The Invisible War

Pre-Positioned Cyber Weapons Are Already Inside the Power Grid

A Macroeconomic Threat Assessment

Dr. Gregory S. Carmichael

DBA, MA, BA, Lt. Col. USAF (Ret.)

CryptoSoWhat.com

February 2026

Macroeconomics & Strategic Risk Analysis

Contents

Executive Summary

The most dangerous cyber weapons targeting American infrastructure are not being developed. They are already deployed.

Intelligence agencies have confirmed that nation-state actors—China's Volt Typhoon, Russia's Sandworm, and Iran's Cyber Av3ngers—maintain persistent access inside the Supervisory Control and Data Acquisition (SCADA) systems that control the U.S. power grid. The malware is mapped, tested, and waiting for activation.

This is not a technology problem. It is a strategic problem with macroeconomic consequences that dwarf any single market event. The EMP Commission estimated that a coordinated electromagnetic-cyber attack could cause $2 trillion in economic damage with a 4–10 year recovery timeline for the electrical grid. Even a conventional cyber-only attack causing a two-week regional blackout would produce cascading failures across financial markets, supply chains, healthcare, water treatment, and telecommunications.

This paper examines the convergence of cyber and electromagnetic threats to the U.S. power grid, the macroeconomic exposure created by decades of under-investment in critical infrastructure protection, and the policy and investment implications for decision-makers across government, finance, and industry.

How the Grid Actually Works—And Why It Is Vulnerable

The modern power grid runs on SCADA systems—industrial computers that monitor and control everything from generator output to substation breakers. These systems were designed in an era of isolated, serial-connected networks. They have since been connected to IP networks for remote monitoring and cost efficiency.

The result is that protocols like MODBUS and DNP3, which include **no authentication, no encryption, and no integrity verification**, are now accessible from corporate IT networks—and in some cases, from the internet.

The OT/IT Convergence Problem

Operational Technology (OT) networks were originally air-gapped from Information Technology (IT) networks. The economic pressure to enable remote monitoring, predictive maintenance, and centralized control has eroded this separation over the past two decades. The convergence creates attack surfaces that neither OT engineers nor IT security teams fully understand.

> **Key Vulnerability:** Industrial control protocols designed in the 1970s–1990s are now exposed to modern network attack techniques. MODBUS, developed in 1979, has no concept of authentication. DNP3, developed in the 1990s, offers optional authentication that is rarely implemented. An attacker who reaches these protocols can read sensor data, modify setpoints,

> and issue control commands without credentials.

The SCADA Architecture

A typical utility SCADA architecture includes:

- **Field devices:** Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) at substations and generation facilities
- **Communication networks:** Serial, radio, cellular, and increasingly IP-based links between field devices and control centers
- **Master stations:** Human-Machine Interface (HMI) systems where operators monitor and control the grid
- **Historian servers:** Databases that log all operational data for analysis and compliance
- **Corporate IT:** Business systems connected to the internet, often with pathways into the OT network

The attack surface exists at every junction between these layers. The most common initial access vector is through the corporate IT network—via phishing, compromised credentials, or vulnerable internet-facing services—followed by lateral movement into the OT environment.

The Threat Landscape: Who Is Inside

China: Volt Typhoon

In May 2023, U.S. intelligence agencies and Microsoft disclosed that a Chinese state-sponsored group designated Volt Typhoon had been pre-positioning itself inside critical infrastructure networks across the United States, including energy, water, communications, and transportation sectors.

> **Case Profile: Volt Typhoon**
>
> **Attribution:** People's Republic of China, Ministry of State Security
> **Active Since:** At least mid-2021
> **Targets:** U.S. critical infrastructure, particularly Guam and Pacific-adjacent assets
> **Technique:** "Living off the land"—using legitimate system tools (PowerShell, WMI, cmd.exe) to avoid detection. No custom malware deployed.
> **Objective:** Pre-positioning for disruption during a Taiwan contingency, not espionage.

What distinguishes Volt Typhoon from traditional espionage operations is the **absence of data exfiltration**. The group is not stealing information—it is establishing persistent access for future disruption. This is the digital equivalent of pre-positioning demolition charges on a bridge during peacetime.

CISA Director Jen Easterly described Volt Typhoon's activity as preparation to "disable or destroy" infrastructure in the event of a conflict with the United States. The group's focus on Guam and other Pacific facilities suggests contingency planning related to a potential Taiwan scenario.

Russia: Sandworm

Russia's GRU Unit 74455, known as Sandworm, is the most operationally proven cyber threat to power grids in the world.

> **Case Study: Ukraine Power Grid Attack (December 2015)**
>
> **Vector:** Spear-phishing emails with malicious Microsoft Word attachments
> **Malware:** BlackEnergy 3, KillDisk
> **Impact:** Three regional utilities compromised. Attackers remotely operated SCADA HMIs to open breakers at 30+ substations. 230,000 customers lost power for 1–6 hours.
> **Recovery sabotage:** KillDisk wiped SCADA servers. Firmware on serial-to-Ethernet converters was overwritten, preventing remote restoration. UPS systems at control centers were disabled.

The 2015 Ukraine attack demonstrated a complete kill chain: initial access via phishing, persistence through scheduled tasks and VPN backdoors, reconnaissance of the OT environment over several months, coordinated execution across three utilities, and deliberate sabotage of recovery capabilities.

In December 2016, Sandworm struck again, this time using CrashOverride (also called Industroyer)—the first publicly known malware specifically designed to interact with power grid protocols. CrashOverride could speak IEC 101, IEC 104, and OPC DA natively, allowing it to directly control substation equipment without an operator's HMI.

Iran: Cyber Av3ngers

In late 2023, an Iranian-affiliated group calling itself Cyber Av3ngers compromised Unitronics programmable logic controllers at water utilities across the United States, including the Municipal Water Authority of Aliquippa, Pennsylvania.

> **Case Study: Aliquippa Water Authority (November 2023)**
>
> **Vector:** Default credentials on internet-exposed Unitronics Vision Series PLC
> **Impact:** Attackers gained control of a booster station pump. The compromised HMI displayed "You have been hacked. Down with Israel."
> **Significance:** Demonstrated that even unsophisticated attacks on internet-exposed industrial controllers can compromise U.S. water infrastructure.

While the Aliquippa incident was relatively unsophisticated compared to Sandworm's operations, it demonstrated a critical vulnerability: many small and medium utilities have industrial controllers directly accessible from the internet with default or weak credentials.

The Triton/TRISIS Escalation

The 2017 Triton attack against a Saudi Arabian petrochemical facility represents the most dangerous escalation in industrial cyber warfare to date.

> **Triton targeted the Safety Instrumented System (SIS)**—the last automated line of defense against catastrophic industrial accidents. The SIS exists to prevent explosions, toxic releases, and equipment destruction when the process control system fails. Disabling it while inducing a fault condition could cause physical destruction and loss of life.

The Triton malware, attributed to Russia's Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), was designed to reprogram Schneider Electric Triconex safety controllers. The attack was detected only because a bug in the malware caused the SIS to enter a safe shutdown state, triggering an investigation. Had the malware functioned as designed, the consequences could have been catastrophic.

The Convergence: Cyber + Electromagnetic Pulse

Figure 1: The grid at ground level: malicious code flowing through power infrastructure.

The most alarming dimension of the grid threat landscape is the potential convergence of cyber and electromagnetic attacks. A sophisticated adversary would use pre-positioned cyber access to disable protective relays and wipe recovery systems *before* delivering a physical electromagnetic pulse.

The Combined Attack Sequence

A coordinated cyber-EMP attack would follow a predictable sequence:

1. **Phase 1—Pre-positioning (months to years):** Establish persistent access in utility SCADA networks. Map the OT environment. Identify critical protective relays, transformer monitoring systems, and recovery infrastructure.
2. **Phase 2—Cyber preparation (hours before):** Disable or reconfigure protective relays so they will not trip during the electromagnetic event. Wipe firmware on serial-to-Ethernet converters to prevent remote restoration. Disable backup generators at control centers by manipulating fuel or starting circuits through connected building management systems.
3. **Phase 3—Electromagnetic delivery:** Detonate a nuclear device at high altitude (HEMP) or deploy a directed-energy weapon against key substations. The resulting electromagnetic pulse damages power electronics, transformers, and communications equipment.
4. **Phase 4—Recovery denial:** With protective relays disabled, SCADA systems wiped, and communications equipment damaged, restoration requires physical access to every affected substation. Replacement of damaged high-voltage transformers—which have 12–24 month lead times—creates a protracted blackout.

High-Altitude Electromagnetic Pulse (HEMP) Physics

A nuclear detonation at altitudes of 30–400 km above the Earth's surface generates three distinct electromagnetic pulse components:

Component	Duration	Primary Threat	Mechanism
E1	Nanoseconds	Electronics, communications	Compton electrons gyrating in Earth's magnetic field produce fast-rising fields (50 kV/m at ground level)
E2	Microseconds to ms	Communications, power lines	Scattered gamma rays and neutrons; similar to lightning but geographically widespread
E3	Seconds to minutes	Power grid transformers	Magnetohydrodynamic disturbance of Earth's magnetic field induces quasi-DC currents in long conductors

Table 1: HEMP components and their infrastructure effects

The E1 component is particularly dangerous to modern electronics because its rise time (2–5 nanoseconds) is faster than most surge protection devices can respond. The E3 component threatens

the power grid's most irreplaceable assets—large power transformers—through geomagnetically induced currents (GIC) that cause core saturation, overheating, and permanent damage.

The Transformer Crisis

The United States operates approximately 2,000 high-voltage transformers (HVTs) rated above 345 kV. These units are:

- Custom-built to specifications unique to each installation
- Manufactured primarily overseas (South Korea, Germany, Japan, India)
- 12–24 months from order to delivery under normal conditions
- 200–400 tons each, requiring specialized transport
- Not interchangeable between installations without significant modification

> **The Strategic Implication:** There is no domestic surge production capacity for high-voltage transformers. If a coordinated attack destroyed or damaged even 5–10% of the nation's HVT fleet, the replacement timeline would exceed the ability of modern society to function without electricity. Food supply chains, water treatment, healthcare, financial systems, and communications would fail sequentially within days to weeks.

Macroeconomic Exposure

Direct Economic Impact

The EMP Commission's analysis estimated the following economic consequences of a large-scale grid failure:

Impact Category	Short-term (0–30 days)	Long-term (1–4 years)
GDP loss (annualized)	$1–2 trillion	$4–8 trillion cumulative
Financial market disruption	Circuit breakers triggered	Systemic risk event
Supply chain failure	Regional within 72 hours	National within 2 weeks
Healthcare system collapse	Emergency care only	Mass casualty event
Food supply disruption	Refrigeration loss (48 hrs)	Distribution failure
Water/sanitation failure	Treatment plants offline	Contamination risk
Communications blackout	Cellular within 8–72 hours	Long-term degradation

Table 2: Estimated economic and societal impact of coordinated grid attack

Cascading Failures

The power grid is the foundation upon which all other critical infrastructure depends. A sustained grid failure triggers cascading effects:

Financial markets: Electronic trading halts. Clearing and settlement systems fail. ATMs and point-of-sale systems go offline. The Federal Reserve's payment systems (Fedwire, CHIPS) require continuous power. A multi-day outage could trigger a liquidity crisis comparable to or exceeding 2008.

Healthcare: Hospitals have backup generators rated for 48–96 hours. Without grid restoration, hospitals face fuel supply challenges (fuel pumps require electricity) and cold-chain failure for medications and blood products. Dialysis centers, which serve approximately 500,000 Americans, become inoperable within days.

Water and sanitation: Water treatment and distribution rely on electric pumps. Most municipal water systems can maintain pressure for 12–48 hours on reservoir capacity alone. After that, boil-water advisories become the norm—assuming residents have alternative heating sources.

Telecommunications: Cellular towers typically have 4–8 hours of battery backup. Some have diesel generators extending this to 24–72 hours. Without grid power, mobile communications degrade rapidly, eliminating the primary coordination mechanism for emergency response.

Insurance and Reinsurance Exposure

The insurance industry has begun to recognize cyber-physical attacks on critical infrastructure as a potential systemic risk. Lloyd's of London has estimated that a severe cyber attack on the U.S. power grid could generate $71–243 billion in insurance claims, with potential for "silent cyber" exposure in property and casualty policies that were never priced for this risk.

> **Investment Implication:** The gap between the probability of a grid attack and the level of protection currently deployed represents one of the largest unpriced systemic risks in the global economy. For insurers, reinsurers, and institutional investors, this is not a tail risk to be monitored—it is a present-day exposure that is growing as adversary capabilities improve and grid vulnerability persists.

The Protection Standards Landscape

Multiple regulatory frameworks address grid protection, but none comprehensively covers the combined cyber-electromagnetic threat:

Standard	Scope	Gap
NERC CIP	Cybersecurity for bulk electric system	No EMP provisions
MIL-STD-188-125	Military HEMP protection	Not applicable to civilian grid
EO 13865 (2019)	Coordinating EMP resilience	Executive order, no enforcement
ICD 705 / TEMPEST	Classified facility emanations	Government-only, no grid focus
IEEE 1613	Substation environment standards	Addresses surges, not HEMP

Table 3: Regulatory framework gaps

The fundamental problem is jurisdictional: NERC CIP addresses cybersecurity but not electromagnetic threats, while military standards address electromagnetic hardening but not civilian infrastructure. No single framework addresses the combined cyber-EMP attack scenario that represents the most severe threat.

Policy and Investment Implications

For Policymakers

1. **Mandate combined threat assessments.** Current regulations treat cyber and physical threats separately. A combined assessment framework is needed that evaluates how cyber pre-positioning amplifies the impact of physical attacks.
2. **Establish a strategic transformer reserve.** The U.S. has no meaningful inventory of spare high-voltage transformers. A federal program to manufacture and pre-position replacement units—analogous to the Strategic Petroleum Reserve—could reduce recovery timelines from years to months.
3. **Incentivize grid hardening.** Current rate structures do not adequately compensate utilities for investments in resilience. Federal incentives tied to demonstrated hardening milestones could accelerate protection deployment.
4. **Close the OT/IT security gap.** NERC CIP standards must be expanded to address legacy protocol vulnerabilities, require authentication on all control communications, and mandate network segmentation between IT and OT environments.

For Investors and Financial Institutions

1. **Price the systemic risk.** Grid vulnerability should be treated as a systemic exposure in portfolio risk models, not as a low-probability tail event. The pre-positioning of adversary access means the "trigger probability" is a function of geopolitical conditions, not technical feasibility.
2. **Evaluate critical infrastructure exposure.** Any investment thesis dependent on continuous electricity—data centers, cold-chain logistics, healthcare REITs, financial exchanges—carries implicit grid risk that is currently unpriced.

3. **Identify the protection market.** The gap between threat severity and current protection levels represents a market opportunity measured in hundreds of billions of dollars. Companies developing grid hardening technologies, transformer manufacturing capacity, advanced shielding materials, and OT cybersecurity solutions are positioned for structural growth.

For Corporate Leaders

1. **Test your continuity assumptions.** Most business continuity plans assume grid restoration within 24–72 hours. A coordinated attack scenario requires planning for weeks-to-months timelines.

2. **Audit your OT security.** If your operations depend on industrial control systems, assume that the OT/IT boundary is permeable. Conduct a penetration test that specifically targets OT protocols from the IT network.

3. **Evaluate on-site generation and storage.** For critical operations, the question is not whether backup power is needed but whether it is sufficient for an extended grid outage. Solar, battery storage, and on-site generation provide resilience that grid-dependent operations cannot match.

Conclusion: The Cost of Inaction

The pre-positioned cyber weapons are not a warning about the future. They are a description of the present. The intelligence community has confirmed that adversary access exists, that the access is designed for disruption rather than espionage, and that the capabilities to cause catastrophic infrastructure damage are mature.

The convergence of cyber and electromagnetic threats creates a scenario in which the U.S. power grid—the foundational infrastructure upon which all other systems depend—could be disabled for an extended period with consequences measured in trillions of dollars and potentially millions of lives.

The only question is whether the response will come before or after activation.

The cost of comprehensive grid protection is measured in tens of billions of dollars. The cost of a successful coordinated attack is measured in *trillions*. By any rational cost-benefit analysis, the investment case for critical infrastructure protection is overwhelming.

For investors, insurers, policymakers, and corporate leaders, the "So What?" is clear: critical infrastructure protection is no longer a niche defense concern. It is a systemic risk to the global economy, and the gap between threat severity and current protection levels represents both a policy failure and a market opportunity of historic proportions.

References and Further Reading

1. CISA Advisory: "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" (February 2024)
2. Microsoft Threat Intelligence: "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques" (May 2023)
3. ICS-CERT Alert: "Cyber-Attack Against Ukrainian Critical Infrastructure" (IR-ALERT-H-16-056-01)
4. Dragos Inc.: "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations" (2017)
5. FireEye/Mandiant: "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools" (2018)
6. EMP Commission: "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack" (2008, updated 2017)
7. Lloyd's of London: "Business Blackout: The insurance implications of a cyber attack on the US power grid" (2015)
8. NERC: "GridEx Exercise Reports" (2013–2023)
9. Executive Order 13865: "Coordinating National Resilience to Electromagnetic Pulses" (March 2019)
10. NIST SP 800-82 Rev. 3: "Guide to Operational Technology (OT) Security" (2023)