Information Provided by Trident Group America, Inc

THE FLEET POISONED AT THE SOURCE

Maritime Software Supply Chain Attacks and the New Mass-Casualty Cyber Threat

The maritime industry's digital backbone is under attack. Malicious code inserted into trusted software can compromise vessels, ports, and critical systems—simultaneously, silently, and at global scale.

THE NEW REALITY

GLOBAL REACH
A single compromise can propagate across fleets, fleets, and supply chains

STEALTHY BY DESIGN
Malicious code in trusted software evades detection and persists in critical systems

MASS-CASUALTY RISK
Simultaneous disruption of operations could endanger lives, cargo, and the environment

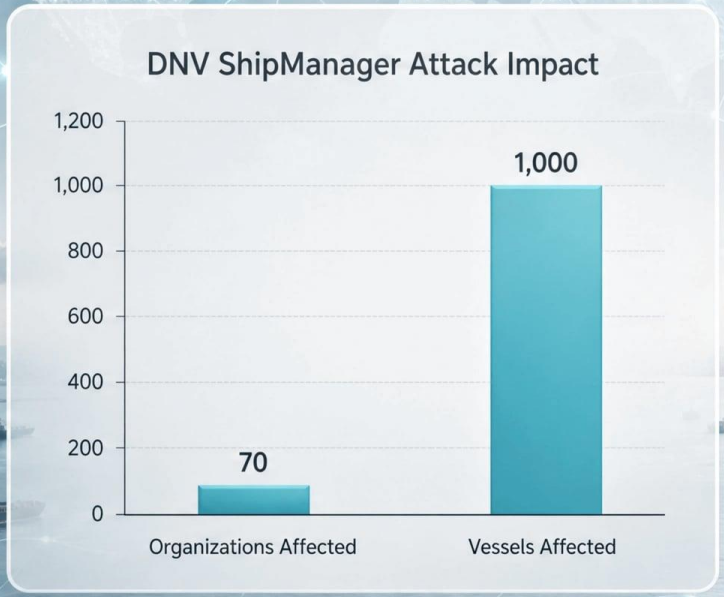
TRUST IS THE TARGET
Attackers don't break in—they build in. The supply chain is the new battleground.

THE QUESTION ISN'T IF—IT'S WHEN.
Resilience starts with securing the source.

THE NEW MASS-CASUALTY CYBER THREAT

Fleet-Scale Consequences from Single Operations

- **1. DNV SHIPMANAGER ATTACK (JAN 2023):** Ransomware struck DNV's ShipManager, affecting 70 organizations and ~1,000 vessels, rendering shore-side management "effectively blind."
- **2. LAB DOOKHTEGAN CAMPAIGN (2025):** Compromised a satellite communications provider, paralyzing ~180 vessels simultaneously by wiping VSAT modems.
- **3. BEYOND SINGLE VESSEL TARGETING:** Industry faces state actors or well-resourced criminals compromising shared infrastructure, imposing fleet-scale consequences.
- **4. REGULATORY LAG:** Existing frameworks and security planning assumptions are not designed to address this category of centralized cyber threat.



THE ATTACK ARCHITECTURE

How One Breach Becomes a Fleet Crisis

1. **SUPPLY CHAIN ATTACK MODEL:**
   Compromising one supplier (e.g., software platform, SATCOM provider) grants access to thousands of individual targets.

2. **SYSTEMIC TRUST:**
   Attackers exploit the trusted relationship between suppliers and customers, bypassing direct interaction with individual vessels.

3. **KEY MARITIME SUPPLIERS:**
   Fleet management platforms, satellite communications providers, ECDIS manufacturers, and OEM maintenance platforms are prime targets.

4. **ESCALATING IMPACT:**
   From collateral damage (NotPetya, 2017) to deliberate sabotage (Lab Dookhtegan, 2025), the model evolves to destructive operational control.

THE LAB DOOKHTEGAN CAMPAIGN

Operational Sabotage Through Provider-Level Infrastructure Compromise

1. TARGET: FANAVA GROUP: Iranian satellite and IT provider, a single point of systemic failure for NITC and IRISL fleets.

2. METHOD: INFRASTRUCTURE COMPROMISE: Attackers compromised Fanava's core infrastructure, not individual vessel terminals, gaining logical access to every ship.

3. EXPLOITED VULNERABILITIES: Weak credential management and outdated firmware in iDirect Falcon VSAT service (documented since 2014/2018).

4. DESTRUCTIVE OUTCOME: Wiped iDirect modems across the fleet, forcing manual reinstallation and maximizing downtime for 116 vessels in the first wave.

Information Provided by Trident Group America, Inc

GLOBAL IMPLICATIONS

The Attack Architecture is Not Context-Specific

ALLIED COMMERCIAL FLEETS: CIMSEC analysis warns that the attack model is applicable to any modern commercial fleet, regardless of flag or ownership.

SYSTEMIC TRUST MODEL: Centralized satellite provision, fleet management software, and OEM remote access define the vulnerability, not political context.

HIGH-IMPACT VECTORS: Attacks through software and communication service providers represent one of the highest-impact vectors for global maritime disruption.

SIMULTANEOUS DISTRIBUTION: Attackers can distribute malicious code simultaneously to tens of thousands of vessels worldwide via compromised OEM update servers.

THE PLATFORMS AT RISK

Systemic Concentration of Trust Creates Supply Chain Vulnerabilities

- **FLEET MANAGEMENT SOFTWARE:** Platforms like ShipManager run on centralized servers; compromise leads to simultaneous operational blindness for all users.
- **VSAT PROVIDERS:** More immediately dangerous; compromise severs critical communications for weather routing, cargo management, and situational awareness.
- **ECDIS & OEM MANUFACTURERS:** Update servers for electronic charts and engine control systems push critical corrections; compromise creates a 'safety vacuum'.
- **OPERATIONAL REALITY:** Vessels are dependent on these platforms for daily compliance, maintenance, and operational functions, making them prime attack surfaces.

Information Provided by Trident Group America, Inc

THE REGULATORY GAP

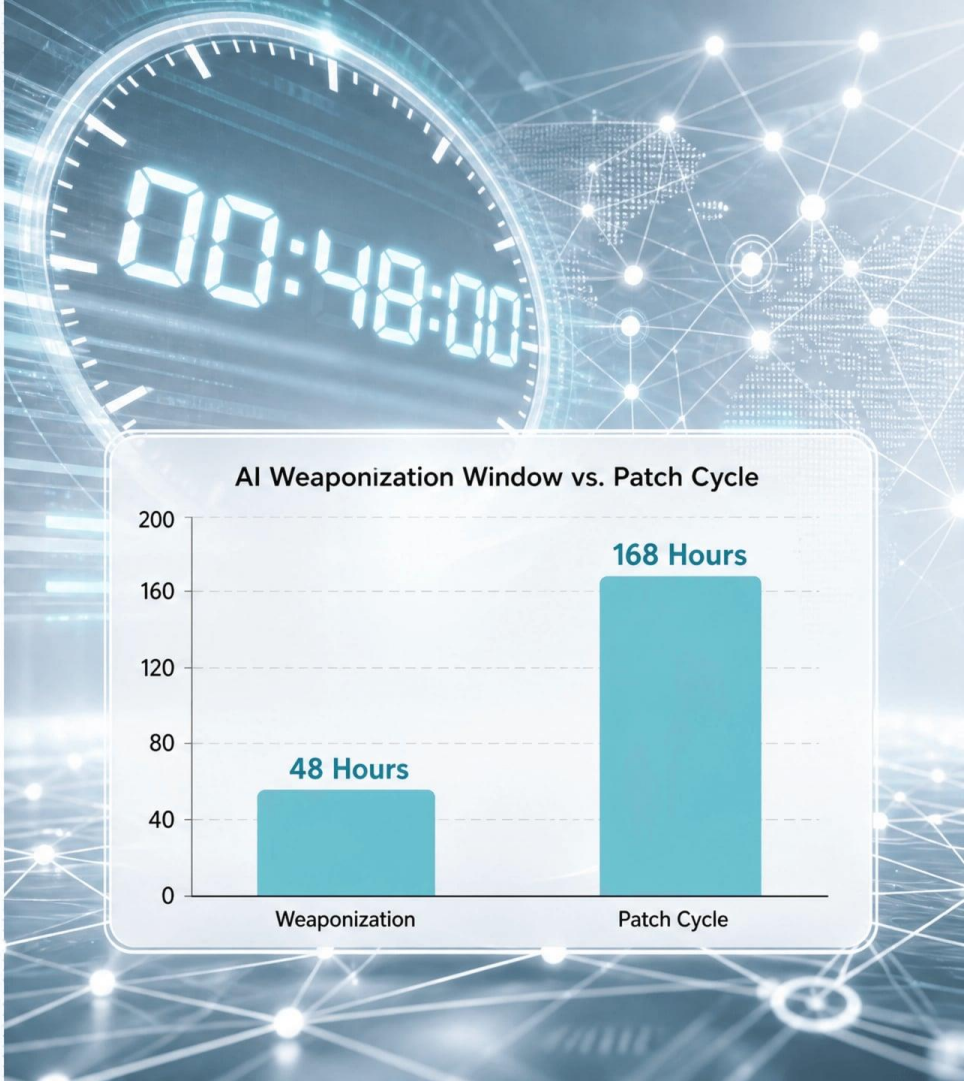
Compliance Without Comprehensive Supply Chain Risk Management

- **USCG CYBERSECURITY RULE (JULY 2025):** Requires incident reporting, CSO designation, and Cybersecurity Plans by July 2027 for U.S. maritime sector.
- **IACS UR E27:** Extends cyber resilience standards to OEM equipment for newbuilds after July 2024, addressing hardware supply chain at component level.
- **MISSING LINK:** Neither framework directly mandates third-party software vendor security vetting for fleet management, VSAT, or OEM platform relationships.
- **'OPERATOR DISCRETION':** The current framework leaves supply chain risk assessment to individual operators, creating a gap between compliance and genuine security.

THE AI-ACCELERATION DIMENSION

Adversaries Weaponize Vulnerabilities Faster Than Patches

- **48-HOUR WEAPONIZATION:** Adversaries can now exploit newly disclosed software vulnerabilities within 48 hours, a window shorter than most patch cycles.
- **TRADITIONAL MODEL OBSOLETE:** The traditional patch-and-monitor security model is no longer adequate for the threat tempo established by AI-enabled adversaries.
- **FLEET-WIDE EXPLOITATION:** A zero-day vulnerability in a fleet management platform can be exploited across every vessel it serves before a patch is developed.
- **NEW SECURITY IMPERATIVES:** Real-time monitoring of vendor infrastructure and incident response plans modeling 'vendor compromise' are now minimum requirements.



MARITIME SUPPLY CHAIN SECURITY POSTURE

Beyond the Vessel Boundary to the Full Ecosystem of Trust

COMPREHENSIVE INVENTORY: Mapping every software platform, communications provider, OEM remote access relationship, and third-party data service connected to vessel systems.

VENDOR SECURITY ASSESSMENT: Asking critical questions about architecture, access controls, incident response, audit trails, and third-party vetting of suppliers.

TECHNICAL INDICATORS OF SECURITY: Software composition analysis, Software Bill of Materials (SBOM) documentation, and verified multi-party code signing.

SHIFTED PERIMETER: Conceptualizing the security perimeter not at the vessel boundary, but across the entire ecosystem of trusted software and communications relationships.

Information Provided by Trident Group America, Inc

CONCLUSION: POISONED AT THE SOURCE

The Maritime Industry's Unaddressed Upstream Threat

- **INSUFFICIENT VESSEL-LEVEL SECURITY:** Hardened onboard systems and compliance are necessary but insufficient; the threat has moved upstream to the source.
- **VENDOR COMPROMISE:** Attackers compromise fleet management platforms, VSAT providers, or OEM firmware update servers to affect entire fleets simultaneously.
- **AI-ACCELERATED THREAT:** AI tools enable adversaries to weaponize vulnerabilities at a pace that individual operator security programs cannot match.
- **CLOSING THE GAP:** Requires treating every vendor relationship as a potential attack vector and recognizing that the most dangerous point of entry is the software the ship trusts.