulatory structures, and reliability, see Jacob Mays et al., “Private Risk and Social Resilience in Liberalized Electricity Markets,” *Joule*, vol. 6 (February 16, 2022), pp. 369-380, and DOE, *Staff Report to the Secretary on Electricity Markets and Reliability*, Washington, DC, August 2017, https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf. Market-based regulations are not universally used in the United States. For information on ownership structure and regulation, see CRS Report R47521, *Electricity: Overview and Issues for Congress*, by Ashley J. Lawson. In 2023, DOE solicited a series of concept paper submissions on behalf of the Grid Deployment Office to address issues related to market design to meet a congressional mandate “to provide States and regions with technical and financial assistance related to developing, expanding, and improving wholesale electricity markets so that markets can contribute to an affordable, reliable, resilient, and equitable electric grid.” See DOE Grid Deployment Office, *Wholesale Electricity Market Studies and Engagements*, Funding Opportunity Announcement (FOA) Number: DE-FOA-000312, Washington, DC, 2023, pp. 1-2.

¹³⁸ Jacob Mays et al., “Private Risk and Social Resilience in Liberalized Electricity Markets,” *Joule*, vol. 6, no. 2 (February 16, 2022), pp. 369-380.

¹³⁹ “Southern CEO Looks to Steer Biden Away from Next Grid Crisis,” *E&E News: Energywire*, February 19, 2021, <https://subscriber.politicopro.com/article/eenews/1063725479>.

¹⁴⁰ Jacob Mays et al., “Private Risk and Social Resilience.” Also see Figure 1 in NERC, *2020 Long-Term Reliability Assessment (Hereinafter NERC 2020 LTRA)*, December 2020, p. 13, https://www.nerc.com/pa/RAPA/ra/Reliability/Assessments/DL/NERC_LTRA_2020.pdf. Energy-only markets compensate electricity producers solely for energy produced, relying on price signals to ensure adequate supply to consumers during spikes in demand or other contingencies.

margins in Texas then increased markedly between 2021 and 2024, in large part because of construction of new power plants.¹⁴¹

Transmission

Under certain conditions, transmission constraints may act as a bottleneck even when generation capacity is plentiful. Ukraine is adjacent to plentiful generation capacity located in neighboring European countries that are not under Russian bombardment, but relatively little of this capacity is accessible due to transmission constraints (see “Physical Resilience” section). In the United States, experts have long raised concerns that transmission constraints decrease grid flexibility—the ability to route electricity over a wide area as needed to balance supply and demand while maintaining grid stability and avoiding price spikes.¹⁴² The continental United States—and parts of Canada and Mexico—are served by three distinct grids: the Eastern Interconnection (covering most of the country east of the Rocky Mountains), the Western Interconnection (covering most of the country west of the Rocky Mountains), and ERCOT (covering most of Texas).¹⁴³

Fragmentation that exists even within major U.S. interconnections due to limited transfer capacity between different regional service areas could limit grid flexibility, even though generation facilities operate on a common synchronized frequency. A 2022 U.S. National Renewable Energy Laboratory (NREL) study examined the potential economic and environmental benefits of expanded transmission and transfer capacity between major interconnections, but did not specifically examine potential “non-quantified” reliability and resilience benefits.¹⁴⁴ Some legislative proposals in Congress would require minimum levels of transfer capacity between regions. Key points of debate around these proposals are costs and benefits for consumers as well as the appropriate role of federal and state governments in determining electricity transmission needs. Some believe a stronger federal policy supporting interregional electricity transmission could potentially lower costs for consumers and improve reliability and resilience. Others believe the current process sufficiently identifies benefits for consumers and allows state regulators greater say in transmission development.¹⁴⁵

The 118th Congress enacted the Fiscal Responsibility Act of 2023 (P.L. 118-5), which requires a study of interregional transfer capacity that includes information on current capabilities, recommendations for “prudent additions,” and recommendations “to meet and maintain total transfer capability.”¹⁴⁶ The proposed Clean Electricity and Transmission Acceleration Act of 2023

¹⁴¹ The NERC 2020 LTRA found that ERCOT had a 2021 anticipated reserve margin of 16.25% (p. 137). In its 2023 LTRA, NERC found ERCOT had an anticipated reserve margin for 2024 of 33.3% (see *NERC 2023 LTRA*, December 2023, p. 99, [https://www.nerc.com/pa/RAPA/ra/Reliability Assessments DL/NERC_LTRA_2023.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2023.pdf)).

¹⁴² See, for example, DOE, “Grid Deployment Office: National Transmission Needs Study,” <https://www.energy.gov/gdo/national-transmission-needs-study>.

¹⁴³ The electricity systems in Alaska and Hawaii are not connected with other states. Moreover, those states have multiple, isolated grids within the state. For example, each of Hawaii’s largely populated islands has its own electrical grid.

¹⁴⁴ Aaron Bloom et al., “The Value of Increased HVDC Capacity Between Eastern and Western U.S. Grids: The Interconnections Seams Study,” *IEEE Transactions on Power Systems*, vol. 37, no. 3 (May 2022), pp. 1765 and 1768. (Hereinafter “the Seams Study.”)

¹⁴⁵ For more on interregional transfer issues see CRS Report R47627, *Electricity Transmission Permitting Reform Proposals*, by Ashley J. Lawson.

¹⁴⁶ The report is due 18 months after enactment, or December 3, 2024. FERC must then publish the study and seek public comment, and then provide recommendations for legislative changes to Congress within one year of conclusion of the comment period. On May 10, 2023, the White House released a fact sheet outlining the Biden Administration’s priorities for permitting reform, which identified developing minimum interregional transfer requirements as a priority. (continued...)

(H.R. 6747) would require FERC to issue requirements for minimum transfer requirements between regions within two years of enactment, among other provisions. For more information on regulatory issues and legislative proposals in the 118th Congress related to interregional transfer capacity, see CRS Report R47627, *Electricity Transmission Permitting Reform Proposals*, by Ashley J. Lawson. Other proposals would provide tax credits for transmission infrastructure improvement and buildout, which may also increase grid flexibility.¹⁴⁷

The 117th Congress enacted legislation aimed at accelerating transmission development. For example, the Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) appropriated \$11 billion in grant programs for grid reliability and resilience (some of which may be used for the distribution system). The IIJA also appropriated \$2.5 billion for a new Transmission Facilitation Program through which DOE can provide financial and technical assistance for transmission line construction. In 2022, DOE initiated a Building a Better Grid Initiative in response to this mandate.¹⁴⁸ These programs are in the implementation phase, and the extent to which they may encourage new development remains unknown.

Energy Management Systems and Cybersecurity

Russia targeted Ukrainian energy management systems repeatedly with cyberattacks (see “Cyber Effects” section). A 2021 National Academies of Sciences, Engineering, and Medicine study on the future of the U.S. electric grid notes several potential vulnerabilities related to energy management systems:¹⁴⁹

- increasing use of internet-based information and communications technologies (ICT) for automation of grid energy management systems, which expands the *attack surface* for cyberattackers;
- increasing interconnection between information technology and operational technology;
- generally weak cybersecurity and resilience culture in the industry;¹⁵⁰
- lack of industry experience dealing with the full spectrum of threats; and
- prevalence of pre-digital legacy systems that are not readily incorporated with modern cybersecurity options.

According to NERC, there are no recorded instances of failure of energy management system functions leading to “loss of generation, transmission lines, or customer load” in the United

See White House, “Fact Sheet: Biden-Harris Administration Outlines Priorities for Building America’s Energy Infrastructure Faster, Safer, and Cleaner,” May 10, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/10/fact-sheet-biden-harris-administration-outlines-priorities-for-building-americas-energy-infrastructure-faster-safer-and-cleaner/>. Opponents of federal action on this topic say current permitting rules protect the ability of states and local governments to approve (or disapprove) infrastructure that is in the best interest of their citizens. See CRS Report R47627, *Electricity Transmission Permitting Reform Proposals*, by Ashley J. Lawson.

¹⁴⁷ See the Grid Resiliency Tax Credit Act (S. 1793 and H.R. 5803).

¹⁴⁸ See DOE, “Grid Deployment Office: Building a Better Grid Initiative,” <https://www.energy.gov/gdo/building-better-grid-initiative>.

¹⁴⁹ National Academies of Sciences, Engineering, and Medicine, *The Future of Electric Power in the United States*, Washington, DC, 2021, pp. 218-238, <https://doi.org/10.17226/25968>.

¹⁵⁰ The DOE-funded Roadmap to Achieve Energy Delivery Systems Cybersecurity, last updated in 2011, lists “Build a Culture of Security” as one of five strategies constituting the roadmap’s strategic framework. See Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, p. 3, https://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

States, although EMS failures leading to lesser consequences occur with some regularity, due mainly to software and communications issues.¹⁵¹ NERC recommends that operators adopt several risk mitigations, including:¹⁵²

- planning for loss of grid visibility and ensuring availability of backup communications measures;
- ensuring adequate staffing, and realistic training and exercises, for manual interventions in the field if computer-aided energy management systems are not available; and
- increasing available backup power supplies to account for time needed for manual system restoration.

Resilience Metrics and Valuation

An emerging field of research develops metrics to inform public and private sector investments in grid resilience. Resilience metrics differ conceptually from widely-used reliability metrics. According to NREL, a resilient power grid “withstands, responds to, and recovers rapidly from major power disruptions as its designers, planners, and operators anticipate, prepare for, and adapt to changing grid conditions.”¹⁵³

By contrast, reliability measures the ability to minimize the frequency and duration of more transitory and routine disruptions under steady-state conditions. Therefore, “a highly reliable system is not necessarily resilient.”¹⁵⁴

Risk mitigation strategies to improve grid resilience may include hardening of physical and cyber infrastructure, incorporating redundant systems to eliminate single points of failure, diversification of generation sources, response planning, and spare parts stockpiling, among others.¹⁵⁵

Resilience investments often involve up-front costs. Resilience metrics may facilitate more accurate valuation of those investments by quantifying losses or potential losses due to preventable outages or damage to critical infrastructure. Resilience metrics focus on “event duration and recovery time through a more qualitative lens,” and are designed to capture “economic consequences, critical infrastructure damages, and effects on local and regional communities.”¹⁵⁶

Examples of quantitative metrics include Value of Lost Load, which measures the losses incurred by customers during outages, or Time to Recovery. Qualitative attributes of resilient systems, such as redundancy, may also be used.¹⁵⁷

According to the National Academies of Sciences, Engineering, and Medicine study, industry has made some investments in relevant measures to mitigate risk from potential cyber, physical, and electromagnetic pulse attacks. However, the study states that “standard metrics for quantifying resilience [as opposed to reliability] have not been established,” and that “there are no simple statistical methods to assess how these investments individually or collectively contribute to

¹⁵¹ North American Electric Reliability Corporation, *Risks and Mitigations for Losing EMS Functions Reference Document*, *ibid.*, p. 9.

¹⁵² FERC and NERC, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans, Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*, Washington, DC, June 2017, pp. 6-7, <https://www.ferc.gov/media/06-09-17-ferc-nerc-reportpdf-1>.

¹⁵³ NREL, “Power System Resilience,” <https://www.nrel.gov/research/power-system-resilience.html>.

¹⁵⁴ Zhaohong Bie et al., “Battling the Extreme: A Study on the Power System Resilience,” *IEEE Proceedings*, vol. 105, no. 7 (2017), p. 1255.

¹⁵⁵ Kate Anderson et al., *Energy Resilience Assessment Methodology*, NREL, Golden, CO, October 2019, p. 13, <https://www.nrel.gov/docs/fy20osti/74983.pdf>.

¹⁵⁶ Leddy et al., *Measuring and Valuing Resilience*, p. 10.

¹⁵⁷ For a more detailed overview of resilience metrics, see section on “Measuring Resilience,” *ibid.*, pp. 11-14.

improved resilience.”¹⁵⁸ An after-action report on a major grid-resilience exercise conducted by DOE in 2021 found that many organizations lacked “secondary and tertiary communication options and/or procedures ... within a degraded communication environment.”

The IIJA authorizes several cybersecurity initiatives or programs under Division D (Title I, “Grid Infrastructure and Resilience,” Subtitle B, “Cybersecurity”), which target the electricity sector. It authorizes \$600 million in appropriations over five years, targeting rural and municipal utilities and other sector stakeholders.¹⁵⁹ Examples of authorized activities include development and deployment of advanced cybersecurity technologies; grid modeling and vulnerability assessments (including for related communications, control, and power systems); supply chain security research; grid security exercises; and pilot demonstration projects for industry to gain experience with new technologies. Additional mandates include a requirement for federal regulators to develop a cybersecurity testing program for products intended for use in the energy sector; a requirement to develop incentives for industry investments in cybersecurity technology development and deployment; and authorization for DOE to require recipients of grant awards under Division D to submit cybersecurity plans for review.¹⁶⁰

Issues for Congress

Congress may conclude that existing programs and authorities are adequate to address the issues discussed in this report. Alternatively, it may select from a variety of options for legislative and oversight action, including the following:

- *Oversight of national-level exercise programs administered by FEMA, DOE, DOD, and other agencies.* Congressional oversight could include examination of information on scenario design after-action reports for exercises, and assessments of grid-entities’ abilities to maintain national critical functions of electricity production and supply during prolonged crises with degraded systems and persistent and evolving threats (see “Potential Gaps in U.S. Preparedness” section).
- *Promoting greater availability of spare LPTs.* Congress may wish to exercise oversight over DOE’s efforts to identify “actionable objectives, or time frames,” to assist industry in developing adequate LPT reserves as recommended in a GAO report, or modify program goals to address industry feasibility concerns (see “Industrial Base Capacity, Supply Chain Security, and Stockpiling” section).
- *Modification of grant-award procedures for existing programs, such as CDBG.* Such changes could provide for more rapid disbursement of federal funding to grid entities for repairs after one or more major incidents (see “Disaster Assistance” and “Economic Resilience” sections).

¹⁵⁸ National Academies of Sciences, Engineering, and Medicine, *Future of Electric Power*, p. 214. The report treats resilience and reliability—the more commonly used industry metric—as related, but distinct concepts. According to the report, reliability describes “the ability of the grid to deliver electricity, while resilience refers more broadly to the sum of preparation, planning, operations, and learning activities that increase the ability of the grid to continue—or quickly resume—operation when subjected to stresses or attacks.

¹⁵⁹ Actual appropriations may be found in Division J, Title III—Energy and Water Development and Related Agencies, of the IIJA.

¹⁶⁰ FERC issued a final rule on incentives for industry investments in cybersecurity technology development and deployment on April 21, 2023. See FERC, *Incentives for Advanced Cybersecurity Investment*, Order No. 893, April 21, 2023, <https://www.ferc.gov/media/e-1-rm22-19-000-0>; and FERC, “Cybersecurity Incentives,” <https://www.ferc.gov/cybersecurity-incentives>.

- *Expanding Stafford Act major disaster coverage.* The Stafford Act could be amended to ensure that manmade incidents not produced by fire or explosion—such as small arms fire, electromagnetic pulse, and cyberattacks—are covered by the act’s major disaster definition (see “Disaster Assistance” section).
- *Measuring the impacts of low-income ratepayer assistance programs.* Congress may be particularly interested in how such assistance may broaden and stabilize the existing ratepayer base for utilities, and could consider these factors for purposes of program authorizations, appropriations, and oversight. Additionally, the relatively low (22% in 2015) program participation rates could be an oversight issue (see “Affordability, Access, and Social Welfare” and “Economic Resilience” sections).
- *Grid resilience impacts of weatherization assistance and building efficiency programs.* The impact of these programs in reducing electricity load and energy intensity could be of particular interest to Congress, and could be considered for purposes of program authorizations, appropriations, and oversight (see “Efficiency, Jobs, and the Environment” section).
- *Oversight of IIJA mandates.* Existing IIJA mandates for federal agencies to develop incentives for industry investments in cybersecurity technology development and deployment could be a subject for congressional oversight. Additional cybersecurity measures could include mechanisms—both voluntary and regulatory—for information sharing and reporting to provide regulators and infrastructure owner-operators adequate visibility of the electricity sector’s cybersecurity posture and risk profile (see “Energy Management Systems and Cybersecurity” section).

Several bills have been introduced in the 118th Congress related to the issues discussed in this report, including the following:

- Protecting America’s Distribution Transformer Supply Chain Act (H.R. 4167), which would prohibit DOE from revising existing energy conservation standards for distribution transformers in electric power systems for the next five years.
- Clean Electricity and Transmission Acceleration Act of 2023 (H.R. 6747), which would require FERC to issue requirements for minimum transfer requirements between regions within two years of enactment, among other provisions.
- Grid Resiliency Tax Credit Act (S. 1793 and H.R. 5803), which would provide tax credits for transmission infrastructure improvement and buildout.
- Facilitating the Reshoring of Energy Grid Component Manufacturing Act of 2023 (S. 34), which would establish a DOE loan program to expand domestic manufacturing of grain-oriented electrical steel, or GOES—a specialized alloy used in LPT manufacture, LPTs, distribution transformers, and other electric grid components.
- Protect American Power Infrastructure Act (S. 1050), which would prohibit certain transactions that involve using equipment used in bulk-power system substations, control rooms, or power generating stations to provide power for defense critical electric infrastructure in the United States if a foreign adversary owns or exercises influence over the equipment.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.