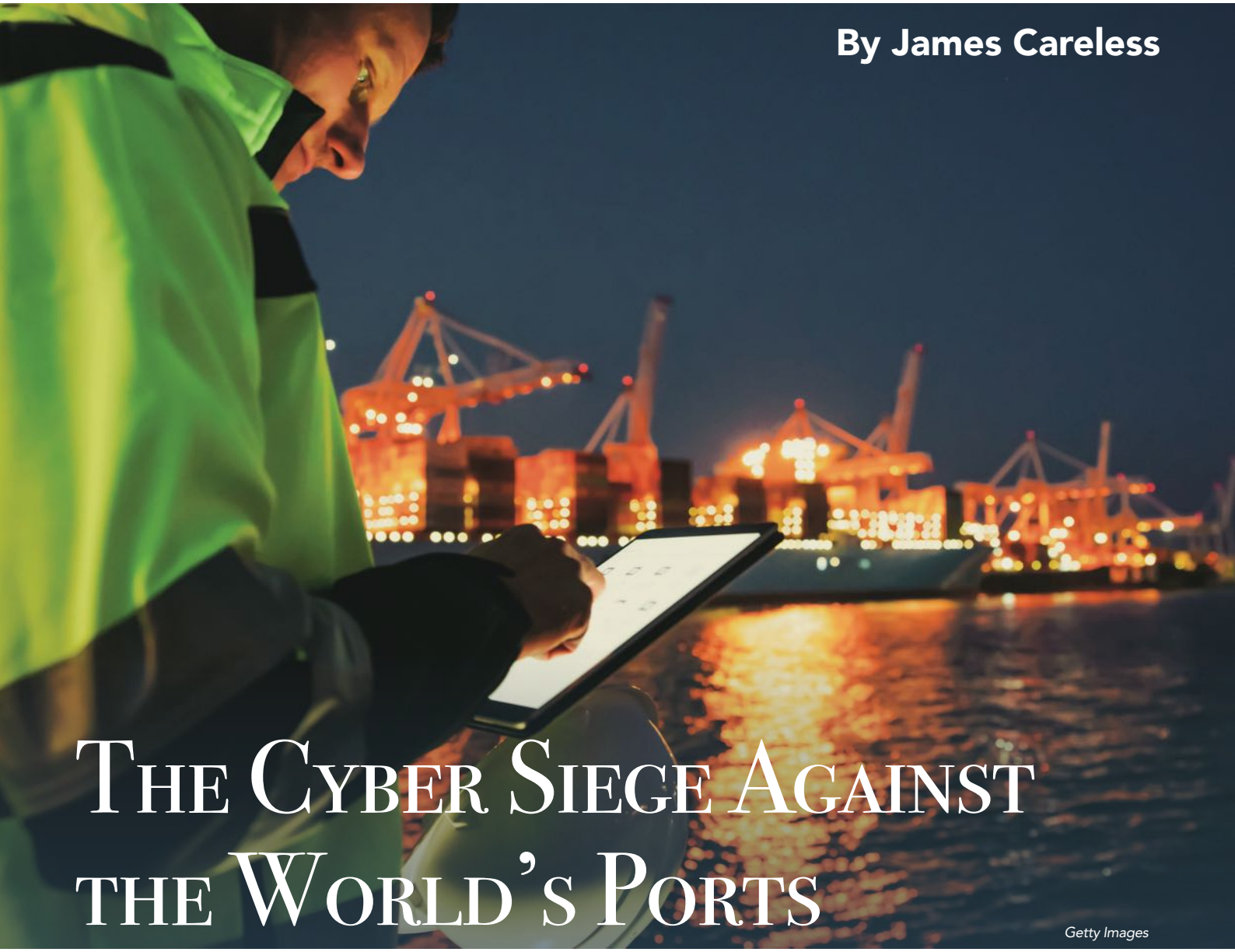


By James Careless

The Cyber Siege Against the World's Ports

Getty Images

The world's ports are under siege, not from navies and battleships, but from hackers and cyber weapons. Unfortunately, their ability to withstand these attacks varies widely across the industry.

"There is significant variation in cybersecurity readiness across the global port sector," said Steve Felder, executive director at Code Blue Cyber, a global cybersecurity company providing end-to-end cyber crisis solutions. "On one end of the spectrum, large international port operators have made substantial investments in cybersecurity. At the other end are smaller ports, individual terminal concessionaires, and ports operated directly by governments or port authorities, where cybersecurity maturity can vary considerably."

Unfortunately, the rapid pace of cyber warfare is making it difficult for even the most advanced ports to cope, let alone the ports that still have to play catch-up.

"Rapid digitization — including the rise of Maritime Autonomous Systems, where ships can be remotely controlled from shore — is outpacing the sector's cybersecurity maturity," said Chris Grove, director of Cyber Security Strategy at Nozomi Networks, a cybersecurity protection firm. "It's common to find ships and terminals running devices and even entire systems that operators aren't aware of, and internal expertise to evaluate OT/IoT exposure is often thin compared to the deep judgment-based expertise the industry has built up for traditional marine safety over decades."

Overall, the state of maritime port readiness is extremely uneven. This fact has serious implications for the global supply chain, which is only as strong as its weakest link.

"Cybersecurity readiness across global ports remains uneven, and, in many cases, has not kept pace with digital transformation," said Daniele Mancini, EMEA Field CISO at Fortinet, a global cybersecurity provider focused on IT and operational technology

Steve Felder
Code Blue Cyber

Chris Grove
Nozomi Networks

Daniele Mancini
Fortinet

Prof. Kevin Jones
University of Plymouth

resilience across critical infrastructure. "The gap is particularly visible between developed and developing economies. ... This is concerning because some of the countries most dependent on maritime trade — such as developing economies and small island states — are often the least prepared for cyber incidents."

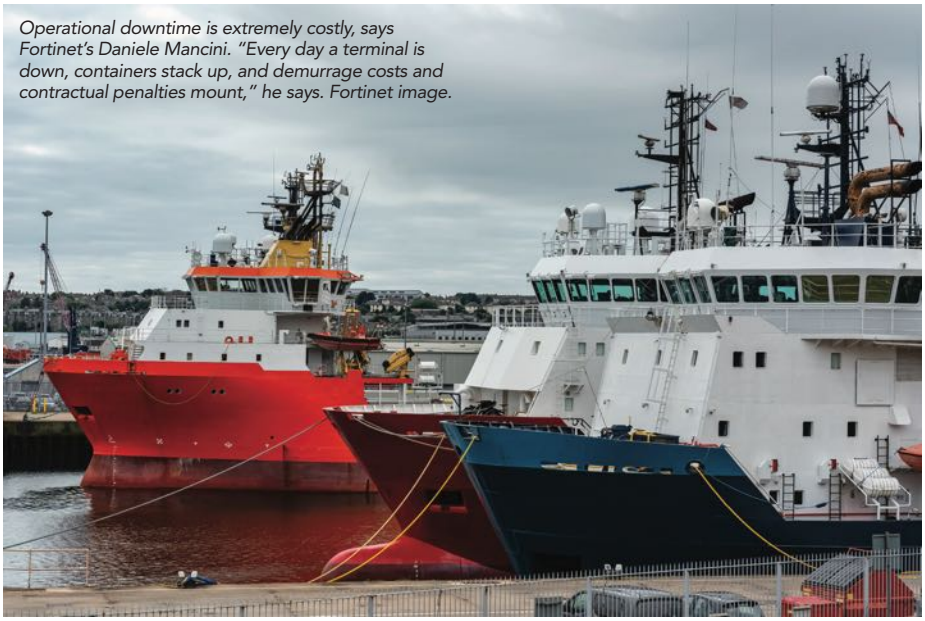
Tempting Targets

Because of their vital role in the global supply chain, maritime ports are tempting targets for hackers. The combination of their economic value and the uneven state of their cyber defenses makes them logical victims for extortion attacks.

The reason port authorities are often willing to pay cyber extortionists comes down to the sheer economic toll of shutting down these critical maritime chokepoints. Anytime a major port — or even a smaller port — is disabled, the resulting delays can translate into massive financial losses for the world economy.

Because terminal downtime cascades immediately into demurrage costs for shippers and contractual penalties for terminals, port operators are under immense pressure to give in to ransomware demands quickly so that their facilities can get back to business.

"Operational downtime is extremely costly," said Mancini. "Ports operate on razor-thin schedules. Every day a terminal is down, containers stack up, and demurrage costs and contractual penalties mount. This makes ports attractive targets for ransomware attackers, who seek to exploit the pressure on operators to restore services quickly. Secondly, criminal groups can use cyber intrusions to locate and redirect high-value container shipments.



Operational downtime is extremely costly, says Fortinet's Daniele Mancini. "Every day a terminal is down, containers stack up, and demurrage costs and contractual penalties mount," he says. Fortinet image.

Compromising these systems can enable cargo theft, smuggling facilitation, and fraud activities, in which organized crime has a large interest. Turnover can sometimes be comparable to the gross domestic product of a small country."

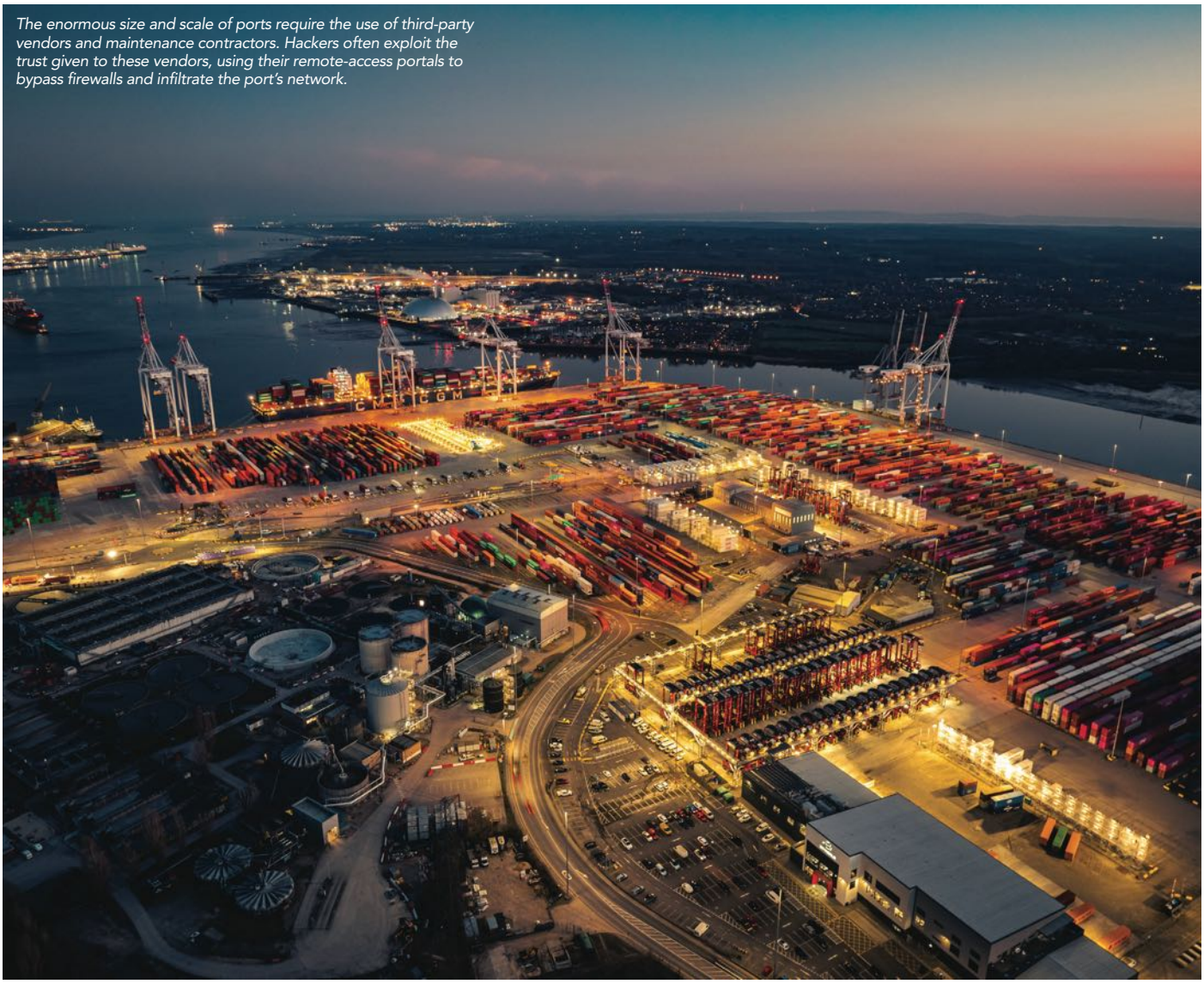
These are crimes aimed directly at stealing from ports or extorting terminal operators. But there are even larger reasons why high-level hackers might target maritime infrastructure. By intentionally gridlocking global shipments, sophisticated threat actors can leverage the resulting economic chaos to pull off multi-billion-dollar financial crimes, including deliberate stock market manipulation.

"If you think about global impact — if for example, you are a major player and have significant cash to invest and significant resources — you could imagine crimes that were literally worth billions by stock market manipulation and other things based on sort of denying a port normal activity," said Professor Kevin Jones, deputy vice chancellor, research and innovation at the University of Plymouth and founder of its Cybership Lab Research Group. "So, you add all that together and the potential for very serious attacks is high."

State-Sponsored Sabotage

While cyber criminals hack ports for money, hostile nation-states target them to gather intelligence and lay the groundwork for disruptions during times of conflict.

"State-sponsored actors view maritime infrastructure as strategically important national infrastructure," said Felder. "This makes ports an attractive target for



The enormous size and scale of ports require the use of third-party vendors and maintenance contractors. Hackers often exploit the trust given to these vendors, using their remote-access portals to bypass firewalls and infiltrate the port's network.

espionage, influence operations, and, in some cases, the ability to disrupt critical supply chains (given the domino effect and multiple players involved in the supply chain) if geopolitical tensions escalate."

One area of particular concern involves Advanced Persistent Threats (APTs). These are sophisticated, long-term intrusions designed to establish and maintain covert access to critical networks.

"State-linked APTs can penetrate port networks, targeting systems such as container cranes and vessel traffic management services to establish persistent, dormant access that can be activated during periods of geopolitical tension or conflict," Mancini said.

In some instances, hostile nation-states don't even need to covertly plant APTs in port software. Purchasing choices made by certain port authorities have made it possible for critical infrastructure to arrive on the docks with potential vulnerabilities already embedded in the hardware itself.

"Nearly 80% of the U.S.'s ship-to-shore cranes are built by a single Chinese state-owned manufacturer, which has pushed for remote access to its machines at U.S. ports," warned Grove. "This raises documented concerns among U.S. officials about hidden backdoors or espionage risk in critical terminal equipment."

While dormant cyber weapons depend on future conflicts to be activated, hostile nation-states are already weaponizing GPS and navigation telemetry on a daily basis. The result is a continuous stream of localized disruptions that physically endanger vessels and throw port schedules into chaos.

"GPS spoofing incidents reached roughly 1,000 disruptions per day in 2025, affecting over 40,000 vessels worldwide, with confirmed impacts causing navigational safety and physical groundings," noted Grove. "There are many reports in the public about a wide array of GPS and other wireless-related attacks impacting operational technologies."

Legacy Dangers

Most of the world's ports have been in operation for decades or even centuries — some for thousands of years. As they age and modernize, new

technology tends to get grafted onto old systems. Unfortunately, combining modern internet connectivity with legacy Operational Technology (OT) engineered solely for physical reliability creates serious security gaps.

"Much of the equipment running ports (crane controllers, sensors, safety systems) is decades old and was never designed with security in mind," said Grove. "Digital and remote-access features have simply been bolted on over time, meaning an unpatched vulnerability in a port crane's software could halt crane movements or cause erratic, potentially dangerous behavior."

Because of the sheer size and scale of ports, many rely on third-party vendors and maintenance contractors to keep their operations going. Unfortunately, hackers often exploit the deep trust given to these vendors, using their remote-access portals to bypass firewalls and quietly infiltrate the port's core network.

"We've seen examples of some ports where they have sort of a nicely segregated network with firewalls and a whole set of cranes with a 5G mesh, which they weren't aware of because it was a third-party supplier that actually had that mesh for updating firmware on those cranes," Jones said. "This meant effectively they were not aware that there was a completely unmonitored backdoor access to their OT network, which was connected through appropriate firewalls to their IT network."

To add to the challenge, much mechanical port equipment contains embedded microcontrollers that operators may not even recognize as part of their cyber-attack surface.

"There are probably pieces of equipment that people aren't even aware are actually computer-based," noted Jones. "We've seen examples of things like conveyor systems and hopper doors that were not regarded as computer equipment and so weren't included in things like cyber audits, but actually did have embedded microcontrollers which ransomware or more sophisticated malware could be installed on."

Because of this complex web of shared access and hidden hardware, many port operators discover that their systems have been compromised not by direct attacks, but through a vendor's careless security hygiene.

"At Code Blue Cyber, we see an overwhelming majority of customers experiencing major cyber incidents as 'collateral damage' through third parties," Felder said. "The challenge is therefore not simply one of technology, but of managing cyber risk across an interconnected operational ecosystem where a weakness in one organization can have cascading effects throughout the port community."

Gridlock on Shore

A successful cyberattack against a port's core management software doesn't just encrypt files; it physically paralyzes the yard, making it impossible to locate, load, or transport cargo.

"A common target is the Terminal Operating System (TOS)," said Mancini. "Attackers encrypt the TOS to disrupt port operations, as without it containers cannot be identified, located, or moved."

When this happens in modern digitized ports, the results can be catastrophic. "As ports and ships have become smarter, more connected, and more autonomous, many cannot seamlessly transition to manual operations during incidents the way an office can work offline temporarily," Grove said. "This makes ports prime targets for ransomware groups seeking leverage and fast payouts."

Meanwhile, the interconnected nature of global logistics means a single vulnerability at a software vendor can trigger a massive, cascading failure across multiple, unaffiliated port facilities worldwide.

"We saw this in 2023 when a BlackBasta ransomware attack on a major crane-maintenance software vendor cascaded down to the ports that relied on that vendor's software," said Grove. "This happened even though the ports weren't the intended target."

This operational gridlock is compounded by the industry's continued reliance on fragmented, outdated communication tools. Because day-to-day logistics still depend heavily on manual workarounds, port operators lack the real-time visibility needed to make fast, informed decisions when an unexpected cyber crisis strikes.

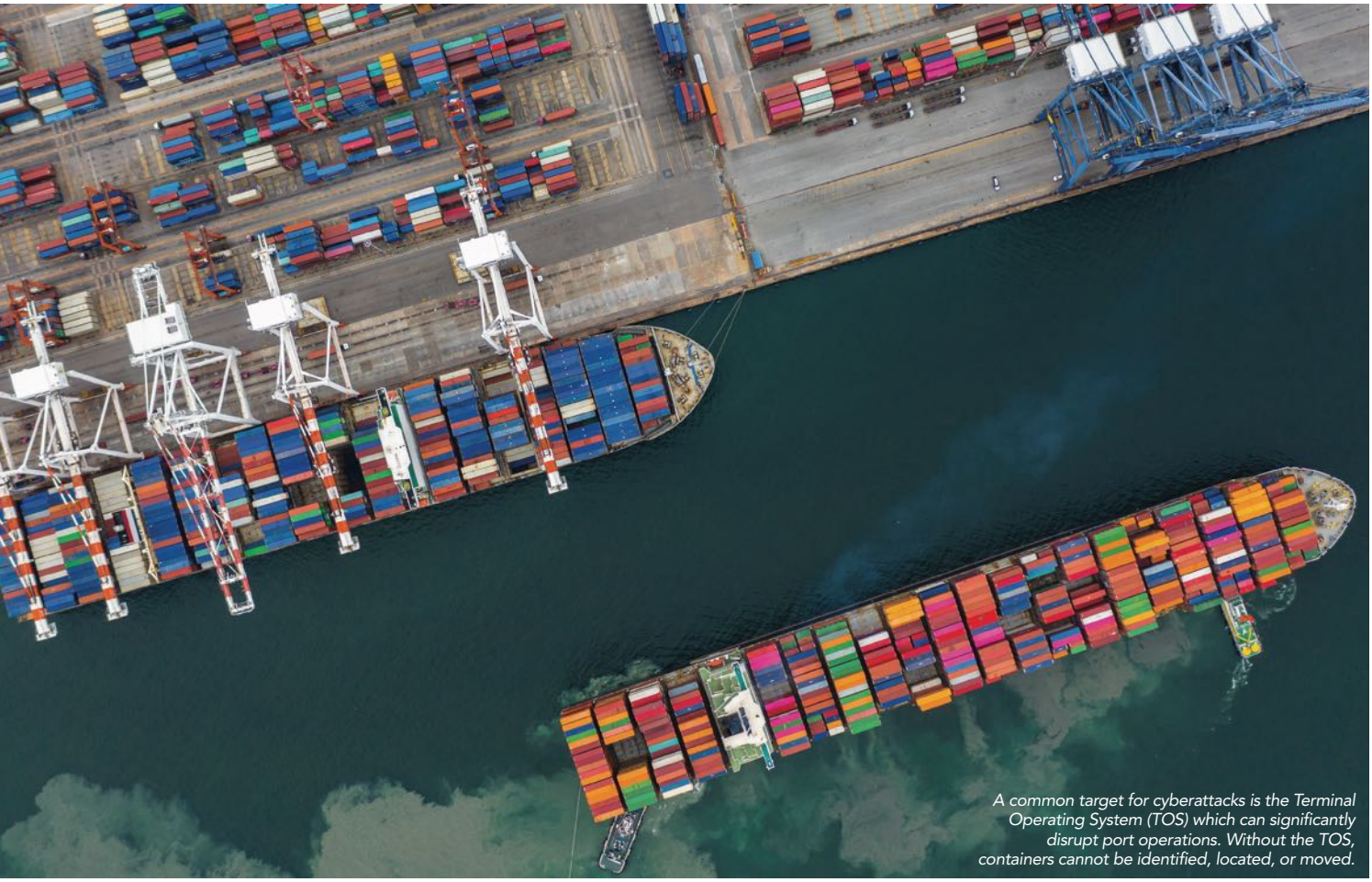
"It is important to note that most functions in the maritime supply chain are still running on legacy EDI systems, email, spreadsheets, and proprietary portals," Mancini told Transport Security International magazine. "As a result, data is often fragmented, delayed, and, in most cases, manually reconciled. Thus, there is no predictive visibility, meaning slower decision-making during unexpected events."

From Encouragement to Enforcement

In response to escalating cyber threats, the maritime port sector is moving away from voluntary best practices toward rigid, enforceable mandates designed to force accountability. A major push for this change comes from the International Association of Classification Societies (IACS). Its Unified Requirements — UR E26 and UR E27 — make cybersecurity requirements mandatory within the IACS classification regime for applicable new ships contracted for construction on or after July 1, 2024.

"2026 is emerging as what some in the maritime cybersecurity community are calling the 'first year of practical verification' for IACS UR E26/E27," Grove noted. "This is happening as vessels contracted under the July 2024 requirements move from design approval into construction, commissioning, sea trials, and class verification."

Government regulators are biting into port cybersecurity with similar legal teeth. "The U.S. Coast Guard's final rule, effective July 16, 2025, marks a notable shift from encouragement to enforcement," said Grove. "It requires port and terminal operators to develop a comprehensive cybersecurity plan and a separate cyber incident response plan, conduct regular risk assessments and exercises, and report significant incidents to the National Response Center." (Implementation is phased, with incident reporting already in force and major



A common target for cyberattacks is the Terminal Operating System (TOS) which can significantly disrupt port operations. Without the TOS, containers cannot be identified, located, or moved.

planning and assessment requirements taking effect through July 2027.)

Nevertheless, the global regulatory landscape remains a patchwork, with massive variations in how different nations mandate incident reporting thresholds.

"They range greatly from very laissez-faire — as in 'please tell us if you notice anything' — through to 'if you notice anything, you are required to inform a central authority,'" Jones said. "The U.S. actually represents one extreme, with a requirement to inform the Coast Guard of basically anything that looks out of the ordinary. The U.K. is on another part of the spectrum, where there are clearly defined levels at which you're required to inform government, and requests for information below those levels are optional."

Despite the push for new rules, experts caution that heavy-handed enforcement can backfire. "There are a lot of places where the 'sky is falling' model has been adopted and people are looking for unrealistic responses, which then means real progress just won't happen," cautioned Jones. "Instead, there's a growing trend toward focusing on low-hanging fruit — basic training and basic cyber awareness can make a big difference."

Making Cybersecurity a Health and Safety Issue

Since cybersecurity is fundamentally involved with computers and the internet, surely it makes sense to consider it as a function of the IT department, correct?

Maybe not. "On the ground, what's proving effective is treating cybersecurity as part of the existing safety and security culture rather than a separate IT concern," said Grove. "This is done by folding it into facility security plans, training programs, and documentation the same way physical safety has long been handled."

That's not all. Recognizing the sheer scale of the cyber threat, national authorities are injecting cybersecurity education into foundational training for the next generation of maritime personnel.

"Within the U.K., the MCA — the Maritime and Coastguard Agency — has recently revamped its training syllabus for deck officers," Jones noted. "It now includes the notion of cybersecurity in about 60 percent of the approximately 18 modules you're required to take. Prior to this revamp, that number was zero."

Ultimately, establishing a defensible cyber posture requires absolute network clarity for maritime port operators. They cannot protect their environments without knowing exactly which devices and vendors are plugged into their networks.

"Practically, that means building the foundational visibility first," Grove

advised. "You need to know what's actually on your network, from crane controllers to IoT sensors to third-party vendor connections, before you can meaningfully assess risk, prioritize fixes, or respond to an incident."

Building True Resilience

The fundamental goal of improving cybersecurity at the world's ports is resilience. There is no question that attacks will continue to escalate and become ever more sophisticated, particularly with the assistance of artificial intelligence. That is why the key is constantly enhancing the sector's defenses — so its operations remain resilient enough to keep moving, no matter what hackers throw at them.

Yet before true resilience can be achieved, the maritime industry must solve a massive forensic data gap. Outdated vessel recorders currently make it nearly impossible to distinguish a deliberate cyberattack from standard mechanical failure.

"If you look at the information recorded by, say, a voyage data recorder, it's basically useless for doing cyber forensics and cyber analysis," said Jones. "There's a belief among people who work in my sector that there are far more cyber incidents than we're aware of, simply because a lot of them are misreported as equipment failure or crew error — people are just not trained to recognize when a cyberattack has occurred."

Building and maintaining this level of resilience over the long haul must be driven from the very top of each port's organization.

Fortunately, that shift is already underway. "The new regulatory requirements are helping to elevate cybersecurity from a technical issue to a board-level operational risk," Felder said. "We at Code Blue Cyber assert that cybersecurity is no longer viewed as simply an IT issue: it's a leadership issue."

In the end, the path forward comes down to a fundamental shift in mindset. To survive and thrive in an increasingly dangerous cyber environment, ports must treat digital defenses as core to their survival.

"Treat cybersecurity as mission-critical infrastructure, not an IT sidebar," concluded Grove. "The clearest message from the recent wave of regulation and high-profile incidents is that ports and shipping operators can no longer separate 'keeping cargo moving' from 'keeping systems secure' — the two are now the same job." TSI