BUILT-IN VULNERABILITY

The Hidden Cyber Risk Inside America's Port Cranes

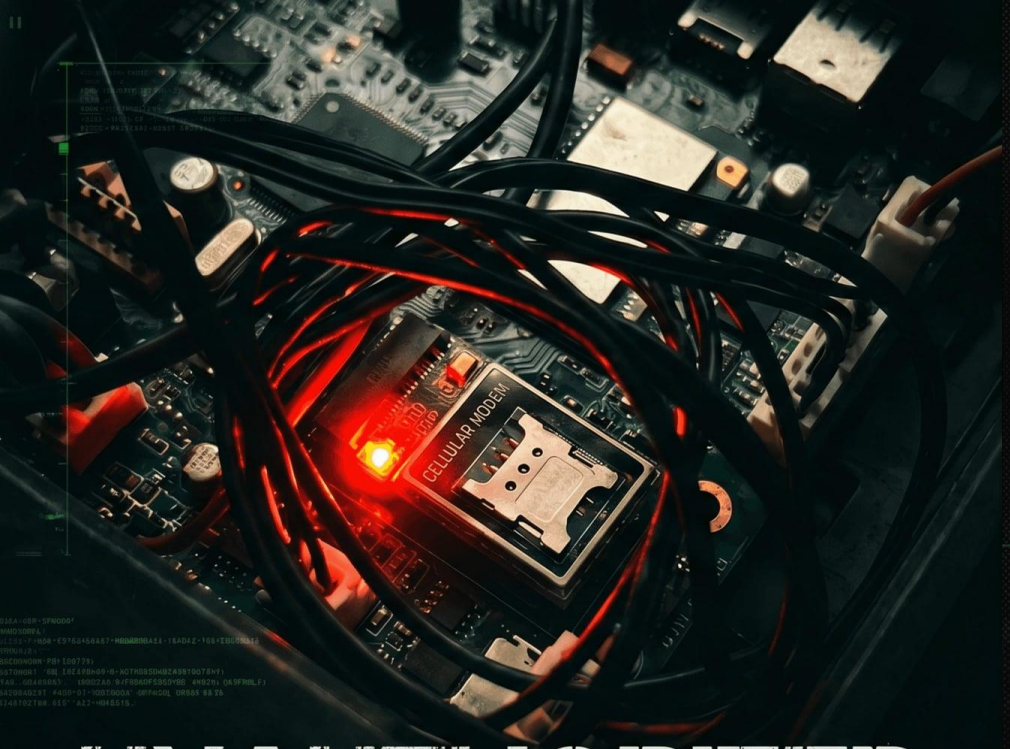
The Architecture of Dependence.

- ZPMC supplies **80%** of U.S. port cranes
- State-subsidized pricing undercuts Western competitors
- Over **200 cranes** integrated into critical infrastructure

Information Provided by Trident Group America, Inc

REMOTE ACCESS RISKS

- Cranes designed for remote control and programming.
- ZPMC engineers maintain persistent access.
- Chinese law mandates intelligence cooperation.



UNAUTHORIZED HARDWARE

THE MODEM DISCOVERY

- CONGRESSIONAL PROBE FOUND UNAUTHORIZED CELLULAR MODEMS ON ZPMC CRANES;
- DEVICES BYPASSED FIREWALL CONTROLS;
- PURPOSE: ‘OBSCURE METHOD’ FOR DATA COLLECTION AND DISRUPTION.

Information Provided by Trident Group America, Inc

SUPPLY CHAIN INFILTRATION

Critical components shipped to China for installation;
Parts stored in China for months;
Hardware-level manipulation risk.

Information Provided by Trident Group America, Inc

STRATEGIC CALCULUS

- Port disruption is a key element of Chinese military planning for a Pacific crisis.
- West Coast ports are vital for moving U.S. military personnel and equipment.
- Control over port data provides "privileged insight" into global commerce.

ECONOMIC CONSEQUENCES

- Port of Long Beach handles $200 billion in trade annually.
- Single day shutdown costs $2 billion to local economy.
- Simultaneous disruption would be catastrophic.

Information Provided by Trident Group America, Inc

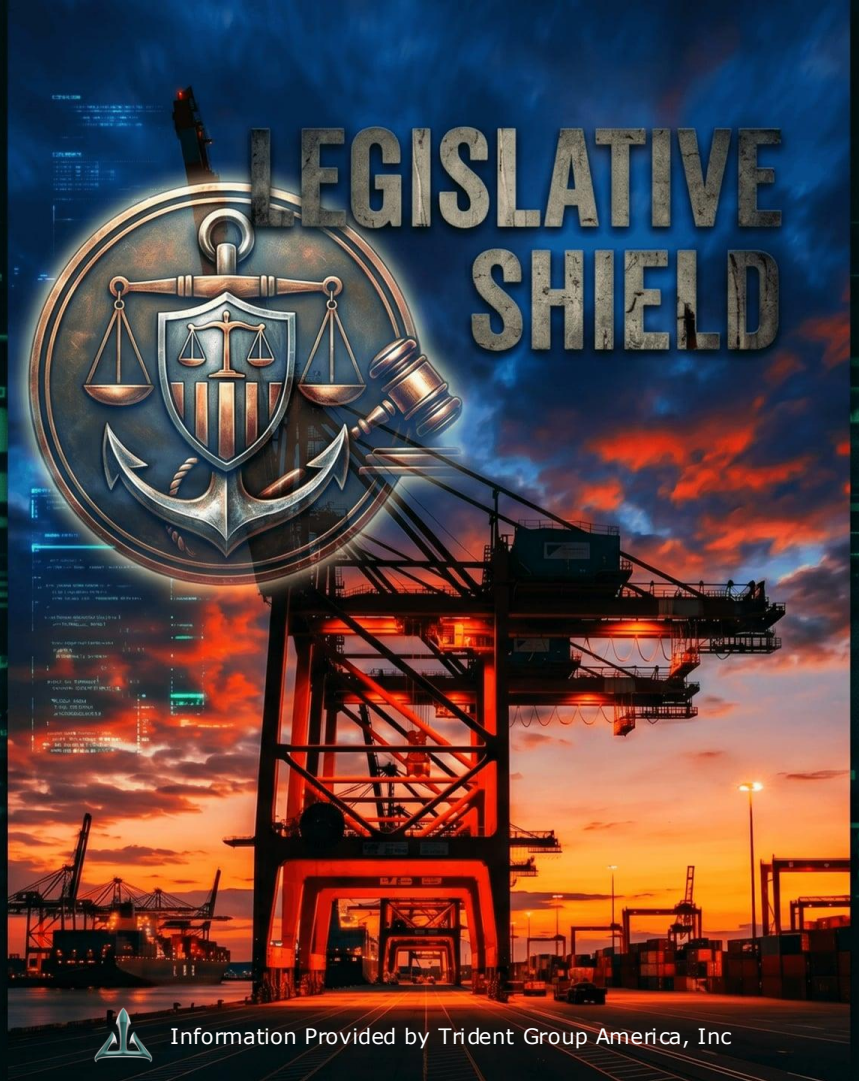
Information Provided by Trident Group America, Inc

DOMESTIC RECOVERY

$20 BILLION FEDERAL INVESTMENT

to restart domestic crane manufacturing

- PACECO Corp. (U.S. subsidiary of Mitsui) leading the onshoring effort
- First U.S.-made ship-to-shore cranes in over 30 years.



LEGISLATIVE SHIELD

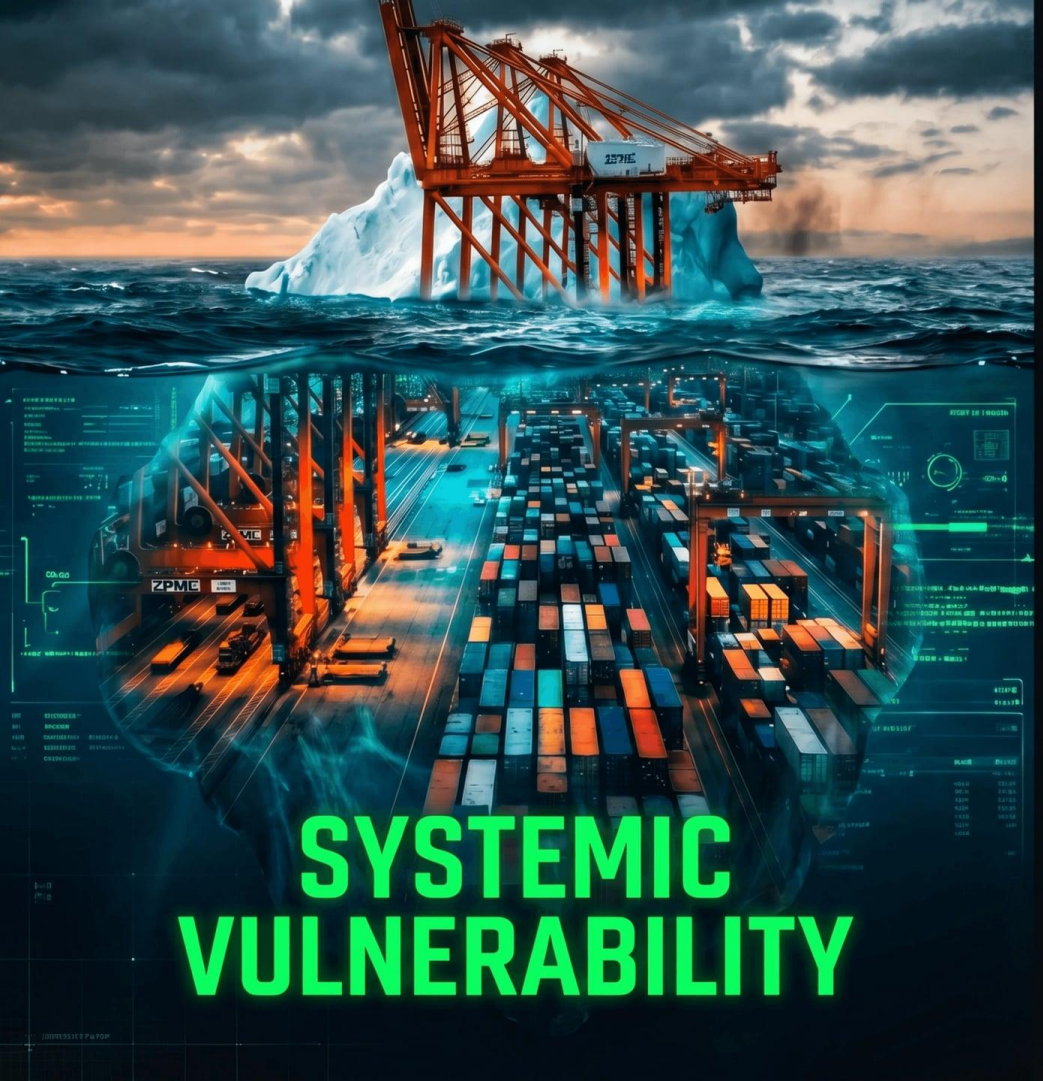
- Senate passed act to fund replacement of Chinese-made cranes.
- Grants available for ports to switch to U.S. or allied-nation equipment.
- Bipartisan recognition of the urgent national security threat.

Information Provided by Trident Group America, Inc

THE TIMELINE GAP

- Replacing 200+ cranes across 23 ports will take 10 to 15 years.
- Current USCG inspections have covered less than half of existing cranes.
- The risk remains “current and ongoing” for at least the next decade.

Information Provided by Trident Group America, Inc



SYSTEMIC VULNERABILITY

- Vulnerabilities extend to cargo scanners, logistics platforms, and sensors;
- Most ‘Western’ alternatives maintain deep PRC supply chain ties;
- Need for comprehensive maritime cybersecurity standards.

Information Provided by Trident Group America, Inc

VIGILANCE & RESILIENCE

- Hardware-based risks cannot be ‘patched’ like software
- Continuous monitoring and proactive defense are essential
- Trident Group: Your partner in maritime resilience

TRIDENT GROUP AMERICA

- Specialized Maritime Cyber Red Cell;
- Global Maritime Security Solutions & Asset Protection
- Professional Training & Security Operations
- Bridging the gap between policy and actual port security.