By James Careless

Securing Smart Ports Against Cyber and Physical Threats

Today's maritime shipping hubs are becoming "smart ports." They are harnessing digitization, network connectivity, automation, and artificial intelligence (AI) to move shipments faster and track them more easily. Aiding this process are vast networks of industrial sensors, automated guided vehicles, and algorithmic scheduling software — transforming maritime shipping into an integrated global logistics system.

But increased connectivity also creates new security risks. "As ports become increasingly automated and digitally connected, cybersecurity has become a core operational and safety requirement," said Daniele Mancini, field chief information security officer (CISO) at Fortinet, a cybersecurity provider focused on the convergence of networking and security to protect both information technology (IT) and operational technology (OT) environments. "The question is no longer whether ports will be targeted, but how effectively they can detect, contain, and recover from cyberattacks while maintaining the flow of global trade."

When IT Meets Heavy Metal

There are many threats confronting modern smart ports, each with its own consequences. What makes these hubs particularly vulnerable to hackers is the messy, accelerated convergence of enterprise IT networks and operational technology (OT) systems. Equipment that was historically isolated from outside operations, such as cranes, weigh stations, and cargo handling machinery, is now plugged directly into networked IT systems to maximize efficiency — often without adequate security protection from hostile players.

"The biggest risk is ordinary operational technology that was never built for the Internet yet is reachable from it, with weak authentication and unpatched firmware," said Saman Zonouz, associate professor at the Georgia Institute of Technology, who directs the Cyber-Physical Systems Security Research Laboratory securing engineered systems. "When we automated discovery of such devices, we found that prior estimates undercounted the exposed population by as much as a factor of 37, and that about 96 percent were open to recent critical vulnerabilities."

This astonishing level of exposure allows hackers to execute complex attacks on smart ports without physical access to the docks. This is because standard, off-the-shelf controllers governing cranes and other massive physical infrastructure are vulnerable to web-based interference.

Vulnerability testing on these systems produced alarming results. "We built proof-of-concept malware that lives entirely in the web interface modern controllers now embed and used it for Stuxnet-style sabotage," Zonouz said. "We confirmed that controllers from every major vendor, roughly 80 percent of the global market, were susceptible. An attacker does not need to touch a crane or implant custom firmware to make it behave dangerously."

The attack surface — the range of smart port systems vulnerable to cyberattacks due to weak security — is widened dramatically by each port's supply chain of vendors, original equipment manufacturers (OEMs), and contractors who require remote access to maintain



Conor McLaren
Dragos



Daniele Mancini
Fortinet



Professor Kevin Jones
University of Plymouth



Michael Langer
Cyolo Security



Saman Zonouz
Georgia Institute of Technology



From port operations to global supply chains, maritime organizations are embracing digital transformation at an unprecedented pace. Building cyber resilience across IT, OT and connected systems is essential to keeping trade secure, efficient and moving forward. Fortinet image.

this specialized equipment.

"The biggest exposure in a modern port is access, more than any single device," said Michael Langer, VP of products at Cyolo Security, a cybersecurity platform that controls and secures access to operational technology and cyber-physical systems. "A typical terminal has dozens of third parties connecting into its environment. Many of them still use legacy VPN [virtual private network] technologies, shared credentials, or remote desktop tools installed years ago that nobody fully tracks."

By exploiting these overlapping access points, attackers can easily breach a port's IT side and then move into its OT environment. It doesn't take much to pull this off. A phishing email opened by an unwary office worker can lead to an attacker taking control of physical machinery miles away on the quay. In fact, "the most critical exposures for a smart port are the connections between enterprise IT and the OT that moves cargo," said Conor McLaren, director of threat intelligence at Dragos, a cybersecurity firm specializing in extended operational technology to protect critical infrastructure.

Sometimes, hackers get in by targeting third-party vendors who have access to a port's web-connected network. One method is a "watering hole" attack, in which attackers compromise a website routinely visited by their intended targets.

A case in point: "In October 2024, a threat group ran a watering hole attack through the water utility serving Haifa Bay Port," McLaren said. "Dragos assessed the activity was most likely aimed at identifying and profiling personnel, demonstrating how adversaries could reach a port's strategic tenants through a lower-barrier supplier rather than attacking them directly."

A programmable logic controller (left), its power supply (center), and a human-machine interface touchscreen (right) on the CPSec Lab bench. Controllers like these run the automated equipment at modern ports, including cranes, gates, and pumps. Georgia Institute of Technology image.

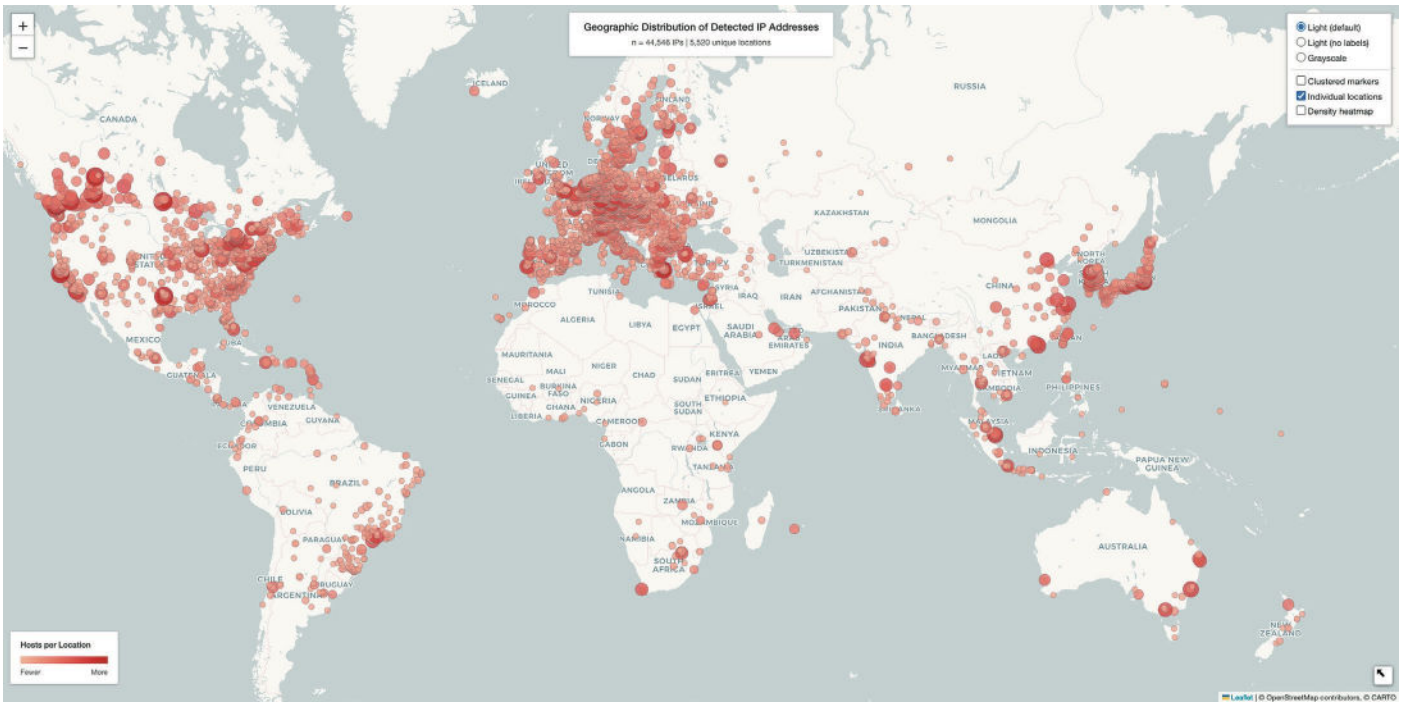


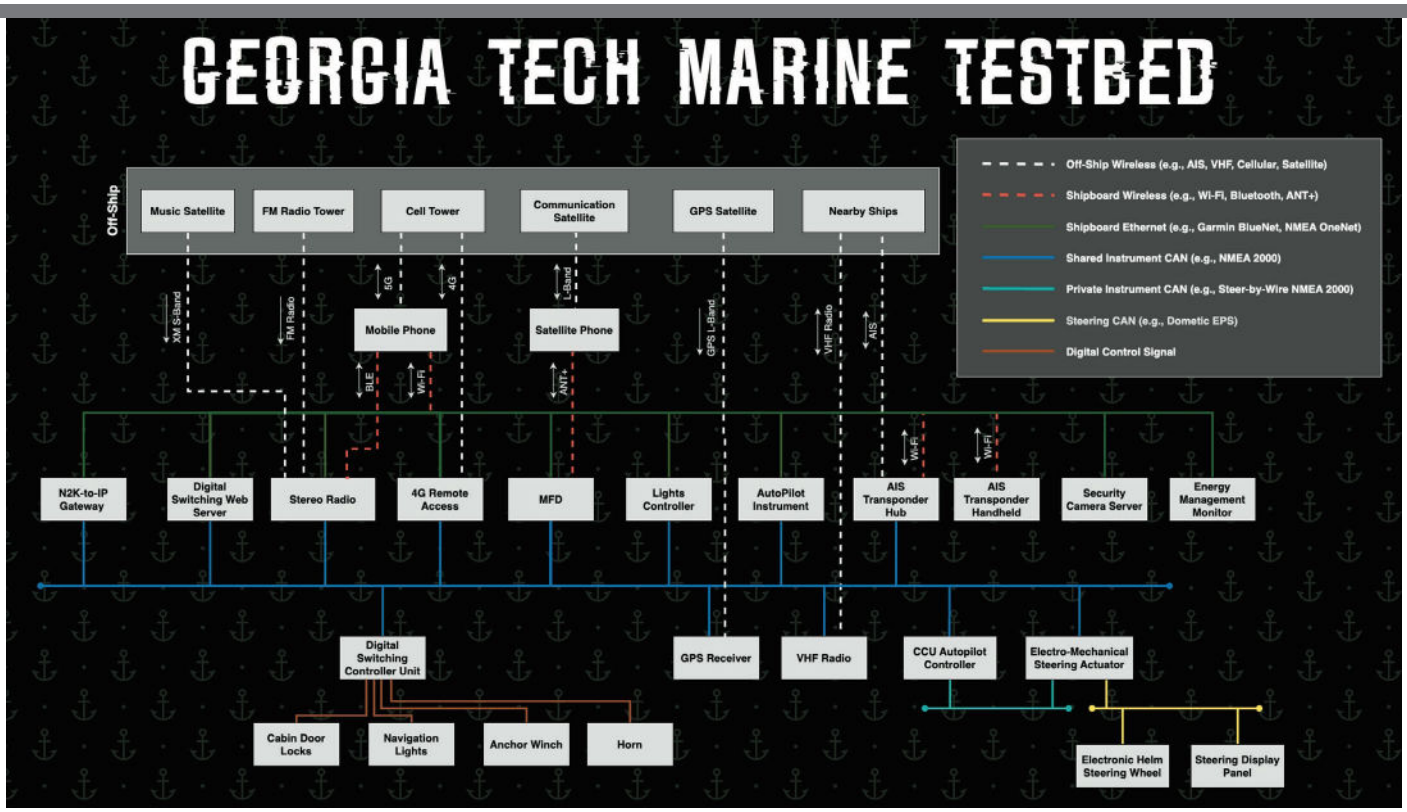
The Blind Spot of Shadow Networks

Even when smart port authorities believe they have established a secure perimeter and properly segmented their IT and OT networks, they can still be attacked through "shadow networks."

These are unmapped, unmonitored communication channels created during equipment upgrades or localized fixes. Typically, these occur when technicians

Internet-exposed energy devices found worldwide in a single large-scale scan by the lab, one example of how much operational technology sits directly reachable on the public Internet. The same kind of exposure affects port and maritime systems. Georgia Institute of Technology image.







Left: The CPSec Lab's full-scale maritime testbed at Georgia Tech, built from real, commercially available marine equipment. It includes a chart plotter and multifunction display, a steer-by-wire helm, autopilot, VHF radio, AIS, NavTex, and satellite and GPS links, together with an electric outboard engine and physical actuators such as an anchor winch and horn. The lab uses it to study shipboard cyber-physical attacks and defenses end to end. Georgia Institute of Technology image.
Above: The network topology of the Georgia Tech maritime testbed, showing how its systems interconnect: off-ship wireless links (AIS, VHF, cellular, satellite), shipboard Ethernet, and instrument and steering CAN buses (NMEA 2000 and steer-by-wire), tying together devices from the multifunction display and autopilot to the steering actuators, door locks, and anchor winch. This interconnection is exactly what lets a cyber intrusion reach physical shipboard equipment. Georgia Institute of Technology image.

or vendors install quick wireless links to monitor or fix gear on the fly without alerting central IT, and then leave these undocumented backdoors in place and open when the job is done.

Shadow networks thrive on the sheer complexity of modern port systems. "In fact, if you look at even a regular port, the number of different networks required to support different aspects of functionality within the port are significant," said Professor Kevin Jones, deputy vice chancellor of research and innovation at the University of Plymouth, who operates the Cybership Lab to research maritime cybersecurity implications. "Those are already a network of devices, many of which probably aren't properly viewed as computing devices."

A prime example of this vulnerability is associated with advanced ship-to-shore cranes. Professor Jones recalled one instance: "There was a pretty good security architecture around most of the port, but there were a number of software-controllable cranes which had effectively an upgrade contract with the suppliers. That upgrade contract worked over a 5G mesh network that the port were not aware of, while the cranes communicated with other parts of the port network for perfectly legitimate functions. What this meant is that their entire perimeter security was fundamentally flawed."

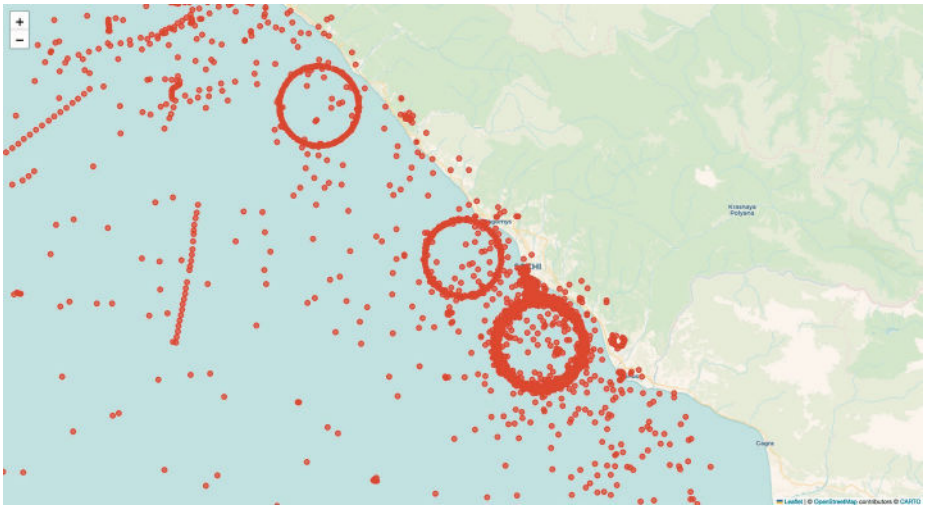
The emergence of shadow networks is compounded by the sheer volume of new hardware being incorporated into smart ports. "This potential vulnerability is converging with how ports are being built," said McLaren. "These [exposures] include automated cranes and yard equipment on cellular gateways at unmonitored OT edges, shore power and battery storage running protocols that allow control without authentication, and a tenant ecosystem of carriers, integrators, and utilities."

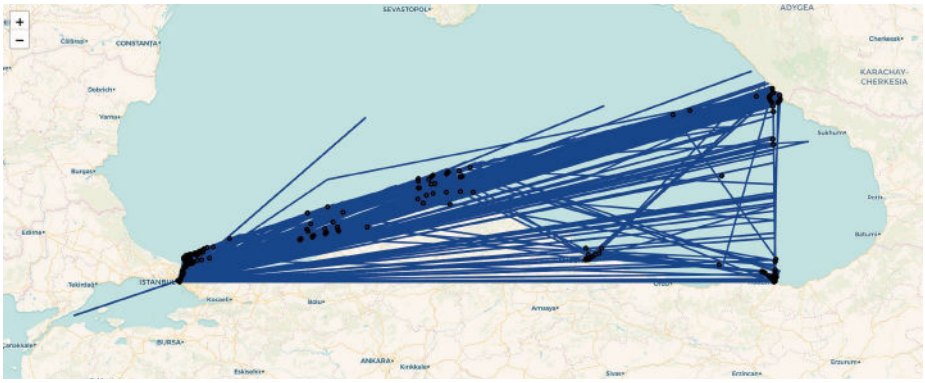
The penetration point for crippling cyberattacks can often be a seemingly harmless piece of peripheral equipment running an active data stream that the port's IT team doesn't know about.

"We have seen an actual example of a conveyor system — which was not deemed to be part of the port network — that actually had a network connection so that it could report issues during hours of operation," Professor Jones said. "That network connection was not one-way and it was not protected by an internal firewall — giving attackers access to all aspects of the port infrastructure and networks."

The Ship-to-Shore Vulnerability

Increasingly, the ships arriving at a smart port's docks are essentially floating smart cities, initiating a complex digital





Above: GPS positions that ships broadcast near the eastern Black Sea, reconstructed by the lab from public vessel data. The tight red circles are physically impossible tracks produced by GPS spoofing rather than real movement. Georgia Institute of Technology image.
Below: Lines connecting vessels' true locations to the false positions their GPS reported across the Black Sea. Widespread displacement like this can send a ship off course without any onboard alarm. Georgia Institute of Technology image.

handshake with the port's IT network every time they berth.

"Vessels now carry their own connected OT," said Langer. "This is because OEMs routinely need remote access to onboard systems for maintenance and monitoring, so every ship-to-shore connection extends the attack surface from the port to the ship."

Unfortunately, this means that a compromised smart port can infect a vessel. Conversely, malware dormant on a cargo ship's IT network can spread into the smart port's operational technology as soon as digital manifests and remote power connections are established. It is the modern IT version of contagious diseases being spread by ocean-going vessels.

From Digital Breaches to Physical Gridlock

Once hackers breach a smart port's physical machinery or terminal operating systems, the fallout is swift: "The immediate impact is operational paralysis," Mancini said. "Ships cannot be unloaded efficiently, containers cannot be tracked accurately, trucks cannot be processed quickly, and cargo begins to accumulate throughout the terminal. Even relatively short disruptions can create significant backlogs."

Cybercriminals can also exploit compromised port systems for cargo theft. In some cases, "attackers reportedly gained access to logistics systems and container information, allowing criminal groups to identify and retrieve specific containers," said Mancini. "This demonstrates how digital compromises can directly affect physical cargo operations."

Cyberattacks can cause major disruptions even when ransomware is not involved. In November 2023, DP World Australia, which handles approximately 40 percent of Australia's maritime freight, detected unauthorized access to its corporate network. The company disconnected its systems from the internet to contain the intrusion, disrupting landside operations at several major ports.

"The downstream impact of these lasts much longer than the outage," Langer said. "Vessels miss their berth windows and skip ports, cascading delays across entire shipping rotations. Perishable and temperature-controlled cargo is at risk. Manufacturers waiting on parts slow or stop production."

Because of these scheduling delays, a localized outage quickly spirals into a wider economic crisis that outlasts the hack itself. The result is that it can take weeks to clear the overall backlog, long after the port's own operating systems are brought back online.

Hardening the Port

To guard against such threats, smart ports need to "harden" their defenses by moving past simply detecting malware to actively controlling access to their IT and OT infrastructures.

This requires adopting zero-trust principles, which verify access requests rather than automatically trusting users or devices, alongside strong network segmentation that limits unauthorized movement between IT and OT systems.

"The application of zero-trust, the notion of segregated networks, the appropriate use of firewalls, and the limiting of access privileges — all of which are well understood techniques — can make a huge difference," said Professor Jones.

Conventional software security testing may overlook how legitimate control commands could be manipulated to create unsafe physical conditions. To catch those blind spots, smart port operators need to test the physical limits of their machinery, not just their software.

"The most effective step is to find the dangerous conditions before an attacker

does, which means testing a control system's physical consequences and not only its code," Zonouz said. "We built a physics-aware tool that treats a controller as a sealed box, sends only the commands an operator is allowed to send, and measures how close the process comes to an unsafe limit."

New Rules and Hard Deadlines

International maritime organizations are strengthening cybersecurity expectations through updated guidance and technical requirements. The International Maritime Organization (IMO) provides cyber risk management guidance, while the International Association of Classification Societies (IACS) has established cyber resilience requirements for newly contracted ships and onboard systems.

"Frameworks like IMO guidance [and] the IACS UR E26/E27 cyber risk assessment and resilience requirements for ships and onboard equipment, are raising the baseline across the industry, including how third parties access vessels," Langer said.

In the United States, the Coast Guard's maritime cybersecurity regulations entered into force in July 2025, with phased compliance deadlines extending into 2027. "Ports should pair [those defenses] with continuous asset discovery, strong authentication and network segmentation, and current firmware," said Zonouz. "And alignment with the U.S. Coast Guard's maritime cybersecurity rule, whose assessment and plan requirements take effect in 2027."

Complicating this cyber-defense strategy, on the human level, is the fact that mariners and longshoremen are trained to prioritize physical safety over everything else. While this approach can save lives, it gives hackers more time to hide in the systems and wreak havoc while crews troubleshoot what they assume are mechanical faults.

Because of this instinct, effective cyber resilience relies on regularly drilling dockworkers on how to run the terminal without computers — using handheld radios, paper manifests, and manual machine controls where possible — so cargo keeps moving while security teams rebuild the network.

"The most effective programs we see focus on controlling access and limiting impact, rather than only detecting threats after the fact," Langer told TSI. "Tested manual fallback and incident response plans [ensure] operations can continue while systems are restored."

Cheap Sensors, AI, and Spoofed Signals

As smart port cyber threats evolve, the maritime industry's ongoing deployment of web-connected devices will result in ever-larger attack surfaces for hackers to exploit, and the increased risk of cheap, unsecured gadgets taking down critical infrastructure.

"By compromising the output of a $5 wind sensor, we were able to show that we could severely damage a multimillion-pound platform," said Professor Jones. "Because, of course, there was no real thought of that sensor being a security vulnerability."

Meanwhile, the rise of customized AI-driven attacks and cheap, off-the-shelf criminal software will lower the barrier for hackers targeting smart ports and ships.

"AI-driven attacks are going to be a big issue," Professor Jones said. "We are already seeing a development of attack capabilities that are more specific to maritime. This includes being able to buy ship attack kits or port attack kits, which includes the kind of skills you need to manifest them."

Hackers may also hide behind the fact that AI is notoriously difficult for humans to double-check. So, if an automated crane or scheduling program suddenly makes a disastrous call, terminal staff won't immediately know whether they are under cyberattack or just dealing with a routine computer glitch — again buying attackers valuable time to inflict even more damage.

If that isn't concerning enough, "operating issues such as AI hallucination can actually be influenced in some circumstances by training sets," Jones said. This opens yet another opportunity for hacker mischief. "There are some parts of the maritime space where a deliberate sort of misinformation feed to mistrain the AI can then cover up future activity."

The fundamental objective of threat actors is also evolving. Many are no longer satisfied with establishing a foothold to steal data; they are actively seeking to manipulate the machinery that moves the global economy.

"The next generation of maritime threats may evolve from maintaining persistent access to mapping control loops," said McLaren. "So they can cause physical disruption to port operations."

Attackers may also manipulate satellite-navigation signals or falsify Automatic Identification System (AIS) data, tricking autonomous marine systems into executing dangerous physical commands while their dashboards report normal conditions.

"The next wave will target the sensors and signals that automation trusts, rather than the computers themselves," Zonouz said. "Our global measurement of maritime positioning data found tens of thousands of anomalous episodes and dozens of persistent spoofing hotspots, including regions that later saw real groundings and disruption such as the Red Sea and the Strait of Hormuz."

Despite the growing sophistication of these threats, cybersecurity experts agree that smart port operators can reduce their exposure through better asset visibility, access controls, monitoring, staff training and incident response planning.

"It is expected that the challenge will grow because new infrastructure and AI are being deployed faster than security keeps pace, but it's a prioritization and investment problem rather than a technology one," said McLaren. "But ultimately, port operators that establish asset visibility, monitoring, access control, and incident response now will be defensible as the threat landscape evolves."

"Port cybersecurity will become a bigger challenge as terminals and vessels automate further, but it's a manageable one," Langer agreed. "Ports that build that control into their operations now will be in a much stronger position to keep cargo moving whatever the threat landscape brings."