G1VE TECHNOLOGIES

The Cyber Aftershock: Operation Epic Fury's Second Front Is Coming Home

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

Mar 16, 2026

Original source

https://www.linkedin.com/pulse/cyber-aftershock-operation-epic-furys-second-front-w-b--tstue/

How Iran's Asymmetric Response to American Airstrikes Is About to Hit Your Hospital, Your Power Grid, and Your Bank — And What the Next 30-60 Days Will Look Like

THE WAR THAT DOESN'T NEED MISSILES

On February 28, 2026, at the opening hours of Operation Epic Fury, the United States and Israel launched coordinated kinetic strikes against Iran — B-2 bombers, Tomahawk missiles, suicide drones, and a cyber-space integration package that the Chairman of the Joint Chiefs publicly confirmed "effectively disrupted Iranian communications and sensor networks."

Iran's conventional military response capability was being systematically dismantled in real time. Its navy was being "annihilated," in the words of Secretary of Defense Hegseth. Its missile production facilities were being "razed to the ground," per President Trump. Iran's ballistic missile launchers, its nuclear pathways, its proxy support infrastructure — all primary targets.

But here is what 46 years of studying Iranian strategic behavior tells us: Iran does not fight the war it cannot win. It fights the war its adversary has not prepared for.

Iran cannot match the United States in kinetic power. It cannot trade sortie-for-sortie with American airpower. It cannot absorb the precision firepower that has been raining down since February 28th.

What Iran can do — and what Iran has been building the capability to do for two decades — is reach through cyberspace and hit America where the kinetic military cannot protect it: the electric grid, the water systems, the financial networks, the hospital infrastructure, the transportation backbone that holds modern civilization together.

The cyber aftershock of Operation Epic Fury is not a hypothetical. It is an operational assessment. And the window of maximum risk is right now: the next 30-60 days.

WHAT IRAN ALREADY DID IN THE FIRST WEEK

Before we look at what is coming, let us be clear-eyed about what has already happened. The opening phase of Operation Epic Fury was not purely kinetic. Cyber operations were woven into the fabric of the campaign from the first hour.

On the opening night, a widely-used Iranian religious calendar application — BadeSaba, with over 5 million downloads — was compromised. Iranian users who opened the app to check prayer times instead received targeted messages: "The Iranian regime will pay for their cruel and merciless actions against the innocent people of Iran." The breach was timed to coincide precisely with the first waves of airstrikes, sowing confusion, disabling regime communications, and amplifying the psychological impact of the kinetic campaign. Attribution has not been formally confirmed, but the operational signature points to Israel, which has integrated cyber and influence operations more deeply than almost any other military in the world.

Iranian state news agency IRNA was compromised simultaneously, with anti-regime messages plastered across its front page. Multiple government services and military target networks were disrupted to prevent a coordinated Iranian response.

Iran's own counter-measure was both brutal and revealing: it imposed a near-total internet blackout, with nationwide connectivity falling to 4% of normal levels. Part of this was deliberate — the regime suppressing information flow the way it has during every domestic crisis since 2019. But part of it was a defensive cyber measure, limiting the attack surface available to external intrusions by simply cutting the country off from the global internet.

Meanwhile, GPS and Automatic Identification System (AIS) signals were disrupted for more than 1,100 ships across Iranian, UAE, Qatari, and Omani waters — creating chaos in commercial maritime navigation across one of the world's most critical oil transit chokepoints. Attribution remains contested. Intent is not.

THE RETALIATION CALCULUS

Iran cannot win a kinetic fight with the United States. This is not analysis — it is arithmetic. But Iran's strategic doctrine has always been built around a different kind of arithmetic: asymmetric cost imposition. Make the price of confrontation high enough, through proxy attacks, terrorism, economic disruption, and now cyber operations, that the adversary decides the objective was not worth the price.

That doctrine is now being applied in cyberspace with a sophistication and scale that should alarm every senior leader responsible for critical infrastructure in the United States.

The historical data is clear: following major Israeli and U.S. military strikes on Iranian-linked targets in 2025, Iran's affiliated cyber actors generated a 700% increase in cyberattacks against Israel in the weeks that followed. That surge represents the known, attributed activity. The unattributed activity is believed to be significantly larger.

Iran's offensive cyber capability is not a blunt instrument. It is a maturing, sophisticated program that includes:

- Wiper attacks — destructive malware designed to render systems unrecoverable, not merely compromised
- DDoS attacks against major U.S. financial institutions (first used by Iran in 2012-2013 in Operation Ababil, and repeatedly since)
- Industrial Control System (ICS) exploitation — Iran has demonstrated the ability to target SCADA systems and operational technology networks that control physical infrastructure
- Election interference operations — documented in 2020 and 2024
- Fuel distribution system disruption — attributed Iranian-backed actors disrupted Jordan's fuel distribution network in a demonstration strike earlier this year

Perhaps most alarming: Iranian Revolutionary Guard Corps officials were previously sanctioned for directing cyber operations against vulnerable water systems across the United States. These are not theoretical vulnerabilities. Iranian cyber actors have already been inside American water utility networks.

THE SECTORS IN THE CROSSHAIRS

Intelligence assessments, CISA advisories, and independent threat research published since the February 28 strikes have converged on the same list of primary targets for Iranian cyber

retaliation. If you lead an organization in any of these sectors, this section is written directly for you.

Energy Infrastructure. The electric grid remains the crown jewel target of Iranian cyber planning. Disruption of power to a major metropolitan area creates cascading failures across every other critical sector — hospitals lose backup power, water treatment plants fail, financial systems go dark, transportation infrastructure stops. Iran has studied this cascading logic for years. The Volt Typhoon "pre-positioning" campaign — which, notably, is a Chinese operation, though Iranian actors are believed to have received tradecraft transfer — demonstrated that adversary cyber operators have been embedding themselves in U.S. grid infrastructure waiting for a strategic trigger to act.

Water and Wastewater Systems. These systems are chronically under-resourced for cybersecurity, often running decade-old SCADA technology with remote access connections that were never designed for the threat environment they now face. Iran has targeted this sector before. The next wave will be more aggressive. CISA's published "high priority" guidance issued since February 28 specifically calls out water utilities as requiring immediate defensive action.

Financial Services. Iranian cyber actors launched the 2012-2013 "Ababil" campaign against JPMorgan Chase, Bank of America, Wells Fargo, and other major U.S. financial institutions, causing significant disruption to online banking services. That capability has not atrophied. It has been significantly enhanced.

Healthcare. U.S. hospitals are already preparing for Iranian-sponsored DDoS attacks. A coordinated campaign against hospital networks — overwhelming emergency care systems during a period of heightened national anxiety — would impose both practical and psychological costs simultaneously.

Transportation and Logistics. The GPS disruption to 1,100+ ships is a preview. Iranian-affiliated actors have targeted port systems, rail networks, and aviation support infrastructure in previous operations. The disruption of commercial shipping through the Persian Gulf has already caused insurance markets to spike.

Communications Infrastructure. This is where Salt Typhoon and the Iranian response vectors converge. Salt Typhoon — a Chinese cyber campaign — has already compromised more than 200 major telecom companies across 30+ nations, including AT&T, Verizon, Charter, and Windstream, plus the call records of senior U.S. government officials. Iranian cyber actors operating in an environment of pre-positioned Chinese access represent a layered threat that traditional perimeter security cannot address.

THE PROXY PROBLEM: ATTRIBUTION AND ESCALATION

One of the most dangerous features of Iran's cyber campaign is its deliberate use of proxy hacktivists who provide the regime with plausible deniability while extending its operational reach globally.

Groups operating under ideological frameworks like the "Great Epic" cyber campaign and the "Cyber Islamic Resistance" umbrella can be activated, directed, or merely encouraged by Iranian state actors — creating a wave of attacks that proliferates beyond direct state control once set in motion.

This creates a specific escalation risk: when Iranian internet connectivity is at 4% (as it is now), the state-directed operations from inside Iran are suppressed. But the geographically dispersed proxies — operating from Lebanon, Iraq, Yemen, Syria, Venezuela, and cells embedded in Western nations — are not constrained by that blackout. They operate autonomously, which means that coordinated Iranian government decisions about cyber escalation may be overtaken by proxy activity that is harder to deter, harder to attribute, and harder to stop.

The Canadian Centre for Cyber Security published a Cyber Threat Bulletin in February 2026, before the major strikes, warning of exactly this dynamic: Iranian cyber actors operating as part of a coordinated response to U.S.-Israeli strikes. That bulletin has aged like a prophecy.

U.S. Cyber Command is conducting offensive operations in support of the kinetic campaign — the Chairman of the Joint Chiefs publicly confirmed as much. But offensive operations in cyberspace, even successful ones, do not eliminate the distributed proxy threat. Russia may also be extending asymmetric support to Iranian cyber operations, as Russian-aligned threat actors have been documented providing proxy services for Iranian campaigns in the past.

THE 30-60 DAY WINDOW: WHAT LEADERS MUST DO NOW

Federal News Network and multiple cyber intelligence firms are converging on the same assessment: the next 30-60 days represent the period of maximum Iranian cyber threat against U.S. critical infrastructure.

This is the window when the regime's motivation is highest, its proxies are most activated, and its tactical objectives are most clearly defined: impose costs on America sufficient to complicate domestic political support for the continuation of Operation Epic Fury.

For critical infrastructure operators and organizational risk leaders, this is not the moment for horizon-scanning. It is the moment for sprint-mode execution.

Immediate priorities:

1. Activate your incident response retainer. If you do not have an active relationship with a cyber incident response firm, you needed it yesterday. Establish it today.

2. Implement CISA's Emergency Directives. CISA has issued specific advisories covering the most common Iranian attack vectors — Cisco router exploitation, FortiGate device compromise, remote access vulnerabilities in OT environments. These are not aspirational guidance documents. They are prescriptions for surviving the next 60 days.

3. Enforce Multi-Factor Authentication everywhere. Particularly for remote access, VPN connections, and administrative accounts. This single control eliminates the most common initial access vector used by Iranian-affiliated actors.

4. Review your third-party access points. The FortiGate compromise that allowed Salt Typhoon/ Volt Typhoon to pre-position across hundreds of organizations exploited vendor and contractor remote access. Your security perimeter is only as strong as the weakest vendor who has keys to your network.

5. Run a tabletop exercise this week. Not next quarter. This week. Specifically for a DDoS + wiper malware combined attack scenario. Your team needs to know exactly who calls whom and in what sequence when the alarm sounds.

6. Protect your OT/SCADA environments. Segment them. Air-gap where possible. Verify that remote access connections meet 2026 security standards, not the standards they were configured to when installed in 2011.
7. Brief your board. This is not a technical update. This is a strategic risk briefing. The Iranian cyber threat is a material risk to operations, and your board has a governance obligation to understand it.

THE STRATEGIC PICTURE: WHAT COMES AFTER

Operation Epic Fury will not last forever. The Iran conflict will reach some kind of resolution — whether a decisive American victory, a negotiated halt, a messy stalemate, or something in between. When the kinetic phase ends, Iranian cyber capabilities will not be demobilized. They will be redirected.

The historical pattern is consistent: Iran uses periods of heightened kinetic tension to test, probe, and pre-position cyber capabilities, then deploys those capabilities as leverage in the subsequent political and economic phase of the conflict. The hacked data, the pre-positioned access, the documented vulnerabilities — these become tools of coercion in the negotiating environment that follows a shooting war.

This means the 30-60 day acute phase is only the first chapter of the cyber risk story that Operation Epic Fury has opened. Organizations that assume the threat recedes when the shooting stops are making a strategic error that their successors will regret.

The intersection of Iranian cyber retaliation, the ongoing Salt Typhoon telecom compromise, the Volt Typhoon pre-positioning in U.S. grid infrastructure, and the broader adversarial cyber environment created by the simultaneous China-Taiwan tension creates a threat landscape of compounding complexity that demands compounding vigilance.

THE BOTTOM LINE

The second front of Operation Epic Fury is not being fought over Iranian airspace. It is being fought in server rooms in Houston and Atlanta and Chicago and New York. It is being waged against the SCADA systems in your water treatment plant and the electronic health records in your regional hospital and the routing tables in your financial clearinghouse.

Iran cannot match American kinetic power. But it does not need to. It needs only to impose sufficient pain, through sufficient disruption of civilian life, to change the political calculus of the American public about whether Operation Epic Fury was worth the cost.

Your infrastructure is the battlefield. Your security posture is the weapon. And the clock is already running.

✨Call to Action✨:

Subscribe to my LinkedIn Newsletter, "Securing Our Future" for more information, research, case-studies, and literature around how National Defense Strategy, National Security, National Policy, Regulatory Compliance, A.I. (Artificial Intelligence) Governance/Ethics, Internal/External Audit, TPRM (Third-Party Risk Management), Fintech Innovations, and "all things GRC"

(Governance, Risk Management, and Compliance) are continuously/dynamically re-shaping and Securing Our Future.
Let's navigate the future together.

🔍 About the Author:

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP, is a seasoned Artificial Intelligence (A.I.), National Defense and National Security Strategist and Subject Matter Expert (SME) in Governance, Risk, and Compliance (GRC), A.I. Governance/Ethics, Regulatory Compliance, Data Governance, Comprehensive/Integrated Risk Management, and Project/Program Management.

As the Managing Partner at G1VE | Technologies and the Strategic Board Advisor to many multi-domain, cross-industry organizations across both the Public Sector (I.e., Fortune 500 and Fortune 1000 companies) and Private Sector entities, W.B. leverages his extensive experience and deep subject matter expertise to drive innovative solutions that enhance organizational resilience and operational integrity. Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP, on LinkedIn to stay updated on the latest insights and trends in these critical areas.