America’s industrial and shipping systems are sitting ducks for China.
Time to learn from our mistakes before it’s too late.

For years, America's intelligence chiefs have warned Congress of critical infrastructure vulnerabilities. Those warnings became concrete with the 2024 revelation of operations "Volt Typhoon" and "Salt Typhoon," highlighting China's deep penetration into our industrial systems. Chinese cyber forces quietly occupy positions inside American telecommunications, transportation, water, power, and defense manufacturing systems—ready to unleash devastating disruptions designed explicitly to shake American resolve during a crisis over Taiwan.

During my tenure as Senior Director for Cybersecurity on President Trump's National Security Council (2017-2021), attacks like "NotPetya" and "Wannacry" crippled global infrastructure, costing tens of billions and revealing severe digital vulnerabilities. President Trump went to great lengths to bolster our national cyber posture during his first term, but his second term offers an opportunity to significantly improve our capabilities. Because America’s infrastructure remains dangerously exposed.

Our industrial base—pipelines, ports, railroads, and critical defense production—is designed primarily for efficiency and profitability, not resilience under attack. Defense-critical manufacturing infrastructure that isn't built to survive past day one of conflict constitutes national negligence, a quiet betrayal hidden behind spreadsheets and quarterly earnings.

Consider oil pipelines. The Colonial Pipeline attack vividly demonstrated this vulnerability. The company chose to shut down—not because the pipeline itself was compromised, but because their cyber systems could no longer track fuel flow for billing. Business insurance covered their losses, but who covers America's strategic vulnerability in wartime?

Our maritime infrastructure is similarly vulnerable. Collateral damage from the NotPetya attack nearly halted East Coast ports, reverting logistics to manual procedures, choking trade, and costing billions. Yet modernization at ports still prioritizes efficiency over security, leaving resilience as an afterthought.

The nation's railway system fares no better. Despite digital upgrades, underlying structures often reflect designs from the late 19th century—now dangerously linked to insecure digital controls. Modernization projects prioritize short-term returns, sidelining resilience against cyber threats.

Reindustrialization, championed by decisive actions on trade, investment, and regulatory reform, represents a critical opportunity. Apple's $500 billion domestic investment highlights the promise of digital-industrial integration. Yet, each advanced facility constructed without embedded cybersecurity multiplies our risk.

Securing critical infrastructure and the defense industrial base is neither glamorous nor–unlike the attacks our adversaries take such pleasure in–politically thrilling. But it's precisely in these overlooked sectors that our greatest vulnerabilities lie, and where decisive leadership can quickly effect meaningful change.

Government cannot easily dictate how private industry operates generally. But critical infrastructure is different—justified clearly by national security. President Trump's second term provides an opportunity to rebuild American industry securely from day one.
America can no longer afford to fake resilience. Infrastructure not designed to operate during conflict is ultimately a threat to our national security. The hour is late—but it's not too late to transform America's vulnerabilities into genuine resilience, safeguarding our prosperity, security, and freedom.