G1VE TECHNOLOGIES

The Port Is the New Front Line: Why UUV Sabotage, Seabed Threats, and Retaliation Risk Are Redefining Critical Infrastructure

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

Aug 2, 2026

Original source

https://www.linkedin.com/pulse/port-new-front-line-why-uuv-sabotage-seabed-threats-w-b--40f6e/

I. Critical Infrastructure Defense Just Went Underwater

For years, when executives and public officials talked about critical infrastructure, they tended to look horizontally:

- Grid,
- Water,
- Telecom,
- Pipelines,
- Ports,
- Logistics,
- Hospitals, and,
- Finance.

In 2026, that framing is no longer enough. You now have to look vertically — from the cloud to the control system to the seabed below the port. That is because a growing share of critical infrastructure risk is converging at the maritime edge, where ports, undersea cables, fuel terminals, waterways, OT environments, and logistics nodes are increasingly exposed to the same blended threat picture.

The clearest sign yet came when the U.S. Coast Guard published a request for information seeking commercially available technologies to defeat unmanned underwater vehicles, or UUVs, in order to bolster port security. The notice was blunt:

- Detection exists, but there are few fielded technologies with real defeat and mitigation capability. That distinction matters.
- Seeing the threat is not the same thing as stopping it. In the port-security environment, that gap can become catastrophic.

This is not a niche maritime-defense issue. It is a national security and homeland-security issue touching the U.S. Coast Guard , US Navy , port authorities, fuel distribution, seabed infrastructure, local governments, National Guard Bureau planners, and every enterprise that assumes the port will still work tomorrow morning.

II. Critical Infrastructure Defense Just Went Underwater

The U.S. Coast Guard 's language is worth taking seriously. Malicious actors can employ UUVs for intelligence gathering, surveillance, smuggling, sabotage of critical infrastructure, and kinetic strikes. Their covert nature and modern navigation capabilities make them difficult to detect, track, and mitigate using traditional maritime interdiction tactics. In other words, ports are not just dealing with faster boats or better drones above water. They are dealing with a threat that can approach quietly from underneath the operating environment itself.

The request also makes clear that the U.S. Coast Guard is not interested in partial answers. Solutions without defeat capabilities will not be considered. It wants sensor platforms, kinetic solutions, and integrated response systems that can detect, track, identify, and mitigate threats across ports, waterways, and coastal-security operations. That tells you the government's risk assessment has matured:

- Underwater detection without interdiction is no longer enough.

The operational backdrop makes the urgency obvious. U. S. Central Command (USCENTCOM) reported the first known Houthi use of a UUV in February 2024. More recently, U.S. forces used an unmanned surface vessel to strike a submarine and ship-maintenance facility in Iran — the first known U.S. combat employment of such a vessel. Once unmanned maritime systems become normal tools of state and proxy conflict, the port stops being rear-area infrastructure. It becomes front-line terrain.

III. The Cyber And Physical Layers Are Now Fused

The reason this port story matters beyond maritime operators is that it sits inside a broader retaliation-risk environment already documented earlier this year. Threat-intelligence firms warned in March that Iran-linked actors were increasing digital reconnaissance and preparing for potentially disruptive activity following U.S. and Israeli strikes. Analysts said worldwide critical economic infrastructure is now a primary target for Iranian-tied hackers, and specifically warned that critical infrastructure and financial-sector firms should remain vigilant for follow-on activity that could move beyond nuisance disruption into more coordinated operations.

That is the point many leaders still miss. In a modern conflict environment, the port is not only exposed to cyber attack or physical sabotage. It is exposed to both, often in layered or sequential ways. A UUV near fuel infrastructure, a cyber intrusion into OT systems, a logistics slowdown, and degraded communications can all reinforce each other. That is why CI Fortify's assumptions are so important:

- Degraded telecom,
- Unreliable vendors, and,
- Some level of adversary OT access should be treated as baseline planning conditions during conflict, not edge cases.

Put plainly:

- If your port-security concept assumes cyber and maritime threats arrive separately, you are planning for yesterday.

IV. Why Seabed Infrastructure Pulls Ports Into The National Security Center

Ports also sit astride the critical seam between maritime logistics and subsea infrastructure. Undersea cables carry the overwhelming majority of international data and support massive volumes of global finance, military communication, and cloud connectivity. Cable landing stations, nearby coastal infrastructure, and maritime approaches all create a geographic overlap between port operations and seabed dependencies. That means a port incident can have cyber, communications, logistics, and financial effects well beyond the waterfront.

This overlap is exactly why the port should now be understood as a multi-domain operating node, not a transportation asset. It is simultaneously a logistics hub, energy interface, customs

zone, OT environment, communications corridor, and maritime-security seam. It is where JP 4.0-style sustainment logic collides with homeland-security reality. If ports are degraded, everything downstream starts wobbling:

1. Fuel distribution,
2. Container flow,
3. Military mobility,
4. Industrial resupply, and
5. Even public confidence.

The seabed issue sharpens the threat. Once you accept that adversaries map underwater infrastructure in peacetime for possible interference in crisis, ports become natural pressure points because they sit nearest to the economic heartbeat of coastal critical infrastructure.

V. The Federal Response Is Still Uneven

The good news is that the government is at least asking the right questions. The U.S. Coast Guard 's RFI shows awareness that underwater threats are real and that defeat capability, not just detection, must be part of the kill chain. The bad news is that asking the question is not the same thing as fielding an answer. The U.S. Coast Guard is seeking responses by Aug. 7, wants systems that have already completed field testing, and may schedule maritime tests after receiving responses. That is a sensible process — but it also reveals how immature the current defeat ecosystem remains.

On the cyber side, the earlier Iran-linked threat reporting also exposed a worrying vulnerability:

- The Cybersecurity and Infrastructure Security Agency 's capacity can be stressed or politically constrained right when threat pressure is rising.
- In March, amid a funding lapse, reporting described the Cybersecurity and Infrastructure Security Agency operating at sharply reduced staffing levels while lawmakers were simultaneously warning that Tehran's history of retaliatory cyberattacks made critical infrastructure more vulnerable.

Whatever the politics, the strategic lesson is obvious:

- National infrastructure defense cannot depend on ideal staffing assumptions.

That leaves governors, port authorities, U.S. Coast Guard sectors, state fusion centers, National Guard Bureau cyber units, harbor police, and private operators with a heavier share of the real-world burden.

VI. What Port Security Doctrine Should Look Like Now

The port-security model that actually fits 2026 is not just a better fence, a better scanner, or a better cyber dashboard. It is an integrated multi-domain defense posture built around four assumptions.

First, underwater approaches are no longer passive space. They are maneuver space for adversaries using UUVs, divers, remote sensors, and gray-zone tools.
Second, OT and maritime systems are now part of the same mission picture. Fuel handling, ship scheduling, cranes, terminal systems, communications, and port-security response all need to be thought of as one defensive system.
Third, resilience beats elegance. In a conflict scenario, the port that can continue operating in degraded mode will matter more than the port with the prettiest normal-state dashboard.
Fourth, the Joint Force must treat ports as operational readiness nodes. The US Navy , the U.S. Coast Guard , US Transportation Command , NORAD & US Northern Command , Maritime Administration (MARAD) , FEMA , U.S. Department of Homeland Security , and the private sector all have a stake in whether these nodes survive disruption. This is not just public infrastructure. It is strategic mobility terrain.

VII. What Leaders Should Do Next

If you are a port operator, governor, U.S. Coast Guard leader, National Guard Bureau planner, federal executive, or critical infrastructure owner, five actions matter now:

1. Map underwater approaches and port-adjacent critical nodes with the same seriousness you apply to cyber crown jewels.
2. Build joint tabletop exercises that combine cyber intrusion, UUV threat, OT degradation, and communications loss in the same scenario.
3. Demand defeat-capable maritime-security solutions, not just awareness tools.
4. Integrate port planning with CI Fortify assumptions and consequence-based cyber prioritization.
5. Build direct coordination channels among the U.S. Coast Guard , Cybersecurity and Infrastructure Security Agency , local operators, and state emergency management structures before the incident, not after it.

The premier operators will also stop treating maritime physical security and cyber resilience as separate budget lines. They are now part of the same continuity problem.

VIII. Thought-Provoking Close: The Final Assessment

The port is the new front line because it is where the cyber threat, the maritime threat, the logistics threat, and the seabed threat increasingly intersect. The U.S. Coast Guard 's search for UUV defeat technology is not a narrow procurement event. It is a strategic signal that the U.S. is waking up to the reality that critical infrastructure defense now extends below the waterline.
The leaders who recognize that early will build ports that can absorb disruption and keep functioning. The ones who do not will discover, in the middle of a crisis, that the waterfront they thought was “support infrastructure” was actually operational terrain.

✨ 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