5 STEPS TO PREPARE CRITICAL INFRASTRUCTURE FOR A CYBER WAR

In an era of growing cyber threats, protecting the nation's critical infrastructure is a priority. The U.S. Intelligence Community's 2025 Annual Threat Assessment warns that China and Russia aim to "pre-position access on U.S. critical infrastructure for asymmetric options." With cyber attacks targeting the energy, water, transportation, and communications sectors, the nation must prepare now for disruptions to essential services.

In December 2024, over 200 participants from 70 organizations—including federal agencies, state and local governments, and private sector operators—gathered at MITRE's McLean, VA, campus for a classified tabletop exercise simulating a prolonged cyber conflict. The event revealed the urgent need for infrastructure owners/operators, government agencies, and communities to shift from addressing isolated cyber incidents to preparing for large-scale cyber conflicts lasting weeks to months. As one participant noted, "We were prepared for a cyber attack, not a cyber war."

This paper summarizes key takeaways from MITRE's tabletop exercise and subsequent stakeholder discussions on infrastructure resiliency, societal preparedness, and coordinated national-local responses. It delineates observations, challenges, and actionable recommendations, emphasizing the importance of collaboration, contingency planning, and operational readiness for prolonged cyber disruptions.

While security considerations limit the findings shared here, full details are available to U.S. critical infrastructure owners/operators and government entities. For access to the "For Official Use Only" or classified After Action Report, email CICSTTX@mitre.org.

1. Create a Civil Defense Mindset

Stakeholders stressed the need to prepare the public for disruptions to essential services like electricity, water, telecommunications, and transportation during a cyber conflict. Infrastructure owners must collaborate with federal, state, and local governments to align restoration priorities and coordinate emergency responses. This requires adopting a civil defense mindset—a framework that emphasizes education, awareness, and self-reliance to ensure citizens, communities, and businesses understand risks and can respond effectively. Strengthening the nation's ability to counter adversary-driven disruptions will also require contributions from state, local, tribal, and territorial governments; the private sector; academia; and civil society—not just the federal government.

2. Manage Limited Resources During Emergencies

Disruptions to interconnected infrastructure sectors can quickly overwhelm response efforts, as mutual aid agreements may fail in widespread incidents. In addition, uncoordinated restoration and prioritization activities in the federal, state, and private sectors can lead to delays and prolonged outages. Many contingency plans focus on isolated events rather than sustained outages or resource shortages caused by cyber warfare. To mitigate these risks, infrastructure owners/operators should conduct exercises to test their contingency plans, and state, local, tribal, and territorial governments should work with private sector operators to address interdependencies and resource orchestration using scenarios that simulate widespread impacts.

MITRE

3. Plan for Operations Under Extreme Conditions

Maintaining essential infrastructure services during extreme conditions is critical, especially in the face of cyber warfare, which poses unique challenges beyond those of natural disasters. For example, cyber attacks against multiple interconnected critical infrastructures can create cascading impacts that devastate cities and states in ways that make recovery exceedingly difficult. Planning for the scope and scale of these effects, which could last for weeks, is vitally important. In addition, pre-identified regulatory easements can expedite recovery efforts, while training personnel for manual or disconnected operations is a must if automated systems are compromised. Stakeholders must enhance cyber resiliency plans and ensure personnel are prepared to manage manual operations during prolonged crises.

4. Strengthen Emergency Communications Systems

Stakeholders often overestimate the strength of Primary, Alternate, Contingency, and Emergency (PACE) communications plans. Voice communications, often used as a default backup, may not sustain operations during prolonged outages caused by cyber warfare. The limited number of backup communication options between individual operators and the government further exacerbates the ability of key stakeholders to share situational awareness and collaborate on response actions. In addition, the growing threat of deepfakes underscores the need for authentication. Infrastructure owners/operators and state, local, tribal, and territorial governments should strengthen communication protocols by improving backup systems and implementing authentication to ensure resilience during cyber incidents.

5. Ensure Workforce Readiness for Emergencies

Workforce availability may decline during prolonged emergencies due to personal or contractual challenges, threatening critical infrastructure operations. To mitigate these risks, stakeholders should create contingency staffing plans, provide long-term support for critical staff and their families, and train personnel to manage workforce shortages during extended emergencies.

Conclusion

Protecting critical infrastructure from evolving cyber threats requires proactive collaboration and innovative strategies. Stakeholders must build resilience by preparing communities, improving PACE communication plans, and training personnel for manual operations and contingency scenarios. MITRE, working in partnership with industry and government, is advancing research to mitigate these challenges. We must all work together to strengthening our defenses, ensuring recovery, and building lasting resilience in the face of cyber warfare.