PAST IS PROLOGUE:

Creating a Civil Defense Mindset to Address Modern Cyber Threats

May 2025

Mark Bristow and Irving Lachow
– The MITRE Corporation

> THE GROWING THREAT OF CYBERATTACKS ON CRITICAL INFRASTRUCTURE FROM FOREIGN ACTORS PROVIDES AN URGENT EXAMPLE OF THE NEED FOR RENEWED INTEREST IN CIVIL DEFENSE.
>
> —PROJECT BLUE BOOK [1]

The United States must move beyond its current emergency preparedness mindset, which is primarily focused on natural disasters and isolated terrorist attacks. Cyber attacks can disrupt multiple critical infrastructures across the nation in ways that are quite different from natural disasters. For example, it is possible to target key pieces of equipment that are difficult to fix or replace. Adversaries can create cascading failures and alter their tactics to counteract defensive responses. They can also launch attacks over a period of weeks or months, creating a cascading set of crises that instigate new effects or exacerbate existing disruptions unlike the dynamics experienced during a natural disaster. One thing is clear: “The homeland is no longer a sanctuary” [2]. Our nation must update its conception of emergency preparedness to include elements of traditional civil defense.

Cyber Threats to Critical Infrastructure

Concerns about cyber threats to critical infrastructure have existed for decades. However, two recent developments have heightened awareness and deepened concerns about the risk of sustained and widespread cyber attacks on our homeland.

The first major development is the growing threat to critical infrastructure posed by the People’s Republic of China (PRC). The PRC has a history of using cyber means for espionage, but it now poses a serious threat to our nation’s economic and national security. According to the Office of the Director of National Intelligence (ODNI): “If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces” [3].

Several private sector companies have reached similar conclusions. For example, Microsoft has stated that the PRC’s Volt Typhoon campaign “is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises” [4]. Similarly, Mandiant’s chief analyst has noted that “the Volt Typhoon campaign included ‘very deliberate targeting of critical infrastructure’ installations and represents a major shift by Chinese hacking teams known mostly for economic espionage and IP theft” [5]. Another PRC actor, Salt Typhoon, is concerning because it has demonstrated the PRC’s ability to embed itself into the core networks of our nation’s major telecommunications providers.

ODNI has specifically called out these two campaigns and the threats they pose to U.S. critical infrastructure: “The PRC’s campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure" [3].

The second development worth noting is that Russia has launched sustained cyber campaigns against multiple critical infrastructure sectors in Ukraine [6]. There is a well-documented history of Russian cyber actors targeting Ukrainian infrastructures, causing a great deal of collateral damage across the world [7].[1] The frequency of such attacks increased at the start of the war in Ukraine. As ODNI has noted, "Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware" [3].

Russia has demonstrated both the technical acumen and the willingness to attack the infrastructures of other countries. Reports of Russian incursions into the U.S. energy sector for more than a decade indicate that Russia likely has the access needed to cause harm to the United States [8]. Other sectors have also been targeted: "Since at least March 2016, Russian government cyber actors—hereafter referred to as 'threat actors'—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors" [9].

Revitalizing Civil Defense

During the Cold War, U.S. citizens were aware that the government had a limited ability to protect them from the risks posed by nuclear weapons and intercontinental ballistic missiles. It was up to them to take some responsibility for protecting themselves. That mindset began to shift after the fall of the Berlin Wall in 1989. By the early 2000s, the United States' Cold War concept of civil defense had shifted to a focus on all-hazards emergency management. All-hazards approaches are important and useful, but they fall short when trying to address sustained cyber attacks against multiple critical infrastructure sectors throughout the nation.

A risk-based approach, as called for in the White House Executive Order (EO) Achieving Efficiency Through State and Local Preparedness, is well suited for helping the United States address nation-state cyber threats targeting critical infrastructure. The EO makes this point clear: "Citizens are the immediate beneficiaries of sound local decisions and investments designed to address risks, including cyber attacks, wildfires, hurricanes, and space weather" [10].

Our nation will benefit from a revitalization of a civil defense mindset, which was created to help citizens, communities, and others outside of government prepare for and withstand major infrastructure outages. Two areas where civil defense principles must be applied are (1) education and awareness and (2) emergency preparedness training.

[1] These incidents would have been worse if various companies had not provided technical support to Ukrainian defenders. See [14].

Education and Awareness

A key element of the United States' approach to civil defense during the Cold War was a sustained educational effort funded by the federal government. These ongoing activities included creating films and print media that "gave Americans information on how to prepare themselves and their homes in the case of a nuclear attack. … Audiences of both the film and print sources learned specific skills on how to ensure their safety in the case of emergency" [11]. It may be time to envision what a modern version of such a program would entail.

Policymakers are challenged to determine the appropriate roles of the private and public sectors in such an awareness campaign. While historically the federal government has reached out to citizens about civil defense issues, the evolution of technology and increasing distrust of government institutions may require a different approach moving forward.[2] The private sector and civil society are more likely to capture the attention and trust of large segments of the U.S. population. However, it is uncertain whether they are motivated to pursue courses of action that support this goal.

Training

The Federal Emergency Management Agency's (FEMA) Community Emergency Response Team (CERT) program seeks to "educate volunteers about disaster preparedness for the hazards that may occur where they live" [12]. The training focuses on equipping U.S. citizens with basic skills in fire safety, light search and rescue, team organization, and disaster medical operations.

So far, this program has trained 600,000 people. Although this seems substantial, considering the U.S. population is 345 million, it may be beneficial to explore ways to significantly increase that number. Simultaneous disruptions across multiple regions and critical infrastructure sectors would quickly exhaust our supply of trained experts and responders. In comparison, the government of Taiwan aims to provide similar training to 400,000 citizens, which represents approximately 1.7 percent of the country's total population of 24 million [12]. For the United States to match Taiwan's goal of having one CERT trainee for every 60 citizens, FEMA would need to train 5.8 million people. This is nearly 10 times the number of people currently trained.

Given the Trump Administration's focus on individual, local-, and state-level responsibility for preparedness and response—"It is the policy of the United States that State and local governments and individuals play a more active and significant role in national resilience and preparedness" [10]—our nation must explore new ways to increase the number of citizens equipped with the knowledge and training needed to assist during major disasters.

Recommendations

U.S. critical infrastructure is facing a possible scenario where cyber attacks could strike multiple sectors simultaneously with disruptions lasting for weeks or months. To be resilient during such a crisis, we must learn from the past and revive a civil defense mindset. This will require reimagining emergency preparedness so our citizens, communities, and businesses are aware of potential risks and are equipped to respond to them. A civil defense mindset will increase resiliency, which will serve to both minimize harm to the nation

[2] Over the last 60 years, the percentage of Americans who trust the government to "do what is right" has dropped from over 70 percent to approximately 20 percent. See [15].

and deter attacks in the first place by reducing the potential benefits adversaries would gain by launching such attacks.

When it comes to education and awareness, the U.S. government needs to explore the best options for shifting the country's collective mindset. Should federal, state, or local governments provide funding to the private sector and let them take the lead or should this be a governmental function? Should this topic be addressed in schools as it was decades ago? There are many questions that need to be answered, and the authors urge our nation's leaders to begin addressing these issues.

At the same time, action needs to be taken to bolster our nation's ability to respond to the threats posed by adversary-driven disruptions to critical infrastructure. We should not rely solely on the federal government to train citizens and prepare communities—state, local, tribal, and territorial governments; the private sector; academia; and civil society must also play a role. States like Virginia, Texas, and Massachusetts have created programs that address cyber threats to critical infrastructure. For example, Virginia's Project Blue Book [2] specifically addresses the importance of civil defense measures, while Texas' new Cyber Command [13] seeks to counter nation-state threats to Texas' critical infrastructure sectors via public-private partnerships, training programs, and planning/exercise activities. The authors recommend research to determine if these efforts are effective and if government agencies should seek to develop similar programs across other states and localities.

References

[1] The Blue Book Project, “Civil defense: From the Cold War to contemporary threats,” Virginia Department of Emergency Management, n.d. [Online]. Available: https://www.vaemergency.gov/aem/blue-book/civil-defense-from-the-cold-war-to-contemporary-threats.pdf.

[2] Virginia Department of Emergency Management, “The Blue Book Project,” 2024. [Online]. Available: https://www.vaemergency.gov/divisions/commonwealth-coordination-bureau/planning/project-blue-book.

[3] Office of the Director of National Intelligence, “Annual threat assessment of the U.S. intelligence community,” March 2025. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[4] Microsoft Threat Intelligence, “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques,” 25 May 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/emerging-threats/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/?msockid=3f19e70d8cfb66ea384ff2b48d566717.

[5] R. Naraine, “Mandiant Intelligence chief raises alarm over China’s ‘Volt Typhoon’ hackers in US critical infrastructure,” SecurityWeek, 25 October 2023. [Online]. Available: https://www.securityweek.com/mandiant-intelligence-chief-raises-alarm-over-chinas-volt-typhoon-hackers-in-us-critical-infrastructure/.

[6] G. B. Mueller, B. Jensen, B. Valeriano, R. C. Maness and J. M. Macias, “Cyber operations during the Russo-Ukrainian War: From strange patterns to alternative futures,” Center for Strategic and International Studies, July 2023. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf?VersionId=tIzsIXBig6NG2QKBsqTIOIf0wENNeo87.

[7] A. Greenberg, “The untold story of NotPetya, the most devastating cyberattack in history,” Wired, 22 August 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[8] Cybersecurity and Infrastructure Security Agency, “Tactics, techniques, and procedures of indicted state-sponsored Russian cyber actors targeting the energy sector,” 24 March 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

[9] Cybersecurity and Infrastructure Security Agency, “Russian government cyber activity targeting energy and other critical infrastructure sectors,” 16 March 2018. [Online]. Available: https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors.

[10] D. J. Trump, “Achieving efficiency through state and local preparedness,” The White House, 18 March 2025. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/03/test/.

[11] Wikipedia, “Civil defense in the United States,” 14 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Civil_defense_in_the_United_States.

[12] Federal Emergency Management Agency, “Community Emergency Response Team (CERT),” 4 April 2025. [Online]. Available: https://www.fema.gov/emergency-managers/individuals-communities/preparedness-activities-webinars/community-emergency-response-team.

[13] Office of the Texas Governor, “Emergency item: Texas cyber command,” n.d. [Online]. Available: https://gov.texas.gov/uploads/files/press/GA_TEXAS_CYBER_COMMAND__SOST_onepager.pdf.

[14] G. Rattray, “CDAC supports and endorses the establishment of cyberspace funds,” Cyber Defense Assistance Collaborative, CRDF Global, 9 January 2024. [Online]. Available: https://crdfglobal-cdac.org/supports-cyberspace-funds/.

[15] Pew Research Center, “Public trust in government: 1958-2024,” 24 June 2024. [Online]. Available: https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/.

About the Authors

Mark Bristow is the Director of MITRE's Cyber Infrastructure Protection Innovation Center, where he leads efforts to enhance the resilience of critical infrastructure against cyber and non-kinetic threats. With over two decades of experience in cybersecurity, including key roles in responding to high-profile incidents like the Ukrainian power grid attack and breaches of U.S. election infrastructure, he is passionate about protecting critical infrastructure. An advocate for mentorship and education, Bristow shares his expertise as a certified SANS instructor and frequent speaker on industrial control systems security.

Dr. Irving Lachow is a Senior Principal, Cyber Strategy and Policy at MITRE. He has spent over 30 years working at the intersection of technology and policy issues and has held leading positions in government, industry, and academia. He is currently affiliated with the Center for Strategic and International Studies and Stanford University's Center for International Security and Cooperation.

About MITRE

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE