G1VE TECHNOLOGIES

The 72-Hour War Starts Before the First Shot

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Aug 12, 2026

Original source

https://www.linkedin.com/pulse/72-hour-war-starts-before-first-shot-w-b--4kuve/

How the Cybersecurity and Infrastructure Security Agency , The U.S. Coast Guard , and Mission Assurance Leaders Are Reframing Critical Infrastructure as a Battlespace

I. The Homeland Is No Longer Rear Area.

For too long, too many leaders treated critical infrastructure security as a compliance issue, a regulatory issue, or a technical issue. It is now plainly a national defense issue. Cybersecurity and Infrastructure Security Agency 's 2026 posture makes that impossible to ignore.

Its CI Fortify initiative explicitly tells critical infrastructure owners and operators to plan for a conflict scenario in which telecommunications, internet, vendors, service providers, and upstream dependencies may become unreliable — and to assume that threat actors may already have some access to operational technology networks.

That is not ordinary cyber hygiene language. That is mission assurance language. That is battlespace language.

II. The Infrastructure Fight Starts Before Open Conflict.

One of the most important truths in the geopolitical environment is that pre-conflict shaping does not begin at the front. It begins in the seams:

- Ports,
- Pipes,
- Water systems,
- Logistics networks,
- Industrial control systems,
- Data links,
- Suppliers, and
- Public trust.

Cybersecurity and Infrastructure Security Agency has said for years that U.S. officials assess China has been infiltrating non-military critical infrastructure to enable sabotage during a major conflict, especially one involving Taiwan.

CI Fortify is essentially an acknowledgment that continuity planning can no longer rest on the assumption that civilian infrastructure will remain untouched while military operations unfold elsewhere. The homeland sustainment layer is now part of the operational equation.

III. AI Has Changed The Speed Of The Threat.

If this were only about conventional cyber risk, it would already be serious. But AI has changed the pace of the fight. Nextgov/FCW 's July reporting found that AI is now being used in some form across every stage of cyberattack operations. Cybersecurity and Infrastructure Security Agency's updated vulnerability-remediation directive reflects that reality directly, saying the move responds to a threat landscape in which AI software services can help adversaries find and exploit flaws.

The new directive establishes patch timelines ranging from three days for the highest-risk vulnerabilities to 60 days for lower-priority items, and Cybersecurity and Infrastructure Security Agency said an analysis at one major civilian agency found only about 1% of vulnerability instances fell into the three-day category while more than 60% could be deferred until scheduled system upgrades.

That is an important nuance: The answer is not "panic patching" everything. The answer is consequence-based prioritization at combat tempo.

IV. The 72-Hour Clock Is Strategic, Not Administrative.

The coming CIRCIA final rule matters because it forces a cultural transition from voluntary disclosure toward mandatory incident reporting. Cybersecurity and Infrastructure Security Agency expects the rule in September, and the law requires critical infrastructure entities to report substantial incidents within 72 hours and ransomware payments within 24 hours.

That timeline is not just a compliance burden. It is a strategic discipline. In a live crisis, the quality of national response depends heavily on how fast the government understands attack patterns, sector interdependencies, and adversary behavior.

Delayed reporting does not merely harm the victim organization. It degrades shared situational awareness across the homeland-defense architecture.

V. Port Security Is Now A Front-Line Problem.

The U.S. Coast Guard 's July notice looking for tested and fielded solutions to defeat unmanned underwater vehicles should wake up anyone still imagining maritime infrastructure security as a niche issue. The service said malicious actors can use UUVs for intelligence gathering, surveillance, smuggling, sabotage of critical infrastructure, and even kinetic strikes.

More importantly, the U.S. Coast Guard made clear that detection alone is not enough; it is specifically seeking defeat and mitigation capabilities that can scale across ports, waterways, and coastal security operations.

That is a major signal. It means the maritime edge of critical infrastructure protection is evolving from passive monitoring toward active counter-threat capability.

VI. Mission Assurance Now Requires Thinking Like A Joint Operator.

Here is the mistake many civilian organizations still make:

- They separate cyber continuity, physical security, vendor resilience, and crisis operations into different committees.

The threat does not respect that org chart. A real readiness posture now demands an integrated view aligned with mission assurance and sustainment logic:

1. If the telecommunications path fails, what is the operational workaround?
2. If OT has already been touched, what can be isolated fast enough to preserve essential service? If maritime access is degraded, what supply nodes become critical?
3. If the reporting clock begins at 02:00 on a weekend, who owns the decision authority to classify the event, notify federal counterparts, and activate recovery playbooks?

That is why JP 3.0 and JP 4.0 thinking matters here more than many civilian executives realize. Operations and logistics are inseparable under pressure. Critical infrastructure resilience is now a practical sustainment problem as much as a security problem.

VII. What Leaders Should Do Next

The leaders who will get this right are the ones who stop using the word "resilience" as branding and start translating it into operator-grade questions:

1. Which systems are truly mission essential?
2. Which upstream dependencies would break us fastest?
3. Which functions must be manually executable if digital trust collapses?
4. Which incidents would force immediate cross-sector reporting?
5. Which facilities require physical, cyber, and maritime coordination as a single defensive problem set?

That is the posture shift underway now across Cybersecurity and Infrastructure Security Agency, the U.S. Coast Guard, and the broader national security community. The 72-hour war starts before the first shot because the shaping activity happens before the headlines. By the time the public sees the conflict, the infrastructure fight may already be well underway.

VIII. Thought-Provoking Close: The Final Assessment

Critical infrastructure is not adjacent to national security. It is national security.

And the organizations that thrive in this environment will be the ones that learn to think less like compliance shops and more like mission assurance commands:

- Consequence-driven,
- Time-disciplined,
- Cross-domain, and,
- Built for degraded conditions.

...That is what this moment requires.

✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Future to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.

This is built for professionals responsible for decisions that carry consequence—not commentary.

📅 Ready to operationalize these insights and move beyond theory?

☞ https://calendly.com/g1ve-technologies
Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.

As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.

His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.

📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance