Texas Public
POLICY FOUNDATION
BETTER TECH FOR TOMORROW

# THE PROMISE AND PERIL OF AI: IMPACT ON CRITICAL INFRASTRUCTURE

## WHAT IS CRITICAL INFRASTRUCTURE?

Critical infrastructure refers to 16 sectors essential to the economy, public health, safety, and security, including communications, energy, water systems, emergency services, and financial services. While traditionally insulated from digital threats, the rapid digitalization of these systems has introduced significant vulnerabilities. Historically air-gapped systems are now increasingly interconnected, creating new opportunities for cybercriminals to infiltrate and exploit.

**Interested in learning more about Artificial Intelligence?**

Scan the QR code above to access our latest research.

## HOW AI IMPACTS CRITICAL INFRASTRUCTURE

- **Cyberattack Amplification**
  - Enhanced Hacking Capabilities: AI enables cybercriminals to improve attack precision, automate exploits, and accelerate discovery of vulnerabilities. Tools powered by Generative AI (GAI) can bypass traditional defenses with greater efficiency.
- **Spear Phishing and Social Engineering:**
  - Attackers use AI to craft convincing emails or communications in a victim's language, tone, or even voice, making it easier to deceive employees. For instance, GAI can generate customized emails that mimic colleagues' or executives' communication styles to lure victims into compromising sensitive systems.
- **State-Sponsored Threats**
  - Nearly 60% of critical infrastructure cyberattacks are perpetrated by state-affiliated actors, often targeting water, energy, and communication systems to destabilize systems or steal sensitive data. In one instance, Russian hackers targeted Muleshoe, Texas, infiltrating its water treatment systems to create potential harm.

**Read More** →

## RISKS OF AI IN CYBERSECURITY

- **Increased Attack Precision:**
  - AI provides attackers with tools to automate exploitation, refine malware, and conduct adversarial machine learning to bypass security systems. This is especially problematic in sectors like energy and nuclear facilities, where disruptions can have catastrophic consequences.
- **Extended Network Infiltration:**
  - Hackers are maintaining access to systems for prolonged periods. A Chinese campaign targeting American transportation hubs and infrastructure went undetected for over five years.
- **Ransomware Escalation:**
  - AI allows attackers to develop more adaptive ransomware that evades detection. Ransom demands often cripple small organizations, forcing many to pay to minimize service disruptions.

# LEGISLATIVE SOLUTIONS

**The Texas Senate WAR Committee Interim Report provided seven policy recommendations to bolster Texas' critical infrastructure cybersecurity against AI enhanced attacks.**

- **Require** all Texas water systems to isolate their SCADA networks or, if applicable, equivalent operational IT infrastructure from the internet;
- **Support** the expeditious establishment of the additional RSOCs DIR is currently developing plans for;
- **Grant** DIR the authority to conduct cybersecurity assessments of public water systems;
- **Require** all Texas water systems to utilize multi-factor authentication protocols for users to obtain access to their SCADA networks or, if applicable, equivalent operational IT infrastructure, and grant DIR authority to update that requirement by rule as multi-factor authentication technology advances;
- **Expand** access to cybersecurity-related services procured through or from DIR to include private water systems in Texas;
- **Eliminate** the effective exemption from required cybersecurity training for public water system employees who use local government computer systems or databases for less than 25% of their required duties; and
- **Require** all Texas water systems to report to DIR all security incidents resulting in the unauthorized disclosure of sensitive personal information, the introduction of ransomware, or the disruption of water system operations.