September 2025

ICIT

Resilient Foundations: Securing America's Critical Infrastructure in a New Era

Cory Simpson
CEO of ICIT,
Founder & CEO of Gray Space Strategies

Barry Mainz
CEO of Forescout Technologies

www.icitech.org

Table of **Contents**

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s).

To learn more, please visit www.icitech.org

CyberRisk ALLIANCE | Thank you to our Strategic Partner **CyberRisk Alliance** | cyberriskalliance.com

Resilient Foundations

Critical infrastructure—our power grids, transportation systems, water utilities, and communications networks that sustain modern life—is the backbone of America's security and prosperity. These systems enable commerce, deliver essential services, and connect communities. Their strength defines national resilience.

That significance makes them a top priority for foreign adversaries. Sophisticated campaigns such as Volt Typhoon and Salt Typhoon have already infiltrated operational technology (OT) environments across multiple sectors. Adversaries are present—probing for vulnerabilities and preparing capabilities to act at their discretion.

Meanwhile, the technological environment is advancing rapidly. Quantum breakthroughs threaten the encryption that protects sensitive systems. Artificial intelligence accelerates both the discovery and exploitation of weaknesses. Globalized supply chains embed risks deep within hardware and sensors spread throughout infrastructure.

This convergence creates a defining moment. By prioritizing resilience, Congress can transform today's vulnerabilities into a foundation of enduring national strength—securing the systems that power daily life and reinforcing the trust that underpins public safety, economic security, and national defense.

The New Era of Vulnerabilities

Critical infrastructure is more interconnected, automated, and data-driven than ever before. This modernization drives efficiency and innovation, yet it also creates systemic fragility. Identical programmable logic controllers (PLCs), shared operating systems, and repeated configurations form a monoculture where a single exploit can ripple across entire sectors.

At the same time, emerging technologies are reshaping the threat environment:

Post-Quantum Cryptography (PQC)

Advances in quantum computing are moving rapidly toward the ability to break widely-used encryption in seconds. Hardware and networking breakthroughs from leading chipmakers are accelerating this reality. Preparing critical systems for PQC is no longer theoretical—it is an essential step to safeguard the confidentiality and integrity of infrastructure in the years ahead.

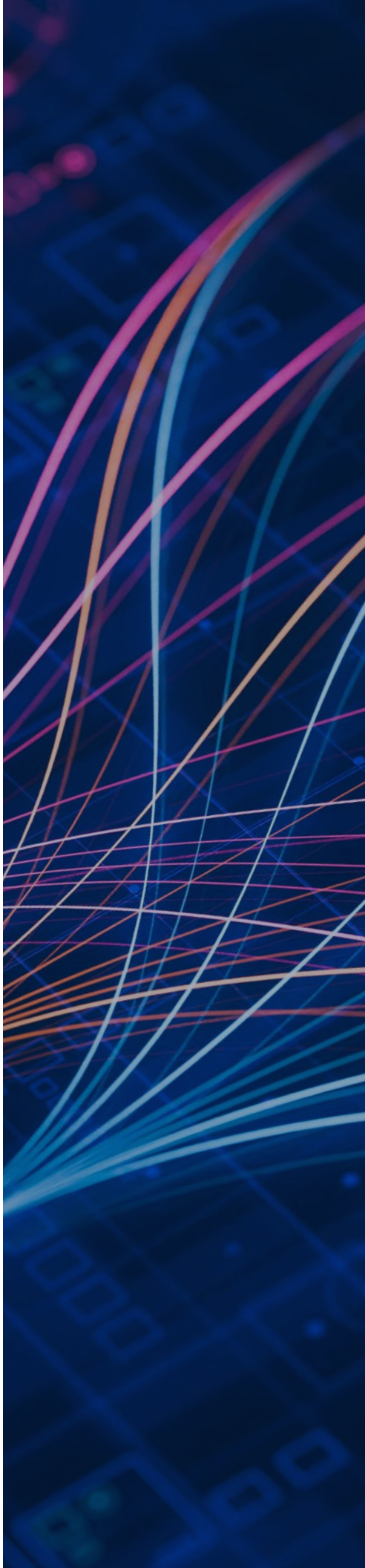
Artificial Intelligence (AI)

AI accelerates the discovery of device-specific vulnerabilities and enables adversaries to scale attacks across similar systems nationwide. Yet AI also strengthens defense. Predictive analysis can identify weaknesses before they are exploited, automated patching can speed remediation, and intelligent decoys can redirect attackers. AI will either destabilize defenses or serve as a force multiplier for resilience.

Light Detection and Ranging (LiDAR)

LiDAR provides high-resolution 3D mapping that improves efficiency and safety in transportation, logistics, and port operations. Sensors sourced from adversarial supply chains, however, risk embedding vulnerabilities deep within infrastructure. Trusted sourcing and secure integration can ensure LiDAR delivers its benefits without becoming an avenue for espionage or disruption.

Taken together, these trends reveal a central truth: resilience depends on visibility and proactive defense. Leaders must be able to see every device connected to their networks, understand how technologies interact, and act quickly when vulnerabilities emerge. Continuous monitoring, intelligent automation, and trusted supply chains are no longer optional—they are the foundation of resilience in a new era of infrastructure security.



Congressional Responsibility

The federal government—and Congress in particular—has a unique role in safeguarding critical infrastructure. Leadership from Washington can ensure that resilience is prioritized, funded, and coordinated across all levels of government. Proactive leadership strengthens trust, protects stability, and prevents cascading disruption.

Current federal investments in infrastructure security mark important progress, but gaps remain, especially at the state and municipal level. Smaller communities, which often operate with limited resources and expertise, can become entry points into larger interconnected systems. Extending support to these jurisdictions is essential for national resilience.

Congress has the opportunity to close these gaps through sustained funding, targeted technical assistance, and legislation that accelerates modernization. A comprehensive, whole-of-nation approach—federal leadership combined with local execution—ensures that every community contributes to a secure foundation. The right legal, policy, and budgetary frameworks can transform infrastructure protection from fragmented efforts into a coordinated national strength.

A Roadmap for Resilience

Resilience is built through deliberate action. A clear roadmap can guide Congress, infrastructure operators, and communities toward a stronger foundation:

1. **Lead with Urgency**

   Recognizing the scale of the challenge is the starting point. Transparent communication about evolving risks and the proactive steps underway creates shared awareness and builds the consensus needed for sustained action.

2. **Invest in Modernization**

   Establish multi-year funding streams dedicated to infrastructure resilience. Prioritize sectors and communities with the highest risk and least capacity, ensuring resources flow where they can deliver the greatest impact. Investments should accelerate PQC-ready systems, expand AI-enabled defenses, retrofit outdated OT environments, and develop the skilled workforce required to secure them.

3. **Strengthen Local Capacity**

   National resilience depends on the ability of every community to defend its lifelines. Technical assistance, public-private collaboration, and training programs can ensure even the smallest jurisdictions contribute to collective security.

4. **Engage and Educate**

   Public awareness is essential to sustaining political will. Highlighting successful protection initiatives, showing the value of investments, and demonstrating how resilience benefits daily life reinforce trust and ensure accountability.

Together, these steps form a blueprint for resilience. They transform vulnerabilities into opportunities for strength, ensuring that America's lifeline systems remain secure, reliable, and trusted in the face of accelerating change.

The Defining Moment for American Resilience

America's critical infrastructure sits at the intersection of rising threats and historic opportunity. The technologies shaping this new era—quantum, AI, and intelligent sensors—will determine whether vulnerabilities expand or unprecedented strength is built.

Congress holds the responsibility to lead with foresight. By acting now, investing in modernization, and sustaining national commitment, it can secure the systems that sustain our daily life and strengthen the trust that underpins security, prosperity, and freedom.

This is the defining moment for American resilience. Seizing it ensures the backbone of the nation remains strong for generations to come.

About

Cory Simpson

CEO of ICIT | Founder & CEO of Gray Space Strategies

Cory Simpson · ICIT · Gray Space Strategies

Cory Simpson has over twenty years of experience in government, the military, and the private sector, specializing in national security, cybersecurity, business, law, and strategy. He served in the U.S. Army Judge Advocate General's Corps from 2004 to 2016 and continues as a legal advisor to U.S. Army Cyber Command. His military career includes roles as general counsel, prosecutor, and national security law advisor, with multiple combat tours and extensive trial experience. Cory is the CEO of Gray Space Strategies, a strategic advisory firm, and the Institute for Critical Infrastructure Technology (ICIT), a nonprofit think tank dedicated to critical infrastructure security. He also serves as a senior advisor to CSC 2.0, continuing the work of the U.S. Cyberspace Solarium Commission, and is on the Board of Directors for the Cyber Guild. Cory holds a Master of Laws in Military Law, a Juris Doctorate, and a BA in accounting with a minor in philosophy. He is globally recognized for creating effective solutions to complex challenges.

Barry Mainz

CEO of Forescout Technologies

Barry Mainz · Forescout Technologies Inc.

Barry Mainz brings more than 25+ years of experience in executive leadership, global sales, marketing, product-led growth, and product development to Forescout. In addition to being an Operating Partner at Crosspoint Capital Partners, Barry most recently served as COO of Malwarebytes, responsible for development and execution of the go-to-market strategy. Prior to joining Malwarebytes, Mainz was CEO and a member of the Board of Directors for MobileIron. Before MobileIron, he served as President of Wind River Systems (an Intel subsidiary). Additionally, Mainz has held leadership roles, as well as advisory and board positions, at private and public companies such as Mercury Interactive, Makara (acquired by Red Hat, Inc.), and Sun Microsystems. He currently also serves on the Board of Directors of BlackBerry. Barry holds a BA in Communications from San Francisco State University.

About

ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s).

To learn more, please visit www.icitech.org

CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through its trusted information brands, network of experts, and innovative events it provides cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. CyberRisk Alliance brands include SC Media, the Official Cybersecurity Summits, TechExpo Top Secret, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, Security Weekly, ChannelE2E, MSSP Alert, and LaunchTech Communications.

ICIT

www.icitech.org