Irregular Warfare Center
PRISM Insights

America Needs a National Irregular Warfare Stress Test

By Dr. Sandor Fabian

23 September 2026

Dr. Sandor Fabian is a contractor currently serving as the Deputy Regional Adviser for U.S. Africa Command in the Irregular Warfare Center and the IWC Functional Area Networks.

The United States regularly tests its ability to respond to disasters, cyber incidents, terrorist attacks, financial shocks, and military crises. The Department of War exercises combat forces, the Cybersecurity and Infrastructure Security Agency (CISA) works with critical infrastructure operators, states rehearse emergency response, and financial regulators stress-test banks. These efforts often involve multiple agencies, regional partners, and pre-positioned resources. Yet they rarely test, on a national scale and over sustained time, how simultaneous disruptions across military, civilian, economic, and information systems could combine into a single adversary campaign. That integration gap is becoming increasingly dangerous.

The United States is not ignoring these vulnerabilities. Across government, substantial efforts already exist to protect infrastructure, improve cybersecurity, counter foreign influence, strengthen emergency preparedness, and secure military logistics. The problem is how these challenges are conceptualized. Government institutions tend to divide threats according to organizational responsibilities. A ransomware incident becomes a cybersecurity problem. Sabotage becomes a law-enforcement problem. Manipulated information becomes a foreign-influence problem. Port disruption becomes a transportation problem. Supply-chain interference becomes an economic-security problem. An adversary has no reason to respect those bureaucratic boundaries.

Consider the 2021 Colonial Pipeline ransomware attack. Malicious actors compromised the company's business systems, prompting the company to disconnect systems associated with pipeline operations. Fuel deliveries were temporarily disrupted across significant portions of the southeastern United States. The Government Accountability Office subsequently pointed to the attack as evidence of persistent weaknesses in critical-infrastructure cybersecurity. Colonial Pipeline was not a foreign state irregular warfare campaign. But it demonstrated something strategically important -- disruption originating in the digital domain can quickly create physical, economic, political, and psychological effects. Now imagine the same disruption occurring not as an isolated criminal incident but simultaneously with attacks on communications, manipulated information, port delays, financial disruption, and an international military crisis. That is the scenario for which America needs to prepare. The essential question is therefore not whether individual agencies can successfully manage individual incidents, but it is whether leaders recognize when apparently unrelated events constitute a coordinated adversary campaign. Recognition should be the first test.

America's competitors do not need to invade the continental United States to create decisive effects inside it. They can combine cyber operations, covert influence, economic coercion, sabotage, espionage, criminal proxies, supply-chain disruption, information manipulation, and military pressure to exploit vulnerabilities across American society. The United States therefore needs a National Irregular Warfare Stress Test, a recurring whole-of-nation exercise designed to determine whether the country can continue governing, mobilizing military forces, sustaining critical services, communicating with its population, and supporting allies while subjected to a coordinated campaign of adversarial pressure. The objective should not be to demonstrate that America can stop every attack, but it should determine whether an adversary can prevent the United States from achieving its strategic objectives.

The Homeland Is Already Part of the Battlespace

For most of the post–Cold War era, the United States enjoyed an extraordinary strategic advantage; it could fight overseas while treating the homeland largely as a sanctuary. American forces deployed through functioning transportation systems, defense contractors produced equipment using reliable electricity and communications, civilian ports and rail networks supported military mobilization and global financial and supply networks continued functioning. American society experienced wars in Iraq and Afghanistan largely without sustained adversarial disruption inside the continental United States. However, a major-power conflict would look very different.

U.S. military power begins long before American forces reach a theater of operations. It begins in factories, data centers, commercial ports, rail networks, highways, energy grids, telecommunications systems, warehouses, financial institutions, civilian supply chains, and American communities and many of those systems are vulnerable. The threat posed by the People's Republic of China (PRC)–linked Volt Typhoon campaign offers perhaps the clearest warning. U.S. cybersecurity agencies concluded that PRC state-sponsored actors had gained persistent access to networks in the communications, energy, transportation, and water sectors.

More importantly, U.S. agencies assessed with high confidence that this activity was not simply conventional espionage. The actors were pre-positioning for potential disruption of operational technology during a future crisis or conflict. The strategic logic is straightforward. If Beijing ever confronted Washington over Taiwan or another major contingency, disrupting American infrastructure could complicate military mobilization and impose domestic costs without requiring China to defeat U.S. forces directly. Former FBI director Christopher Wray explicitly warned that Chinese hackers were positioning themselves inside American infrastructure so they could potentially cause real-world disruption during a future crisis.

However, the challenge extends beyond China. The US intelligence community's 2026 Annual Threat Assessment warns that China, Russia, Iran, North Korea, and nonstate ransomware groups continue seeking access to U.S. government, private-sector, and critical-infrastructure networks for intelligence collection, disruption options, or financial gain. The homeland can therefore no longer be understood simply as the rear area supporting military operations abroad. It is increasingly part of the theater.

Stress the National System

The proposed National Irregular Warfare Stress Test should deliberately attack the seams among six interconnected national systems: governance, national security, critical infrastructure, economic and industrial capacity, information and society, and alliances. The governance component should test whether federal, state, and local authorities can coordinate when attribution is uncertain, and authorities overlap. Suppose intelligence agencies conclude that a foreign power probably sponsored an infrastructure disruption, but law-enforcement agencies lack sufficient evidence for public attribution. Governors demand information, private infrastructure operators need technical indicators, congress requests briefings and social media fills the information vacuum. Who decides? Who communicates? Who has authority to act? And how quickly can classified intelligence become actionable information for organizations that actually operate the affected infrastructure?

The national security component should deliberately blur the categories the U.S. government normally uses to organize threats. Participants should confront activities that could plausibly constitute crime, espionage, sabotage, covert action, foreign influence, or preparation for military conflict. The ambiguity is essential because adversaries have incentives to remain inside precisely these gray areas.

Critical infrastructure should then be stressed as an interconnected system rather than as independent sectors. Power enables communications, communications enable finance, finance enables commerce, transportation enables military deployment, cloud infrastructure supports both government and industry, fuel systems underpin logistics, water and healthcare sustain communities, failures therefore cascade. The United States should measure whether critical national functions survive—not whether every facility remains operational.

The stress test should culminate in a military mobilization scenario. That is where irregular warfare against the homeland becomes directly relevant to conventional deterrence. A recent U.S. Army analysis concluded that American forces will almost certainly face a contested mobilization environment at U.S. seaports during future conflicts, citing adversary cyber capabilities, infrastructure vulnerabilities, and transportation constraints. The Department of War has likewise emphasized that success in contested logistics requires a resilient ecosystem connecting the military, allies, partners, and industry. A National Irregular Warfare Stress Test should put that ecosystem under pressure.

Imagine an Indo-Pacific crisis requiring substantial U.S. force deployment. The adversary does not try to sink transport ships in American ports. Instead, malware disrupts logistics software and manipulated data delay rail schedules and cargo movement. Fabricated safety warnings reach longshore workers, while cyber incidents interrupt defense suppliers and financial institutions. A critical foreign-made component suddenly becomes unavailable, and suspected sabotage at an energy facility creates uncertainty about attribution. At the same time, false reports claim that infrastructure attacks have killed civilians, that deployments have left parts of the homeland undefended, and that senior officials concealed the scale of the crisis. Military families receive targeted messages suggesting that deployed service members have been abandoned. No single action cripples the United States or necessarily constitutes an act of war. Together, however, they consume government attention, weaken public confidence, strain federal-state coordination, and slow deployment enough to affect operations thousands of miles away. The critical measure is straightforward: Can the United States still generate and project combat power while the homeland is actively contested? If American war plans assume that domestic infrastructure will function normally during mobilization, the stress test should attack that assumption relentlessly.

Infrastructure disruption represents only half the challenge. An adversary would simultaneously attempt to shape how Americans interpret events. The United States has already seen sophisticated foreign efforts intended to exploit domestic divisions. In 2024 the Department of Justice disrupted a Russian government–directed influence campaign that used fabricated websites, social media, paid advertisements, influencers, and AI-generated material to reach American and international audiences. U.S. intelligence officials similarly assessed during the 2024 election cycle that Russia sought to promote divisive narratives and covertly influence U.S. public opinion, while Russia, China, and Iran all viewed domestic political divisions as opportunities.

A national stress test should therefore challenge government communication as aggressively as it challenges infrastructure. Participants should confront fabricated documents, synthetic audio, manipulated video, contradictory unofficial reports, foreign information operations, genuine leaks mixed with false claims, and rapidly evolving public narratives. Success should not be measured by whether government messaging dominates the information environment. In a democracy, it should not. The test should instead measure whether authorities can provide rapid, factual, credible, and politically nonpartisan information while acknowledging uncertainty. The most dangerous information vulnerability may not be that Americans believe an adversary's false narrative. It may be that they stop believing anyone.

A national stress test that remains primarily a federal exercise would fail before it begins. Much of the infrastructure upon which national security depends lies outside direct federal control. CISA has long emphasized that significant portions of U.S. critical infrastructure are operated by private-sector companies and state or local governments, making resilience inherently a shared responsibility. Telecommunications companies, cloud providers, electric utilities, railroads, ports, trucking companies, financial institutions, healthcare systems, defense contractors, technology firms, and commercial suppliers therefore need meaningful roles. Governors and state National Guard organizations should participate, with the National Guard Bureau helping coordinate Guard involvement across jurisdictions. Major metropolitan governments should also participate. Universities, media organizations, and civil-society organizations should be represented where appropriate because societal resilience cannot be simulated exclusively inside government operations centers. This creates an uncomfortable reality for national security planners. American national power is distributed across society, while authority to coordinate that power remains fragmented. That is precisely what an adversary would exploit. And precisely what the stress test should expose.

Build the Crisis Slowly

Most exercises begin too dramatically. A National Irregular Warfare Stress Test should initially feel almost boring and unfold through a phased approach. During the first phase, the adversary should conduct cyber reconnaissance, espionage, covert influence, illicit financial activity, supply-chain manipulation, and information operations. Most events should appear insignificant individually, testing whether anyone recognizes the pattern. The second phase should introduce synchronized but still manageable disruptions: intermittent communications failures, port delays, cyber incidents affecting financial institutions, suspicious infrastructure failures, and coordinated false narratives. The question then becomes whether government shifts from incident response to campaign response. The third phase

should introduce the overseas military contingency. As the United States begins major mobilization, pressure against domestic systems intensifies. Transportation disruptions increase, defense-industrial suppliers experience problems, communications networks become unreliable, allied governments face coercion and manipulated information targets military personnel and families. The final phase should test endurance and adaptation over an extended period. The adversary should change tactics, pause selected attacks, exploit workarounds adopted by U.S. organizations, and shift pressure toward newly exposed dependencies. Participants should rotate leaders, operate with degraded staffing and incomplete information, ration scarce resources, restore essential services in priority order, and revise authorities and coordination mechanisms as circumstances change. The exercise should test whether lessons move quickly across agencies, states, military commands, private firms, and allies—and whether successful adaptations endure after the immediate crisis. The final question is perhaps the most important of all: Can American institutions learn and adapt faster than the adversary?

Institutionalize the Test

One exercise will not solve the problem. The United States should establish a three-tier testing system. First, an annual senior-level tabletop exercise should force cabinet officials, combatant commanders, governors, intelligence leaders, regulators, and private-sector executives to confront questions of authority, attribution, escalation, and strategic response. Second, a periodic national functional exercise should connect federal agencies, states, critical infrastructure operators, military commands, and selected allies in a distributed scenario. Third—and most important—the United States should conduct a periodic national resilience campaign lasting several weeks or months. Organizations would receive irregular warfare injects while continuing normal operations. This would better approximate the reality of strategic competition.

Adversaries do not normally provide convenient exercise start times. They probe continuously, observe responses, change tactics, and return through another vulnerability.

The United States should practice doing the same thing defensively. An independent red team should drive the process. Its mission should not simply be to "play China" or "play Russia." It should be instructed to produce strategically significant effects against the United States without triggering an obvious conventional military response. That single instruction would force the red team toward the seams that matter most: jurisdictional confusion, private-sector dependencies, political hesitation, infrastructure chokepoints, alliance divisions, and gaps between peace and war.

The results should feed a recurring national resilience assessment. Critical functions could be evaluated against five stages: anticipate, absorb, adapt, recover, and transform. The first asks whether the threat can be detected before major disruption occurs. The second asks whether the function can continue operating when attacked. The third assesses whether institutions can modify their behavior as the threat evolves. The fourth measures restoration. The fifth asks whether lessons from the crisis produce structural improvements that make the next attack less effective. These measures would transform resilience from a broad aspiration into something policymakers can repeatedly test. Failures identified during one stress test would become requirements for the next. Progress—or the absence of progress—would become visible.

Conclusion

A National Irregular Warfare Stress Test would expose vulnerabilities. That is not an argument against conducting it. It is the reason to conduct it. The United States stress-tests financial institutions because policymakers understand that a bank can appear healthy under normal conditions while hidden dependencies become catastrophic during simultaneous shocks. National security now requires similar thinking.

The United States possesses extraordinary military, technological, economic, and societal resources. But possessing resources is not the same as being able to coordinate them under sustained pressure. A future adversary will search for the seams between federal and state governments, military and civilian infrastructure, public and private responsibility, domestic and foreign security, and ultimately peace and war. Americans should find those seams first. The ultimate measure of the National Irregular Warfare Stress Test should therefore not be the number of attacks stopped, networks protected, or facilities left functioning. After months of coordinated adversarial pressure, policymakers should have to answer one question -- does the United States still possess the freedom of action required to pursue its national objectives? If the answer is uncertain, America has identified a vulnerability. Better to discover it during a stress test than during a war.