G1VE TECHNOLOGIES

They Are Already Inside: Sanctions, Seizures, And The Pre-Positioned Adversary In American Infrastructure

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

Aug 30, 2026

Original source

https://www.linkedin.com/pulse/already-inside-sanctions-seizures-pre-positioned-w-b--fvnpe/

I. The Pivot: Last Week Was About Keeping The Harbor Open. This Week Is About Who Is Already Inside The Gates.

The previous articles in this series built a posture:

1. Assume intrusion,
2. Reduce harm,
3. Preserve continuity,
4. Keep the mission moving.

That posture just received its most vivid validation of the year. In a single week — August 24 through 27, 2026 — the federal government sanctioned five Iranian hackers for breaching American energy companies, defense contractors, and government offices, and the Federal Bureau of Investigation (FBI) seized the infrastructure of a Chinese state-sponsored hacking operation that had scanned or exploited more than 2 million targets in a single day.

This is no longer about preparing for the adversary's arrival. The adversary arrived years ago, mapped the terrain, and in some cases is still sitting inside. The leadership question for critical infrastructure has therefore shifted one more level: not "how do we keep them out," and not even "how do we operate through compromise," but how do we find, expose, and evict adversaries who pre-positioned for a conflict that has not started yet — while the ones already here get counted, named, and squeezed.

II. Case Study One: The Iranian Network That Treated American Infrastructure Like An ATM

The U.S. Department of the Treasury 's August 24 action — part of what Secretary Scott Bessent billed as an "economic D-Day" against Iran — named five Iranian nationals tied to a hacking operation directed by Iran's Ministry of Intelligence and Security. The details matter. Since late 2023, three of them allegedly breached and stole data from U.S. energy companies, defense contractors, health care institutions, technology firms, and financial institutions — and compromised several local, state, and federal government offices during the summer of 2024.

Four of the five were also charged days earlier in the U.S. Department of Justice 's expanded case against 17 Iranian cyber actors affiliated with the Mabna Institute, a Tehran-based hacking-for-hire operation accused of stealing more than 31 terabytes of academic research and intellectual property on behalf of the Islamic Revolutionary Guard Corps.

Two details elevate this from a sanctions story to a strategic warning:

1. The Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation (FBI) have recently been helping water utilities across at least 12 states recover from cyberattacks — intrusions some officials suspect are Iran-linked, though Cybersecurity and Infrastructure Security Agency has not publicly attributed them.
2. The U.S. Department of the Treasury 's own filing noted the hackers sometimes stole from Iranian targets too, prioritizing personal profit over Tehran's interests.

...That is the profile that should keep infrastructure operators up at night:

- State-directed capability fused with criminal opportunism, executing against sectors where the attack surface is wide and the security investment is thin.
- Water, energy, health care, local government — this is not target selection by chance. It is target selection by vulnerability.

III. Case Study Two: The Chinese "Infrastructure Quartermaster" Running Industrial Scale Reconnaissance

If the Iranian case shows opportunistic intrusion, the Chinese case shows industrialized pre-positioning. On August 26, the Federal Bureau of Investigation (FBI) seized three domains powering tools called QScan and QTRouter, attributed to a hacking group operating through Nanjing Xinjiuwei Network Technology Company — a private Chinese firm that sold hacking services to Beijing's main civilian intelligence agency and its military.

The target list reads like a tour of the American command structure:

1. NASA - National Aeronautics and Space Administration ,
2. The Federal Reserve Board ,
3. The The National Institutes of Health ,
4. The United States Senate ,
5. The U.S. Department of Energy (DOE) ,
6. The U.S. Department of Justice , and,
7. The U.S. Department of Health and Human Services (HHS) —
8. Plus hospitals, telecommunications providers, power companies, banks, and defense contractors.

The scale is what separates this from ordinary espionage. QScan carried code for more than 200 different exploits and, on one day in 2024, processed more than 2 million scanning or exploitation tasks. Lumen Technologies , which tracked the infrastructure for roughly a year, called the operator an "infrastructure quartermaster" — a service provider equipping other China-linked hacking teams with ready-made target discovery and concealment.

In May 2024, the group exploited a newly public Check Point Software flaw within days, stealing server settings and account data from more than 300 U.S. organizations. Months later, it used a previously unknown Ivanti flaw to access three national laboratories, The National Institutes of Health , another HHS agency, and a U.S. security device manufacturer.

IV. The Pattern: Pre-Positioning Is The Strategy, Not The Prelude

Step back and the week's two cases form one picture. China builds quartermaster infrastructure — scanning at industrial scale, hiding behind hijacked routers, sharing reconnaissance across multiple state hacking teams — so that when a crisis comes, the access already exists. Iran runs ministry directed intrusions fused with criminal freelancing, hitting water systems, energy firms, and government offices, probing for the seams.

These are different models aimed at the same objective:

- Optionality inside American critical infrastructure ahead of conflict.

This is precisely what the Cybersecurity and Infrastructure Security Agency 's CI Fortify guidance has been warning about — the standing assessment that China is burrowing into non-military infrastructure to enable sabotage during a Taiwan scenario, and that operators should assume third-party connections become unreliable and threat actors hold some operational technology access during conflict.
U.S. Cyber Command 's hunt forward doctrine exists for the same reason:

- You do not wait for the adversary to act inside your networks; you go find them.

This week's sanctions and seizures are what that doctrine looks like executed at national scale — naming individuals, indicting networks, seizing infrastructure, and publishing the receipts.

V. What Actually Works: Attribution, Disruption, And The Power Of Receipts

Critics dismiss sanctions as symbolic. The operational record says otherwise — when sanctions are stacked with indictments, seizures, and technical takedowns. The Federal Bureau of Investigation (FBI) has now removed plugX malware from more than 4,200 U.S. computers, dismantled router networks tied to Flax Typhoon, disrupted Volt Typhoon's concealment infrastructure, and this week seized the QTFY toolset outright.
Each action degrades adversary capability, forces rebuilds, burns operational security, and — critically — publishes forensic detail that lets every other defender hunt for the same signatures. For critical infrastructure operators, the lesson is that defense is now a team sport with referees who publish.
When the Federal Bureau of Investigation (FBI) seizes a domain, the affidavit becomes a free threat intelligence package. When the U.S. Department of the Treasury names five hackers, the filing maps their tactics and target sectors. The operators gaining the most from this cycle are the ones treating federal disclosures as operational inputs — scanning their own environments against published indicators within days, not quarters — rather than as news to acknowledge in the next board deck.

VI. The Operator's Checklist For A Pre-Positioned Adversary Era

1. Hunt, do not just monitor: If a state sponsored quartermaster ran 2 million exploitation tasks in a day, assume your sector was scanned and look for the quiet persistence — unusual router behavior, living off the land techniques, dormant accounts — rather than waiting for alerts designed to catch noisy attacks.

2. Treat water, health care, local government, and smaller energy providers as the soft front line: The Iranian case proves adversaries deliberately select thinly defended sectors; if you operate in one, your threat model is now a state actor, full stop.
3. Ingest government disclosures as operational intelligence with a service level agreement: The Check Point Software exploitation wave hit 300 organizations days after a flaw became public. Your patch and exposure management cycle must now be measured in the same unit of time the adversary uses: days.
4. Rehearse the scenario where you discover pre-positioned access during a geopolitical crisis — when evicting the adversary and keeping operations running must happen simultaneously, under public and regulatory scrutiny. That tabletop exercise is no longer exotic. It is the base case.

VII. Thought-Provoking Close: The Bottom Line

Assume breach was last year's lesson. This week's is harsher:

- They are already inside,
- They have been there for years, and,
- The federal government is now naming them, indicting them, and seizing their infrastructure in public.

For critical infrastructure leaders, the mission has evolved from building walls to hunting tenants — finding the pre-positioned adversary before the geopolitical moment arrives when they flip from watching to acting. The harbor stays open only if someone is actively clearing what is underneath it.

✨ 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