

PROTECTING TEXAS CRITICAL INFRASTRUCTURE:

Prevention, Mitigation, and Recovery from Natural Disasters and State Actor and Terrorist Attacks

WRITTEN BY **The Honorable Chuck DeVore**
OCTOBER 2026

KEY POINTS

- Texas's critical infrastructure remains vulnerable to natural disasters and attacks.
- The federal government largely abandoned civil defense 50 years ago.
- Should key elements of Texas's infrastructure be attacked today (electric transformers), recovery could take years.
- Texas is reviewing the threats from natural disasters, war, and terror attacks, but it should conduct regular field exercises to test its response and look for gaps.
- Texas must fund the creation of a critical stockpile of equipment and medicines under the control of TDEM or the National Guard.

INTRODUCTION

Texas's critical infrastructure underpins both the state's economy and U.S. national security. Critical infrastructure isn't confined to just the electric grid and transportation networks, but also includes energy production and refining facilities, water and wastewater systems, food production and distribution, ports, communications, and financial centers in Dallas and Houston.

But these assets, which span the state, are vulnerable to both natural disasters and attack. Disruptions that lead to fatalities can cascade rapidly, as in Winter Storm Uri in 2021 and regionally during and after hurricane impacts along the Gulf Coast.

Texas cannot prevent every cyberattack, terrorist plot, or hostile-state action, and certainly cannot prevent hurricanes and winter storms, but we can ensure that no single event can produce catastrophic failure resulting in mass casualties. Texas needs to advance a state-level critical infrastructure resilience strategy built around preventing attacks where possible, hardening assets, and restoring essential systems rapidly when prevention falls short.

While the federal government retains primary responsibility for many threats, civil defense was deprioritized starting in the late 1960s and was largely forgotten after the Cold War ended with the Soviet Union's collapse in 1991 ([DeVore, 2023](#)). The formal end of civil defense came

continued

after FEMA's poor performance on Hurricane Andrew in 1992 when the newly appointed FEMA Director, James Lee Witt, ended the dedicated Civil Defense and national-mobilization programs in November 1993. At this time, dedicated nuclear-attack civil-defense planning, shelter surveys, and crisis-relocation programs were discontinued or reduced to residual elements ([Lucie, 2019](#)).

This leaves a mismatch, with an unrealized expectation that the federal government has things well in hand when, in fact, they do not and have not for 33 years. Absent a comprehensive federal response, Texas must lead in preparedness given its unique vulnerabilities, the limitations or uncertainty of distant federal responses, and Texas's outsized importance to national security. To emphasize, in a national (not a regional) emergency, FEMA will be unable to come to Texas's aid.

The public intuitively understands this, with a MITRE-Harris public opinion poll conducted in 2024 showing that 81% of Americans worry about the safety and security of the nation's critical infrastructure ([MITRE, 2024](#)). Further, 85% of respondents viewed protecting critical infrastructure as a "matter of life and death," with "cyberattacks, terrorism, and aging/failing infrastructure (being) considered the greatest risks to our critical infrastructure."

This paper examines three primary threat categories and lays out three core mitigation strategies. The three general threats are natural disasters, war, and terror attacks. The three basic mitigation strategies are prevention, asset hardening, and rapid recovery capabilities.

Lastly, because some critical infrastructure is more important (or more resilient) than others, it is necessary to prioritize limited resources. Critical infrastructure components, by importance of system, are ranked as follows:

1. Electrical Grid: Without electricity, everything else fails.

2. Water Systems: After a lack of breathable air, humans will perish next from a lack of potable water, while waterborne illnesses will severely afflict already stressed people.

3. Fuel: This includes fuel for generating electricity (mostly natural gas), transportation, and home heating.

4. Communications: Information must flow to emergency responders to understand the extent of the damage and to coordinate a response.

5. Finance: Funds must be available to recover.

Some might view other systems as critical infrastructure but on further consideration understand that they are in fact systems dependent on critical infrastructure. These include, but are not limited to:

- **Transportation:** The physical U.S. highway and rail networks have enormous redundancy, so they do not collapse the way a water treatment plant or a regional power grid does. That said, transportation's *operational* resilience is lower than its *physical* resilience. Gas station pumps, pipeline terminals, traffic signals, rail signaling, and port cranes all need electricity. Diesel trucks and the tankers that refill stations need fuel. In Winter Storm Uri, roughly 1,700 Texas stations closed simply because they had no power; remaining stations ran dry because resupply trucks could not move on icy roads and because diesel gelled.

- **Public Health Delivery:** Public health is impossible without electricity (hospitals, water, communications) and fuel (ambulances, backup generators). It is a consumer of the lifelines rather than a lifeline itself.

- **Food Distribution:** Like public health, it is downstream of the top five already listed. Urban grocery inventories are measured in days, not

weeks. Refrigeration, processing plants, and the truck fleet that restocks stores all require electricity and diesel. Unlike electricity, water, and fuel, a wide variety of foods can substitute for one another to sustain a population.

DEFINING THE THREATS

Natural Disasters

Hurricanes pose an annual threat to Texas's Gulf Coast infrastructure. Major storms like Hurricane Harvey in 2017 and Winter Storm Uri in 2021 caused widespread flooding, power outages, and damage to refineries and water systems. Extreme solar storms (e.g., geomagnetic disturbances or GMDs) represent a lower probability (frequency) but a far higher risk (DeVore, 2023). A Carrington-level event could generate geomagnetically induced currents that damage high-voltage transformers across Texas's grid. The 2013 Lloyd's report estimated potential economic losses from a severe solar storm in North America at hundreds of billions to trillions of dollars, with Gulf Coast regions facing elevated risk because of their proximity to the Gulf, grid configuration, and ground conductivity (Lloyd's, 2013).

War—Most Likely Conflict with China over Taiwan

A Taiwan contingency could trigger coordinated Chinese actions against U.S. critical infrastructure to deter or delay American intervention. PRC state-sponsored actors, notably the Volt Typhoon group, have already pre-positioned access in U.S. networks across communications, energy, transportation, and water/wastewater sectors. These actors maintain long-term persistence using “living off the land” techniques, positioning for disruptive cyberattacks on key systems in during a conflict (CISA, 2024).

Physical sabotage by covert teams or proxies is also likely in a pre-war or war scenario (Gertz, 2026). Chinese espionage networks have conducted reconnaissance near sensitive sites with at least 100 incidents reported by September 2023 (Lubold, 2023).

Beyond reconnaissance, analysts harbor growing concerns about operatives developing capabilities for physical disruption (Mitch, 2025).

The rapid development of drone warfare in Russia's war on Ukraine also greatly increases the likelihood that weaponized drones may be used in large numbers to conduct infrastructure attacks. This concept may have already been tested with small numbers of drones operating off Russia's extensive so-called “ghost fleet” of sanctions-avoiding ships operating in European waters (Greene et al., 2026; Edwards et al., 2026). Here, it is instructive to note that the source of the extensive drone sightings in the Norfolk, Virginia area in late 2023 (mainly December), centered on Joint Base Langley-Eustis (Langley Air Force Base) and extending over or toward Naval Station Norfolk for 17 consecutive nights, has yet to be publicly revealed (DeVore, 2024).

Texas has begun to understand these threats through Governor Greg Abbott's Executive Order No. GA-49 in 2024 directing vulnerability assessments, cyber response simulations, and grid restart planning (Abbott, 2024), as well as the signing of SB 2312, which created the Texas Advisory Committee on Geopolitical Conflict (SB 2312, 2025).

Executive Order No. GA-49 initiated surveys on vulnerabilities of critical infrastructure and state and local government; directed the Public Utility Commission (PUC) to conduct annual tabletop exercises to respond to a black start; directed TDEM to conduct annual tabletop exercises simulating an enemy cyber-attack on a sector of the Texas economy; directed TDEM to assemble relevant state agencies to develop a plan to deal with electromagnetic threats; and directed Electricity Reliability Council of Texas (ERCOT) to create a secure, dedicated communications channel for telecommunication and electrical infrastructure companies to use to help ERCOT prioritize load requests during a grid

1 “Living-off-the-land” (LOTL) techniques refer to cyber attackers that avoid planting custom malware and instead abuse legitimate, built-in tools and features that are already present on the compromised systems. This may allow them to operate for years without detection.

incident. These steps, along with creating the Texas Advisory Committee on Geopolitical Conflict, are necessary preparatory actions to understand the threat and how to address it. Importantly, they do not fund recovery items, such as spare high-voltage transformers stored around Texas, nor do they take the required next step of conducting field exercises to physically test a response.

Terrorism—Domestic and Jihadi Directed or Inspired

Jihadist threats in Texas include lone-actor attacks inspired by groups such as ISIS or al-Qaeda affiliates, as well as plots targeting critical sites. Historical examples include the 2009 Fort Hood shooting and the 2015 Garland attack. Broader assessments highlight the risk of cyberattacks or physical sabotage against soft targets in infrastructure sectors, including water systems and energy facilities. Heightened threat environments tied to overseas conflicts can increase lone-wolf mobilization or low-level cyber activity by sympathizers. Access to artificial intelligence may enable more sophisticated attacks using biological or chemical agents or targeting key infrastructure nodes. Domestic groups also present a threat, though history suggests that threat is more likely to be directed against manifestations of government authority.

Additional Threat Vectors

Traditional state actors, whether during an open state of war or during gray zone hostilities, as well as terror groups, may act on systems within their capabilities, using various means they can acquire. These vectors include:

- **Biological:** Genetically engineered or enhanced pathogens could target critical workforces (e.g., energy or water operators) or be used in agroterrorism against food supply chains.
- **Electrical System Attacks:** Beyond cyber, drone swarms (kinetic or electronic warfare) could target substations or transmission lines, as demonstrated in conflicts abroad.

- **Financial System:** Cyberattacks or ransomware on Texas-based financial institutions or payment systems could disrupt economic activity and complicate recovery.
- **Water Infrastructure:** Contamination (physical or cyber-enabled) or sabotage of treatment plants and dams could create public health crises and secondary effects on power generation and industry.

These threats can overlap opportunistically (e.g., a solar storm during hurricane season compounded by opportunistic cyberattacks).

MITIGATION STRATEGIES

Prevention

Foremost, Texas should adopt a strategy of prevention via surveillance, intelligence, and enhanced law enforcement response. For instance, by expanding its intelligence fusion capabilities within the Texas Department of Public Safety's (DPS) fusion center and enhancing information sharing with federal partners (e.g., CISA, FBI, NSA) while asserting state sovereignty to act before a crisis or during one ([CISA, 2024](#)).

Asserting state sovereignty in this context means fully embracing the fact that hostile foreign actors seeking to damage critical infrastructure in Texas, as well as natural disasters, are not solely a federal responsibility; rather, in our dual national/state federal system, there is a clear role and responsibility for the State of Texas to protect its residents. Thus, the State Fusion Center, which describes its mission as

"...a 24/7 unit that works with federal, state, regional, and local law enforcement and serves as the state repository for homeland security information and incident reporting. It provides real-time intelligence support to law enforcement and public safety authorities, and consolidates information and data on suspicious activities and threats from all jurisdictions and disciplines as well as the public." ([Texas Department of Public Safety, n.d.](#))

Unfortunately, Texas is currently structured for a peacetime environment, with at least five separate entities coordinating across multiple agencies, making it difficult to assess a threat and head it off or speed recovery if an attack cannot be stopped. Thus, DPS handles intelligence and law enforcement via its Fusion Center and its investigative arms, while the Texas Division of Emergency Management (TDEM) under Texas A&M, would lead overall recovery coordination through the State Operations Center which is stood up for a particular emergency (TDEM, n.d.), with the PUC and ERCOT handling grid restoration, and finally, the Texas Cyber Command (created in 2025) handling statewide cyber threat intelligence, incident detection, forensics, and coordination with law enforcement. No single agency owns every piece, limiting an effective response to prevent an attack or mitigate its harm if it isn't fully prevented. In this, Texas's critical infrastructure protection structure parallels that of the U.S. intelligence and law enforcement agencies on the eve of the 9/11 terrorist attack—i.e., multiple agencies with overlapping but distinct missions. Texas lawmakers saw and addressed some of these weaknesses when, in 2025, they created the Texas Cyber Command as a centralized state authority for cyber threats to critical infrastructure as well as the Texas Grid Security Commission (housed under TDEM) to evaluate all-hazards risks to the ERCOT grid, including physical and cyberattacks, and to recommend resilience standards. The Grid Security Commission is required to deliver a full all-hazards plan to the legislature by December 2026. The 2026–2030 Texas Homeland Security Strategic Plan also explicitly lists hostile foreign-nation attacks and unmanned systems as priority threats (Texas Department of Public Safety, 2026).

Those steps tighten some of the gaps that existed a few years ago, but they do not create a single operational commander with authority over every piece of the system. In a fast-moving event, the governor can declare a disaster and issue directives, but execution still runs through those separate organizations. A scenario involving coordinated

sabotage teams using drones against substations and transformers would severely test those arrangements. Even so, no state-level structure, including a hypothetical single “Texas DHS,” would make a determined, well-resourced campaign of physical sabotage easy to stop—but its existence might direct attacks elsewhere to targets perceived as being less hardened. The current arrangement is more coordinated than it was before the 2019–2025 reforms, but it is still a networked system rather than a unitary one. Whether that network holds under a true wartime-level physical attack would depend on how quickly intelligence from the Fusion Center reaches operators, how fast TDEM can activate resources, and how well pre-planned hardening and mutual-aid agreements perform—not on the existence of one additional agency.

One area of interest that appears conspicuous by its absence is securing the Gulf Coast, a region of immense importance to Texas and to national security. Coastal and offshore vital infrastructure consists of ports, oil and gas facilities, and even space launch operations. In this region, maritime security is a must, at a minimum, to counter smuggling operations and other cartel threats, as well as hostile nation-state actors. Thus, including coastal security in the fusion center and adding to that an organic ability to react to threats in real time without being wholly reliant on federal assets will be a necessary capability without which hundreds of billions of dollars of infrastructure would be at risk.

Additional key preventative measures include monitoring foreign investments and land acquisitions near critical sites (building on existing scrutiny of adversarial actors), physical surveillance of key nodes (cameras, drone patrols, AI analytics), and border/interior enforcement to detect potential sabotage teams. Public-private information-sharing platforms, modeled on CISA's initiatives but tailored to Texas priorities, can improve early warning. Governor Abbott's 2024 order already advances this by tasking agencies with vulnerability surveys and simulations.

Further, state statutes should be reviewed with an eye toward discouraging gray-zone actions that could result in mass casualties. For instance, if a cell of foreign nationals planned to use mass drones short of open conflict with the intent to damage significant portions of the Texas electrical grid, it is unclear whether such an action would be considered a mere threat to damage infrastructure or, more seriously, a plot to commit murder.

To remedy this weakness, the Legislature could seek to upgrade the penalties for preparatory offenses: for instance, make conspiracy to commit capital murder (or specifically conspiracy to commit murder via attacks on critical infrastructure with terrorist intent) itself a capital felony or first-degree with a higher mandatory minimum or life-without-parole option when multiple deaths are the intended result or when critical infrastructure (e.g., the electrical grid under the Texas Penal code § 28.09) is targeted. The Legislature should also consider expanding or clarifying that attempted capital murder in terrorism contexts carries capital or life imprisonment exposure.

The Legislature should enact stronger terrorism and material-support laws, such as broadening the Texas Penal Code § 76.02 and 76.03, or raise the ceiling so that conspiracy or material support for planned mass-casualty infrastructure attacks can reach capital-level punishment when the intended result is multiple deaths. This could be further enhanced by explicitly including foreign nationals acting as a “cell” or agents of foreign terrorist organizations.

Further, the Legislature should seek to increase penalties for possessing weaponized drones, or drones modified to carry explosives or other military payloads. This would provide law enforcement with additional means to prevent damaging attacks.

Texas law enforcement authorities should also prioritize the early investigation and charging of con-

spiracy/terrorism/material-support cases (including under organized-crime provisions). This should include close coordination with federal authorities (who have broader terrorism tools that can include death eligibility in some cases). Lastly, an effort should be made to improve intelligence sharing, surveillance of high-risk actors, and rapid disruption of plots.

And lastly, the Legislature and the Governor should consider funding and mandating various forms of complementary non-penal deterrence, such as hardening the grid itself (physical/cyber defenses, redundancy, rapid-recovery capabilities), increasing detection of anomalous drone activity near critical sites, and publicizing successful prosecutions of preparatory terrorism cases to raise the perceived risk of detection and severe punishment. In addition, a licensing system for payload-carrying drones could be developed rather than relying solely on the FAA. Further, it should be made explicitly illegal for corporations controlled by adversary nations to possess drones in Texas.

Hardening of Infrastructure

Physical and cyber hardening reduces vulnerability of critical infrastructure, though it isn’t necessarily cost-effective for all scenarios. For the electric grid, utilities should implement North American Electric Reliability Corporation (NERC) reliability standards and consider GMD protections (e.g., series capacitors or neutral blocking devices) where cost-effective, alongside winterization and flood-resistant designs for coastal assets. Cybersecurity hardening involves segmenting IT/OT (Information Technology and Operational Technology) networks², multi-factor authentication, and regular “living off the land” detection exercises per CISA guidance. Physical measures include reinforced perimeters, redundant communications, and drone detection systems around substations and refineries. Water systems require similar segmentation and backup treatment capacity. Texas can incentivize private-

2 An IT/OT network refers to a system that manages Information Technology that manages data, runs business apps, and protects privacy, while Operational Technology controls physical machines, keeps systems safe, and ensures uptime.

sector hardening through regulatory relief, tax credits, or insurance discounts coordinated by the Public Utility Commission and the Texas Department of Emergency Management (TDEM). Redundancy—such as distributed generation and microgrids—further limits single points of failure.

Resilience and Recovery

A rapid recovery minimizes the duration and severity of disruptions. Texas should develop strategic reserves of critical components, particularly large power transformers, which have long lead times, averaging 120 weeks (NERC, 2025). A state or regional cache, potentially managed by the Texas National Guard or TDEM in partnership with utilities, mirrors federal concepts like the DOE Strategic Transformer Reserve—which has been studied, but not implemented, partially because large power transformers are not interchangeable (GAO, 2023)—but with faster and tailored state-level deployment (DeVore, 2023). That this has not been done is due to a few factors, such as the cost of transformers and their long life when operating properly, and the cost of property taxes on expensive equipment. Regarding the latter, installed transformers are taxed, though depreciated over time, while stored transformers are also taxed, though cities or counties can grant temporary abatements under Chapter 312 of the Texas Tax Code. Practically speaking, it makes no economic or business sense for private companies to allow their expensive transformers to sit idle while being taxed in Texas. This leaves the sole practical option being a state-managed emergency supply.

Additionally, there is growing venture capital interest in building transformer manufacturing capacity in Texas, with startup manufacturing firms such as Resolute Grid among them (M. Owenby, personal communication, August 2026). Identifying suitable startups and contracting with them to manufacture some high-voltage transformers would likely spur the creation of a domestic supply chain. Adding additional incentive for American manufacturers, President Donald Trump issued Executive Order 14420, “Declaring a National Emergency to Secure the

United States Bulk-Power System” on August 26, 2026 (EO 14420, 2026). This order starts a process that may require decommissioning large power transformers built in China and banning new installations. In recent years, China has supplied most imported large power transformers, with imports meeting 80% of U.S. demand (Federal Register, 2021).

Lastly, frequent full-scale field exercises—simulating combined natural disaster and adversarial attack scenarios—build coordination among state agencies, ERCOT, utilities, and the private sector while revealing capability gaps. This test should include financial system resilience, including redundant payment paths and contingency liquidity planning.

RECOMMENDATIONS

Texas faces a complex threat landscape where natural hazards, great-power competition, and terrorism can converge. Relying solely on federal resources is insufficient; state-led initiatives offer agility and alignment with Texas’ constitutional role in protecting its citizens.

There are a number of practical actions policymakers should undertake as soon as possible.

Prevention Recommendations

The Legislature should strengthen the Penal Code to discourage infrastructure attacks by upgrading penalties to a capital felony or first-degree felony for the offense of preparing to attack infrastructure to cause mass casualties, enact stronger terrorism and material-support laws, and enhance penalties for possession of weaponized drones or drones modified to carry explosives.

Further, the Governor can strengthen intelligence and counter-espionage efforts targeting adversarial actors. This may be done by expanding the DPS-led Fusion Center and linking its intelligence function to actionable law enforcement action with the Texas Rangers, county sheriff’s offices, city police, and the National Guard and State Guard.

Hardening Recommendations

The Legislature should fund and the Executive fully implement the findings from Governor Abbott's 2024 executive order, namely, the vulnerabilities found as a result of the TDEM-led surveys on state and local government and critical infrastructure; the PUC best practices lessons from its annual tabletop exercise; the foreign adversary cyberattack tabletop best practices; the electromagnetic (EMP) best practices; and the ERCOT dedicated communications channel for load requests.

The Legislature should author statute to incentivize or require risk-based hardening standards for critical infrastructure owners by allowing for a separate return on investment credit for specific key hardware. As a stopgap, the Public Utility Commission of Texas may approve rules that mandate this investment.

Resilience and Recovery Recommendations

The Legislature should establish dedicated funding for strategic reserves (transformers, medical supplies) under TDEM oversight.

The Legislature should fund and the Executive conduct regular, integrated field exercises across threat types, led by TDEM or the National Guard, depending on the scenario. These events will likely produce highly sensitive, classified information once synthesized, so the National Guard may be the best entity to lead such efforts.

Similarly, the Governor should request that state warehouses expand medical and pharmaceutical stockpiles (including countermeasures for biological threats) for rapid distribution to essential workers. Further, the Governor should request that pre-positioned purification equipment, mobile treatment units, and mutual-aid agreements are available to water infrastructure recovery.

CONCLUSION

By prioritizing prevention, hardening, and recovery, Texas can significantly reduce the probability and subsequent consequences of catastrophic infrastructure failures, safeguarding its people and economy regardless of the threat vector. ■

REFERENCES

- Abbott, G. (2024, Nov. 19). *Executive Order GA-49*. Office of the Texas Governor. https://gov.texas.gov/uploads/files/press/EO-GA-49_Protecting_Critical_Infrastructure_FINAL_11-19-2024.pdf
- Cybersecurity & Infrastructure Security Agency (CISA). (2024, February 7). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure*. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
- DeVore, C. (2023). *Texas Defense*. Texas Public Policy Foundation. <https://www.texaspolicy.com/wp-content/uploads/2023/09/2023-09-TexasDefense-ChuckDeVore.pdf>
- DeVore, C. (2024, October 16). *You won't believe how Biden-Harris team responded when drones buzzed sensitive US military bases*. Fox News. <https://www.foxnews.com/opinion/you-wont-believe-how-biden-harris-team-responded-when-drones-buzzed-sensitive-us-military-bases>
- Edwards, C., O'Loughlin, R., & Bearn, L. (2026, July 2). *Russia's UAV Campaign Over Europe*. International Institute for Strategic Studies. <https://www.iiss.org/research-paper/2026/06/russias-uav-campaign-over-europe/>
- Executive Order 14420. (2026, August). *Declaring a National Emergency to Secure the United States Bulk-Power System*. <https://www.whitehouse.gov/presidential-actions/2026/08/declaring-a-national-emergency-to-secure-the-united-states-bulk-power-system/>
- Federal Register. (2021, November 18). *Publication of a Report on the Effect of Imports of Transformers and Transformer Components on the National Security: An Investigation Conducted Under Section 232 of the Trade Expansion Act of 1962, as Amended*. <https://www.federalregister.gov/documents/2021/11/18/2021-24958/publication-of-a-report-on-the-effect-of-imports-of-transformers-and-transformer-components-on-the>
- Gertz, B. (2026, July 22). *Congress told U.S. ill-prepared for China's 'unrestricted warfare' Hegseth confirms China, Russia helping Iran with targeting; Army deploys new hypersonic missile to Guam*. Washington Times. www.washingtontimes.com/news/2026/jul/22/inside-ring-congress-told-us-ill-prepared-chinas-unrestricted-warfare
- Greene, S., Kagan, D., Boulègue, M., Ålander, M., & White, D. (2026, March 31). *War Without End: Deterring Russia's Shadow War*. Center for European Policy Analysis. <https://cepa.org/comprehensive-reports/war-without-end-deterring-russias-shadow-war/>
- Lloyd's. (2013). *Solar Storm Risk to the North American Electric Grid*. <https://assets.lloyds.com/assets/pdf-solar-storm-risk-to-the-north-american-electric-grid/1/pdf-Solar-Storm-Risk-to-the-North-American-Electric-Grid.pdf>
- Lubold, G., & Strobel, W. (2023, September 4). *Chinese Gate-Crashers at U.S. Bases Spark Espionage Concerns*. Wall Street Journal. <https://www.wsj.com/politics/national-security/chinese-gate-crashers-at-u-s-bases-spark-espionage-concerns-cdef8187>
- Lucie, H. (2019, May). *How FEMA Could Lose America's Next Great War*. Homeland Security Affairs, 15(1). https://www.hsaj.org/resources/uploads/2019/05/hsaj_volume-15_issue-1_How-FEMA-Could-lose-Americas-Next-Great-War_042919.pdf

- Mitch, I. (2025, April 11). *Could China's U.S. Spies Conduct Physical Sabotage in a Conflict?* RAND. <https://www.rand.org/pubs/commentary/2025/04/could-chinas-us-spies-conduct-physical-sabotage-in.html>
- MITRE-Harris. (2024, March 13). *MITRE-Harris Poll Public Perceptions on Securing Critical Infrastructure*. <https://www.mitre.org/sites/default/files/2024-03/PR-24-0806-MITRE-Harris-Poll-Securing-Critical-Infrastructure.pdf>
- North American Electric Reliability Corporation (NERC). (2025, May). *2025 Summer Reliability Assessment*. https://www.nerc.com/globalassets/programs/rapa/ra/nerc_sra_2025.pdf
- SB 2312. Enrolled. 89th Texas Legislature. Regular. (2025). <https://legiscan.com/TX/bill/SB2312/2025>
- Texas Department of Public Safety. (2026, February 3). *Texas Homeland Security Strategic Plan 2026–2030*. https://www.dps.texas.gov/sites/default/files/documents/director_staff/txhomelandsecstratplan2026-2030.pdf
- Texas Department of Public Safety. (n.d.). *Texas Fusion Center*. Retrieved August 27, 2026, from <https://www.dps.texas.gov/section/homeland-security/texas-fusion-center#:~:text=It%20provides%20real%2Dtime%20intelligence%20support,as%20well%20as%20the%20public>
- Texas Division of Emergency Management (TDEM). (n.d.). *About Us*. Retrieved August 27, 2026, from <https://tdem.texas.gov/about>
- United States Government Accountability Office (GAO). (2023). *ELECTRICITY GRID DOE Could Better Support Industry Efforts to Ensure Adequate Transformer Reserves* [Report to Congressional Committees, GAO-23-106180]. <https://www.gao.gov/assets/gao-23-106180.pdf>

ABOUT THE AUTHOR



Chuck DeVore is the Chief National Initiatives Officer at the Texas Public Policy Foundation. He writes about the economy, energy, and national security. During session, the Texas Legislature frequently invites him to testify on election integrity and other topics. He guides the Foundation's national work in border security, election integrity, energy, and conservative criminal justice reform. He authored three books: *Crisis of the House Never United – A Novel of Early America*, *The Texas Model: Prosperity in the Lone Star State and Lessons for America*, and *China Attacks*. He regularly appears on Fox News and is a senior contributor at The Federalist.

For six years until he termed out in 2010, DeVore represented almost 500,000 people in the California State Assembly where he was vice chairman of the Committee on Revenue and Taxation as well as a member of the Budget Committee. DeVore was a senior assistant to a U.S. congressman from 1988 to 1990, and in the Reagan-era Pentagon, DeVore was a special assistant for foreign affairs.

Prior to his election, DeVore was an executive in the aerospace industry for 13 years analyzing technology and corporate capabilities and working in business development.

DeVore retired from the U.S. Army as a lieutenant colonel, having served in both the National Guard and the Reserves as an intelligence officer.

