HORIZON3

Building Capacity and Resilience for U.S. Partners: The Art of Cyber Diplomacy

Nation-state actors and cybercriminals are no longer probing the edges of our networks, they're operating inside them, increasingly supercharged by AI. For the U.S. and its allies, that reality creates a simple mandate: we can't just harden our own perimeters; we have to help our partners do the same.

That's the essence of modern cyber diplomacy: using policy, partnerships, and platforms to raise cyber IQ, close misconfigurations, and reduce exploitable attack paths across an entire ecosystem, not just a single network.

WHITEPAPER

From Point Solutions to Programmatic Capacity Building

Over the last few years, we've seen a quiet shift from one-off offers of "help" to structured, repeatable capacity-building programs that combine:

- **Trusted coalitions and mechanisms** with the Department of War (DoW) for the Defence Industrial Base (DIB) efforts, Federal Bureau of Investigation (FBI) campaigns, and internationally recognized coalitions like NATO's CCDCOE.
- **Computer Emergency Response Teams (CERTs)** working across national boundaries.
- **Expanded shared tradecraft** providing common cyber hygiene baselines, incident playbooks, and threat-actor TTPs.Which remediation activities were completed?
- **Advancement in scalable platforms** such as AI-native offensive security platforms like NodeZero® that partners can self-serve.

CERTs play a particularly important role in this model. Because each country's CERT sits close to the realities of its own threat environment, infrastructure, and response mechanisms, they create a practical bridge between local cyber defense needs and broader international coordination. When those CERTs collaborate across borders—sharing advisories, lessons learned, incident response practices, and threat intelligence—they help turn isolated national efforts into a stronger collective defense posture. That kind of coordination helps move capacity building beyond information sharing alone and toward a more operational model of collective defense.

In the era of AI vs. AI, these well-intended programs must become more dynamic, proactive, and operational. It is no longer enough to build awareness, share Cyber Threat Intelligence (CTI), and improve incident response after the fact. To keep pace with adversaries moving at machine speed, governments and their partners must move further up the attack chain—"left of boom" and "left of theft"—by continuously identifying and reducing exploitable attack paths before they can be weaponized. That is the new call to action: Hack, Fix, Verify, and Repeat at scale.

DoW & the DIB: Cybersecurity as a Service (CSaaS)

One of the most successful examples is the NSA Cybersecurity Collaboration Center's Cybersecurity as a Service (CSaaS) model for the DIB.

Through this program, over 700 at-risk DIB companies receive:

- Protective DNS (PDNS) to block known bad destinations
- Attack Surface Management (ASM) to understand what's exposed
- Continuous autonomous penetration testing (CAPT) with Horizon3.ai's NodeZero to prove what's actually exploitable

By turning continuous offensive testing into a shared service, cyber leaders across DoW and critical infrastructure can help under-resourced suppliers:

- Improve their cyber IQ
- Identify and prioritize real attack paths (not just long lists of CVEs)
- Run remediation and 1-click verify campaigns that show measurable risk reduction

This is cyber diplomacy applied to supply chains: strengthening the companies that keep missions moving.

Another successful example is how the NCSC in the UK has rolled out their Cyber Toolkit designed to help small businesses identify and quickly remediate typical attack paths including securing business email systems to thwart phishing campaigns.

Department of State (DOS) & FBI: Outreach as Operational Defense

U.S. capacity building doesn't stop at the DIB. DOS and FBI have embraced the idea that cyber outreach is an operational necessity, not a side project.

On the diplomatic side, State's cyber and digital policy efforts focus on:

- → Helping partners harden civilian and critical infrastructure networks
- → Coordinating civilian cyber assistance among allies and the private sector
- → Building long-term resilience and trust with nations facing persistent cyber pressure

On the law-enforcement side, the FBI is turning lessons from major investigations into practical roadmaps that any organization can act on.

Operation Winter SHIELD

One of the most successful programs has been Operation Winter SHIELD (Securing Homeland Infrastructure by Enhancing Layered Defense.) It distills the FBI's 10 most impactful actions organizations can take to improve cyber resilience from phish-resistant authentication and risk-based vulnerability management to third-party risk and logging hygiene.

Winter SHIELD: https://www.fbi.gov/investigate/cyber/wintershield

- → Aligns with the National Cyber Strategy
- → Positions companies as co-defenders alongside the FBI and partners
- → Provides a practical roadmap for both IT and OT environments

It's not "call us after the breach." It's "here's how we shrink your attack surface now."

“Ahead of the Threat” – Boards, AI, and Resilience

The FBI’s Ahead of the Threat Podcast extends that outreach, tackling questions such as:

- How will emerging technology, including AI, impact corporate America?
- How can corporate boards be structured for cyber resilience?
- What does the FBI think about generative AI in cyber operations?

Guests from big tech, incident-response firms, and insurance firms all echo the same theme: resilience beats perfection. Breaches will happen; the differentiator is how quickly you detect, contain, and recover.

For partners with limited resources, this “resilience-first” mindset, backed by concrete best practices, is far more actionable than abstract standards.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) also represents an important model for how allied cyber organizations can help raise the baseline across a region. Beyond convening experts, the body plays a practical role in helping participants upskill, exchange tradecraft, and stay better aligned on adversary behavior, especially as APT activity continues to evolve across their area of responsibility. That kind of structure matters because it helps turn isolated expertise into shared capability.

Where there is a critical mass of interest, trusted relationships, and sustained support, that model should be replicated elsewhere. The value is not just in sharing information once, but in creating a durable mechanism for collective learning, operational alignment, and more effective regional cyber resilience over time.

Why Offense-Informed Defense Matters

Capacity building isn't just about policies and podcasts. It's about teaching partners to think like an attacker.

Take the well-known Target breach: attackers pivoted through an HVAC supplier, proving that adversaries don't care about accreditation boundaries or theoretical trust zones. If there's a weak point in the extended enterprise, they'll find it.

In a zero trust world, the only way to stay honest about your actual exposure is continuous offensive testing:

- → Map real-world attack paths across internal, external, cloud, and supply-chain assets
- → Show Path → Proof → Impact, not just exposure
- → Re-test after remediation to prove the path is closed

That's where AI-assisted platforms like NodeZero change the game.

Fighting AI with AI: NodeZero™ with Rapid Response

Adversaries are already leveraging AI to:

- → Discover and weaponize new vulnerabilities faster
- → Automate reconnaissance and password spraying
- → Chain misconfigurations, weak identities, and exposed services into full attack paths

Defenders need to respond in kind, AI vs. AI with humans in the loop by exception.

NodeZero does this by:

- Autonomously emulating attackers with production-safe pentests, chaining CVEs, misconfigurations, defaults, and weak creds into end-to-end attacksAutomate reconnaissance and password spraying
- Prioritizing what is provably exploitable, not every theoretical vulnerability
- Enabling a repeatable hack–fix–verify–repeate loop so partners can measure and prove risk reduction over time

With Horizon3.ai Rapid Response, organizations can:

- Rapidly answer, “are we exposed to this new N-day or the celebrity CISA KEV?”
- Identify impacted assets and attack paths based on previously observed environments
- Launch targeted remediation and then **1-click verify** that the exposure is gone

That’s cyber diplomacy, operationalized: US and Allies sponsor the program; partners run the platform; everyone gets safer.

Learn more about Rapid Response.

IN THE DIB CSAAS PROGRAM, THIS MODEL IS ALREADY PROTECTING:

700+
DIB companies

2.9M+
endpoints

700k+
weaknesses exploited, with tens of thousands of issues mitigated, including a large share of critical findings

Aggregating Risk Across the Entirety of US Government, Not Just Enterprises

Now, take this one level up. Imagine being able to:

Summarize all provable attack paths across:

- Defense suppliers
- Critical infrastructure providers
- Financial and economic partners

Roll those findings into executive-level insights:

- Which common weaknesses are driving the most attack paths?
- Where are the most egregious supply-chain choke points for a sensitive weapons platform?
- Which remediation campaigns will deliver the largest risk reduction across the whole ecosystem?

Through a wide lens, allied defenders are now able to aggregate the risk and threat actor mapping across .gov, .mil and .com entities to gain a broader understanding of where to apply critical remediation cycles to fix what matters according to the risks that are most likely to adversely impact your specific environment.

That's where AI-driven offensive platforms become strategic risk instruments, not just technical tools. They allow national-level stakeholders to:

- → See systemic exposures before adversaries weaponize them
- → Fund and coordinate targeted capacity-building campaigns
- → Measure return on security investment (ROSI) in real time

When a new N-day drops, the time to exploitation is effectively zero. Organizations and their partners must move just as fast—find, fix, verify, and share lessons learned.

Critically, NodeZero's MSSP model lets a parent organization or central cyber team operate as a managed security provider for multiple partners or functional orgs. By centralizing assessments across many tenants, the MSSP model:

- → Surfaces cross-partner trends in misconfigurations, weak controls, and attack paths
- → Enables shared KPIs such as Mean Time to Remediation (MTTR) for specific weakness classes
- → Makes it straightforward to roll out Rapid Response capabilities across all subscribers at once, so every partner benefits the moment a new threat is identified

In other words, the same platform that helps a single company close its attack paths can help an entire ecosystem baseline its risk, drive down MTTR, and operationalize Rapid Response as a standard muscle movement.

Ready for Cyber Diplomacy at Machine Speed

Programs like DoW CSaaS and FBI's Operation Winter SHIELD are all pushing toward the same outcome and moving cyber people and programs into a space that highlights the speed and attention that cybersecurity will require:

- **More resilience** for under-resourced but highly valuable partners
- **Better signal-to-noise** in security operations
- **Shared playbooks and platforms** that scale across borders and sectors

To match the speed and creativity of AI-enabled adversaries, defensive cyber capacity building must be just as scalable and flexible. That means:

- Leveraging AI-driven offensive platforms like NodeZero as common rails for partner resilience
- Keeping humans in the loop by exception or judgment, escalation, and diplomacy
- Treating cyber diplomacy not as an annual conference talking point, but as a continuous operational practice

If our adversaries are using AI to break things, our partners deserve access to the world's best AI hacker to fix them—before the next campaign even begins. Because adversaries don't care whether you are .gov, .mil, or .com, they are probing every domain, every day, using AI to discover exploitable attack paths. Cyber is a team sport, and we will only succeed by collaborating with our allies and international partners.

About the Author

Dave Manzolillo is a Senior Program Manager at Horizon3.ai with more than 25 years of experience spanning cybersecurity, enterprise architecture, IT operations, and large-scale technology programs. Prior to joining Horizon3.ai, he served as Technical Director for Defense Industrial Base (DIB) Services at the National Security Agency and held multiple leadership positions within the U.S. Department of Defense. Throughout his career, Dave has focused on improving mission effectiveness through cyber defense, technology adoption, and operational scale. He holds a B.S. in Computer Science from Towson University, an MBA in International Finance from Loyola University Maryland, and multiple cybersecurity certifications, including CISSP and GIAC Security Essentials.