

HANDLING OUR CARGO: HOW THE PEOPLE'S REPUBLIC OF CHINA INVESTS STRATEGICALLY IN THE U.S. MARITIME INDUSTRY



THE SELECT
COMMITTEE
ON THE **CCP**

MARK E. GREEN, MD, CHAIRMAN | JOHN MOOLENAAR, CHAIRMAN |
CARLOS A. GIMENEZ, SUBCOMMITTEE CHAIRMAN



MAJORITY STAFF REPORT

September 2024

TABLE OF CONTENTS

Forward	4
Executive Summary	5
Key Findings	7
Recommendations	9
I. Background	11
A. PRC Efforts to Gain Economic Influence in the United States	11
B. PRC’s ZPMC Cranes Dominate U.S. Market	12
i. PRC Champion ZPMC	12
ii. PRC-Subsidized Steel	12
C. PRC Ownership of U.S. Ports.....	13
i. COSCO Shipping.....	14
ii. China Merchants Group.....	15
D. U.S. Policymaker Concerns with PRC Economic Influence.....	16
E. ZPMC Subcontracting of Crane Control Systems.....	17
F. Role of U.S. Federal Agencies in the Maritime Sector	17
G. Alternatives to ZPMC Cranes	18
II. The Committees’ Investigative Process	20
A. Scope of Investigation	20
B. Investigative Process	21
i. PRC Operational and Strategic Dynamics.....	21
ii. Software Integrity and Safety	21
iii. Engagement with Maritime Sector Stakeholders	22
III. Findings of the Investigation into ZPMC and ABB	23
A. ZPMC Poses a Risk to U.S. National Security	23
i. Mandatory Access for PRC Law Enforcement and Intelligence ...	27
ii. PRC Hides ZPMC Cybersecurity Vulnerabilities.....	28
iii. Hidden Cellular Modems on ZPMC Cranes.....	28
B. ABB’s Role in Port Infrastructure and National Security Risks Arising from Partnership with ZPMC	29
i. ABB Contracts with U.S. Government.....	30

ii. ABB’s Extensive Partnership with ZPMC	30
iii. ABB’s Ransomware and Unreported Cybersecurity Incidents	31
IV. Committee Investigation Engagement.....	32
A. ABB Engagement	32
B. TMEIC and Siemens Engagement	34
C. Crane Manufacturers Engagement.....	35
D. ZPMC Engagement.....	35
E. U.S. Ports Engagement.....	38
i. Port Authority and Terminal Operator Delineation	38
ii. Attempts to Mitigate Vulnerabilities Posed by ZPMC Cranes.....	39
V. Guam’s Strategic Significance and the Need for Enhanced Infrastructure Amid Rising Tensions in the Indo-Pacific	40
A. Guam’s Geopolitical Significance	40
B. Guam’s Critical Infrastructure Vulnerabilities	40
C. Disagreement Between Department of Transportation, MARAD, and Department of Defense on Guam’s Strategic Importance	41
Classified Annex.....	44

FORWARD

By Congressman Carlos A. Gimenez (R-FL)

During my time as Mayor of Miami-Dade County, I saw firsthand through interactions with Port Miami and other maritime stakeholders the range of threats posed to U.S. ports by foreign adversarial actors. Recognizing the gravity of these threats, I have continued to raise alarms about the U.S. maritime sector's increasing reliance on equipment and technology that has been manufactured, assembled, or installed by entities owned, controlled, subsidized, or influenced by Communist China. This equipment, which includes ship-to-shore cranes, could be exploited to malfunction or facilitate cyber espionage, compromising our maritime infrastructure and undermining U.S. national security.

As Chairman of the Transportation and Maritime Security Subcommittee, I spearheaded a joint investigation with my colleagues from the House Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. The goal was to identify cybersecurity risks, foreign intelligence threats, and supply chain vulnerabilities at U.S. ports. Through hearings, roundtable discussions, site visits to U.S. ports, and oversight letters transmitted to relevant stakeholders, we have all but confirmed that our nation's ports face significant threats from adversarial actors. The U.S. maritime sector's reliance on the People's Republic of China equipment and technology is the root cause of that insecurity.

We were alarmed to find that state-owned enterprises, including Shanghai Zhenhua Heavy Industry Co., Ltd., (ZPMC) have made concerted efforts to generate undue economic leverage over U.S. ports, while seeking to increase their influence through investments and non-competitive pricing for equipment and technology. In part due to the regime in Beijing's financial support, ZPMC dominates the global and U.S. maritime equipment and technology market. It accounts for nearly 80% of the ship-to-shore cranes used by U.S. ports.

These ship-to-shore cranes are critical to the U.S. maritime sector's ability to facilitate commercial activity, international trade, and military logistical operations during time of conflict. In a scenario where the functionality of these ship-to-shore cranes is compromised, particularly by a threat actor originating from Communist China, the disruption of commercial activity would reverberate across the U.S. In the event of a future conflict in the Indo-Pacific region, Communist China would undoubtedly seek to limit the U.S. military's response, by targeting or exploiting vulnerabilities in the very same U.S.-based maritime equipment and technology that they produced, manufactured, assembled, or installed.

I am proud to have led this joint investigation to further understand the security risks at our nation's ports. It is clear the threat exists, and our adversaries are looking for ways to undermine our national security. The United States must take steps to secure the equipment at our ports and cease dependence on international threat actors.

EXECUTIVE SUMMARY

In June 2023, the House Committee on Homeland Security (Homeland Security Committee) and the House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee) (Committees) launched a joint investigation into the cybersecurity risks, foreign intelligence threats, and supply chain vulnerabilities at U.S. ports. The investigation focused on the widespread use of foreign equipment and technology, specifically assessing the risks, threats, and vulnerabilities associated with ship-to-shore cranes (STS) and related components produced, manufactured, assembled, or installed by Shanghai Zhenhua Heavy Industry Co., Ltd. (ZPMC), a state-owned enterprise (SOE) controlled by the government of the People's Republic of China (PRC).

The U.S. maritime sector is dangerously reliant on equipment and technology that has been produced, manufactured, assembled, or installed in the PRC, including ship-to-shore cranes, container handling equipment, and various other critical maritime infrastructure components. This is due in large part to noncompetitive pricing that favors PRC SOEs, technological disparities, and the lack of domestic manufacturer alternatives. Contracts between PRC SOEs and U.S. ports do not adequately prioritize security in favor of the latter, and often lack provisions prohibiting unauthorized modifications or access to equipment by the former. The PRC's geopolitical ambitions, particularly regarding Taiwan, raise additional concerns about the security of U.S. maritime supply chains, as the PRC could potentially leverage its dominance to exert pressure on the United States.

The PRC, through its SOEs, has strategically positioned itself as a dominant force in the global maritime sector, aiming to control key components at ports worldwide including in the United States. Leveraging access to cheap labor and subsidized steel, PRC SOEs, particularly ZPMC, have sold STS cranes at non-competitive prices, capturing an overwhelming share of the global market. ZPMC is the world's largest STS crane manufacturer, producing nearly 80% of the STS cranes used at U.S. ports and holding 70% of the global market share. This dominance has been achieved through a complex system of state support, including financing from state banks, direct subsidies, preferential borrowing rates, state-backed fundraising, and other nonmarket advantages. Currently, there are no domestic manufacturing alternatives for STS cranes in the U.S., although at least two companies are considering establishing a manufacturing presence.

The investigation revealed that two PRC state-owned enterprises control portions of five U.S. ports and lead tens of billions of dollars in PRC overseas seaport investments. The Committees engaged directly with multiple U.S. ports designated by the U.S. Department of Defense (DoD) as Commercial Strategic Seaports, located at strategic positions on the West Coast, East Coast, Gulf Coast, and in the

Western Pacific. Alarming, many of these seaports use equipment and technology originating from the PRC. In most cases, these ports entered multimillion dollar contracts with ZPMC, granting it the contractual authority to produce, manufacture, assemble, or install the equipment and technology in the PRC and deliver it upon completion.

When questioned about the risks of using PRC-origin equipment, many Commercial Strategic Seaports claimed to mitigate risks by using critical internal STS crane components from Swiss (ABB), German (Siemens), or Japanese (TMEIC) manufacturers, rather than those produced by ZPMC. However, the Committees found this explanation problematic. Contracts reviewed by the Committees revealed that many agreements allowed critical internal components from third party contractors to be sent to the PRC for installation by ZPMC. For instance, ABB stores its internal components—that it markets to U.S. ports as a secure, Western alternative to ZPMC components—in the PRC for up to 18 months following shipment.

Most third-party components are sent to ZPMC’s “Changxing Base” on Shanghai’s Changxing Island, near the Jiangnan Shipyard, where the People’s Liberation Army Navy’s (PLAN) most advanced warships are built. This proximity is concerning, and the Committees were further troubled by the discovery of unauthorized cellular modems installed on STS cranes produced in the PRC and bound for U.S. ports. According to sensitive documents reviewed by the Committees, these cellular modems, not requested by U.S. ports or included in contracts, were intended for the collection of usage data on certain equipment. This constitutes a significant backdoor security vulnerability that undermines the integrity of port operations.

As the geopolitical landscape in the Indo-Pacific shifts rapidly and the PRC escalates tensions in the South China Sea and the Taiwan Strait, Guam’s strategic importance has increased. Despite this, there are growing concerns about Guam’s critical infrastructure—particularly its ports, airfields, and electric grid, which is vital for both military operations and civilian use. The investigation found that while the Port of Guam is listed as a Commercial Strategic Seaport by the Department of Defense (DoD) Military Surface Deployment and Distribution Command (SDCC), the U.S. Maritime Administration (MARAD) does not extend the same recognition, limiting Guam’s ability to receive resources comparable to other U.S. mainland Commercial Strategic Seaports.

Appropriately cleared parties can read additional analysis on file with the Committee on Homeland Security.

KEY FINDINGS

The Committees make the following factual findings:

- ZPMC, or a third-party company contracted with ZPMC, installed cellular modems onto STS cranes that are currently operational at certain U.S. ports. These installations fall outside the scope of any existing contract between the affected U.S. ports and ZPMC.
 - This incident is not isolated—in February 2021, the Federal Bureau of Investigation (FBI) discovered intelligence gathering equipment near or on ZPMC STS cranes on arrival to the Port of Baltimore.
- ZPMC has repeatedly requested remote access to its STS cranes operating at various U.S. ports, with a particular focus on those located on the West Coast. If granted, this access could potentially be extended to other PRC government entities, posing a significant risk due to the PRC’s national security laws that mandate cooperation with state intelligence agencies.
- By design of contract, and often at the request of ZPMC, all non-ZPMC operational STS crane components are shipped to the PRC by third party companies—particularly from Sweden, Germany, and Japan. These components are then installed by ZPMC engineers without oversight from the original manufacturer, raising significant concerns about the integrity and security of the final assembled crane.
- The U.S. maritime sector is dangerously reliant on equipment and technology produced, manufactured, assembled, or installed in the PRC. This includes ship-to-shore cranes, container handling equipment, and various other critical maritime infrastructure components. This dependency is largely driven by noncompetitive pricing that favors PRC SOE’s, technological disparities, and the lack of viable domestic manufacturer alternatives.
- The contracting practices between PRC SOE’s and U.S. ports, as well as other maritime stakeholders, fail to adequately prioritize security. During the Committees’ investigation, we reviewed multiple contracts between ZPMC and U.S. ports and were alarmed to find no provisions prohibiting or limiting unauthorized modifications or access to equipment and technology bound for U.S. ports. Consequently, ZPMC and other PRC SOE’s are not contractually barred from installing backdoors into equipment or modifying technology in ways that could allow unauthorized access or remote control, enabling them to compromise sensitive data or disrupt operations within the U.S. maritime sector at a later time.
- Most, if not all, global crane manufacturing companies that serve as alternatives to ZPMC maintain ties to the PRC. These companies are either

directly vulnerable to supply-chain disruptions or indirectly susceptible to PRC pressure due to their business dealings within PRC.

- The PRC's geopolitical ambitions and assertiveness, particularly regarding Taiwan, raise concerns about the security of U.S. maritime supply chains. The Committees' investigation found that in a potential future dispute with the United States over Taiwan, the PRC could restrict or manipulate the supply of critical components or materials essential to U.S. maritime infrastructure, including STS cranes. Such actions could severely disrupt U.S. commercial activities and hinder the DoD's ability to deploy supplies and resources to the Indo-Pacific region.
- In recent years, U.S. federal agencies, including the FBI, have alerted U.S. ports and industry partners about the PRC's efforts to establish a strategic presence at certain U.S. ports. On February 1, 2023, the FBI's Office of the Private Sector issued an advisory highlighting indicators of malicious PRC-activity relating to the U.S. maritime sector. The advisory warned U.S. ports and industry partners to be vigilant for specific PRC activity, including, but not limited to:
 - Unusual visits, investments, expansions, renovations, joint ownership, or acquisition of port/maritime infrastructure by PRC government entities and SOEs at strategic U.S. ports;
 - Increased marketing or selling of PRC SOE equipment to U.S. ports that could be remotely disrupted or used to gather information benefiting PRC national security;
 - Unusually low quotes or bids for U.S. maritime equipment or services from PRC SOE's or their affiliates; and
 - Increased outreach from Chinese entities regarding the operations of U.S. ports, particularly their ships, cranes, docks, telecommunications, data, offices, employees, security, and intermodal connections with rail and highway transportation.
- The Committees found that due to inadequate management by the port authority, MARAD, and DoD, Guam struggles to consistently receive grant funding, achieve strategic port status, maintain or enhance its cyber security posture, and avoid the risks associated with installing PRC-made equipment at its port.

RECOMMENDATIONS

Securing U.S. ports and the cranes they rely on will require a comprehensive approach involving short-term, medium-term, and long-term strategies. The Committees therefore recommend:

Short-term:

- The Department of Homeland Security (DHS), through the U.S. Coast Guard, should immediately issue guidance to all U.S. ports to disassemble any connections of ZPMC cranes to cellular modems or any other method of connection to ZPMC, absent an existing contractual obligation.
- DHS, through the Cybersecurity and Infrastructure Security Agency (CISA) and the Coast Guard, should immediately issue guidance to all U.S. ports using ZPMC cranes to install operational technology monitoring software.
- DHS, through CISA and the Coast Guard, should immediately prioritize closing cybersecurity gaps at Guam's port, issuing guidance, and sending experts to provide resources to the port.
- DHS, through CISA and the Coast Guard, and in close coordination with DoD and the Department of Transportation, should take steps to ensure the safety and security of DoD-designated Commercial Strategic Seaports.

Medium-term:

- Congress should pass legislation authorizing U.S. ports to automatically receive waivers from Buy America requirements for purchasing port cranes from non-adversarial countries, using federal grant dollars.
- DHS, through CISA and the Coast Guard, should issue guidance for trusted vendors regarding port cranes, carefully defining the components and subcontracting practices.
- DHS, through the Coast Guard, should commission a report to evaluate the viability of purchasing STS cranes through companies in non-adversarial countries.
- DHS, through the Supply Chain Resilience Center, should commission a report to study the consequences of ZPMC ending contractual support for parts or services to U.S. ports – especially examining the impacts to the U.S. economy.

- DHS, through the Federal Emergency Management Agency (FEMA), should issue guidance for port grants that enable U.S. ports to offset the cost of purchasing STS cranes from non-adversarial countries.

Long-term:

- The U.S. Department of Commerce, in conjunction with appropriate agencies, should commission a study on building a U.S. crane manufacturing base, including the development of the necessary expertise and market consumption.
- The Department of Commerce, in conjunction with appropriate agencies, should commission analysis for U.S. manufacturing competitiveness globally—including port construction and shipbuilding.

I. BACKGROUND

This report details the findings from a joint investigation of the House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party and the Committee on Homeland Security into the nation's critical maritime infrastructure, and threats posed to it by the PRC. It exposes how the PRC has embedded itself into a critical component of the U.S. economy by dominating global market share of port cranes through investment campaigns backed by SOEs. It outlines the potential cybersecurity and national security vulnerabilities posed by PRC control of port cranes, for both the United States and its allies. Finally, the report outlines collaborative strategies for how the United States and its international partners and allies can address the risks posed by the PRC's maritime activities and promote a more secure and fair global maritime infrastructure.

Over the course of the year, the Committees have held hearings, worked closely with executive branch partners, consulted with experts, and traveled domestically and internationally to fully understand the threats posed by the PRC to America's maritime critical infrastructure.

By providing this detailed analysis, the Select Committee and Homeland Committee aim to inform policymakers, industry stakeholders, and the public about the challenges posed by the strategic competition with the PRC in the maritime sector. The goal is to shed light on the PRC's strategy for control of the maritime sector and infrastructure and the implications for U.S. national and economic security. Finally, this report aims to support the development of effective strategies to safeguard U.S. national security interests and those of our allies and partners in the face of evolving maritime threats.

A. PRC Efforts to Gain Economic Influence in the United States

The PRC has strategically positioned itself as a significant player in the global economy, with its sights firmly set on expanding its economic influence within the United States. Through a calculated blend of investments in ports and manufacturing sectors, the PRC has embarked on a journey to not only bolster its economic prowess but also to secure a foothold in critical U.S. infrastructure and industries.¹ This endeavor, part of the PRC's ambitious "Going Out" policy, underscores a deliberate move to extend its reach beyond its borders, marking a pivotal shift in international economic dynamics.²

In the intricate dance of global trade and economics, ports serve as a lifeblood of commerce, and the PRC's interest in these assets is far from coincidental. By acquiring stakes in key U.S. ports, such as the notable investment by China COSCO Shipping Corporation Limited (COSCO Shipping) in the Port of Los

"[P]orts serve as the lifeblood of commerce, and the PRC's interest in these assets is far from coincidental."

Angeles' container terminal, China has cleverly positioned itself at the heart of America's trade ecosystem.³ As a state-owned enterprise, COSCO Shipping has direct ties to the PRC and has reportedly modified its civilian ferries for use as amphibious operations—potentially for use in a future Taiwan invasion.⁴

B. PRC's ZPMC Cranes Dominate U.S. Market

Chinese SOEs have used their access to cheap labor and subsidized steel to sell their STS cranes cheaply and dominate the global market.⁵ STS cranes are essential for loading and unloading cargo from container ships at ports.

China's SOEs have gained a dominant position in the global market for port cranes through a complex and opaque system of formal and informal state support, including financing from state banks, direct subsidies, preferential borrowing rates, state-backed fundraising, and other nonmarket advantages.⁶ This strategy found its place after the 2008 financial crisis, which set ambitious domestic and global targets for shipbuilding and shipping finance, resulting in the consolidation of larger and more competitive firms within the PRC.⁷

“Chinese [state-owned enterprises] have used their access to cheap labor and subsidized steel to ... dominate the global market.”

i. PRC Champion ZPMC

ZPMC, a Chinese SOE, is the world's largest STS manufacturer, producing nearly 80% of the cranes used in U.S. ports and dominating 70% of the global market share.⁸ One of the factors that enables ZPMC to sell its cranes cheaply is its access to cheap labor. China has a large pool of low-cost workers, especially in the coastal regions where most of its crane production is located.⁹ ZPMC employs more than 30,000 workers,¹⁰ many of whom likely work long hours for low wages and in poor safety conditions.¹¹ ZPMC also benefits from economies of scale and the vertical integration of its production chain, which reduces its costs and increases its efficiency.¹²

ii. PRC-Subsidized Steel

Another factor that gives ZPMC a competitive edge is its access to subsidized steel. Steel is the main raw material for crane production,¹³ and China is the world's largest steel producer and exporter.¹⁴ China's steel industry is heavily subsidized by the government, which provides cheap loans, tax breaks, land grants, and other forms of support to its steel SOEs.¹⁵ These subsidies lower the production costs and the market prices of Chinese steel, making it cheaper and more attractive for ZPMC and other crane manufacturers to use.

“ZPMC produc[es] nearly 80% of the cranes used in U.S. ports and [controls] 70% of the global market share.”

By using cheap labor, subsidized steel, and the combined resources of SOEs, ZPMC can offer its cranes at significantly lower prices than its competitors, while still maintaining high quality and performance. This allows ZPMC to capture a large share of the global crane market and expand its presence in strategic seaports around the world, including some used by the U.S. military.¹⁶

“By using cheap labor, subsidized steel, and the combined resources of [Chinese state-owned enterprises], ZPMC can offer its cranes at lower prices than its competitors.”

C. PRC Ownership of U.S. Ports

Two PRC SOEs – COSCO and China Merchants Group (CMG) – control parts of the Ports of Long Beach, Seattle, Los Angeles, Houston, and Miami. More broadly, COSCO and CMG have spearheaded approximately \$30 billion in PRC overseas port investments in at least 46 countries.¹⁷ These ports are operated through joint ventures between PRC state-owned enterprises and Western companies.^{18,19}

- The Port of Long Beach: Pacific Maritime Services (PMS) is a joint venture between COSCO and Stevedoring Services of America (SSA) to operate the Pacific Container Terminal at Pier J. COSCO is the majority shareholder but does not have an effective majority due to voting requirements.
- The Port of Seattle: Two COSCO subsidiaries collectively have held a 33.33% stake in a joint venture since 2007. COSCO’s role is primarily to drive cargo traffic through the terminal.
- The Port of Los Angeles: China Shipping Group (merged with COSCO) entered a joint venture with Yang Ming, owning 40% of the operation. The terminal is known for its significant cargo volumes and environmental mitigation measures.
- Port of Houston and Port of Miami: China Merchants Port (CMPort) holds a minority stake in Terminal Link, a terminal-operating subsidiary of the French firm Compagnie Maritime d’Affrètement (CMA) and Compagnie Générale Maritime (CGM), which operates terminals at these ports. CMPort’s involvement is as an equity investor without direct operational control.

Joint ventures linked to COSCO and CMG at five American ports are concerning given COSCO’s ties to the People’s Liberation Army (PLA).²⁰

i. COSCO Shipping

China COSCO Shipping Corporation Limited is a Shanghai-based company focused on marine transportation services. COSCO Shipping is a state-owned enterprise established and controlled by the PRC government.²¹ They own many subsidiaries, including COSCO Shipping (North America) Inc., which owns COSCO Shipping Terminals (North America). The PLA has conducted numerous military-transportation and port-embarkation training exercises using ships and ferries operated by COSCO Shipping Ferry Company.²² Since 2020, four civilian ferries have had their stern ramps modified to allow amphibious combat vehicles to board and disembark.²³ Although COSCO ports are used for civilian purposes, PLA officials have publicly stated their dual-use applications. In 2013, Colonel Cao Weidong of China's Naval Academy of Military Research said, "COSCO has numerous supply points that provide daily services for civilian vessels. When Chinese naval warships are in the area, they can likewise enter the port for replenishment."²⁴

"The [People's Liberation Army] has conducted numerous military... training exercises using ships and ferries operated by COSCO Shipping Ferry Company."

Additionally, COSCO maintains close relationships with the PLA and the PRC's defense industry. Central Military Commission Chairman Xi Jinping visited COSCO's Yangpu International Container Terminal in Hainan Province and the Port of Piraeus in Athens, Greece, and Premier Li Keqiang sent COSCO Greece a congratulatory letter noting, "it acts as a role model for China-Greece cooperation, and has great importance for promoting the friendship and development of the two countries."²⁵ The PRC Ministry of Foreign Affairs and COSCO Shipping Group have participated in working dialogues focused on international cooperation and connectivity.²⁶

In September 2019, the Treasury Department sanctioned COSCO Shipping Tanker (Dalian) Co. Ltd. – a COSCO Shipping subsidiary – for transporting Iranian oil in violation of United States and United Nation sanctions. The U.S. Department of State found that Dalian knowingly engaged in a significant transaction for the transport of oil from Iran, including knowledge of sanctionable conduct, contrary to U.S. sanctions.²⁷ The sanctions were lifted in January 2020, but nonetheless show COSCO's willingness to disregard U.S. rules and norms.

The Port of Long Beach offers an interesting case study. In 2012, the Hong Kong-based Orient Overseas Container Line (OOCL) agreed to lease a terminal at the Port of Long Beach for \$4.6 billion over 40 years. Five years later, in July 2017, the Chinese state-owned COSCO announced that it would acquire OOCL for \$6.3 billion. This announced acquisition raised concerns within the U.S. government

"COSCO maintains close relationships with the PLA and the PRC's defense industry."

that a PRC state-owned conglomerate would control one of America’s largest ports. In response, DHS and the U.S. Department of Justice (DOJ) reached an agreement with OOCL and COSCO that the OOCL-owned terminals in Long Beach would be sold to a “suitable, unrelated third party” deemed “acceptable,” to the U.S. government. In 2019, after review from the Committee on Foreign Investment in the United States (CFIUS), OOCL announced that the Long Beach Container Terminal (Pier E) was sold to a Macquarie Infrastructure Partners-led consortium for \$1.78 billion.

ii. China Merchants Group

China Merchants Group is a Hong Kong-based company providing freight, logistics, and transportation services. CMG owns 12 subsidiaries including China Merchants Port Holdings, which manages more than 40 ports in 25 countries. CMG is a major participant in, and proponent of the Belt and Road Initiative.²⁸ CMG controls Sri Lanka’s Port Hambantota and Djibouti’s Doraleh Multipurpose Port, both of which are of strategic significance to the PRC.²⁹ Initially presented as a civilian complex, Djibouti’s Doraleh Multipurpose Port was later expanded to include a naval base.³⁰ China now has 2,000 troops permanently stationed at this base, which also features a pier capable of accommodating an aircraft carrier. This dual-purpose facility exemplifies the connections between commercial infrastructure and military capabilities.³¹

“CMG is a major participant in ... the Belt and Road Initiative.”

Both ports have been mired in controversy. In July 2017, CMG sent \$1.5 billion to a debt-stricken Sri Lankan government in return for an 80% stake in the Hambantota Port. Despite Sri Lankan officials pledging the port would not be used for military purposes, a PRC military survey ship – Yuan Wang 5 – docked at the port for a week in August 2022.^{32,33} Separately, the London Court of International Arbitration ruled in 2020 that the Djibouti government handed control of the Doraleh Port to CMG, violating its contract with DP World – the Dubai-based port operator

“CMG controls Djibouti’s Doraleh Multipurpose Port, ... [i]nitially presented as a civilian complex, [the port was] later expanded to include a [PRC] naval base.”

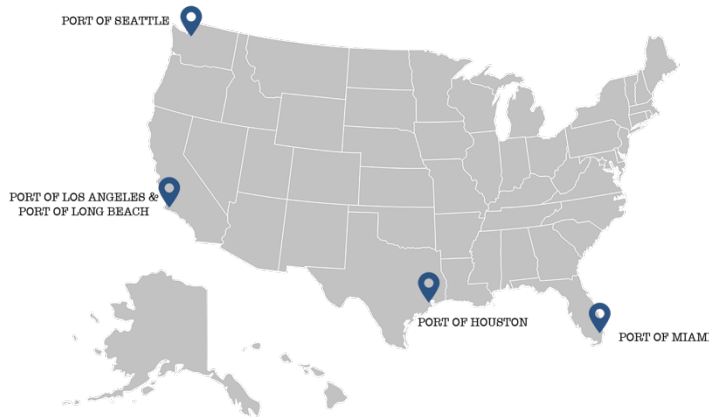
that previously operated the port. DP World’s ongoing lawsuits allege that CMG went as far as pressuring Djibouti’s government to expel DP World from Djibouti.³⁴

CMG’s ties to the PRC are also found in its senior leadership. CMG’s managing director, Miao Jianmin, was an alternate member of the 19th Central Committee.³⁵ Similarly, Duan Xianghai, a CMG board member in charge of CMG’s part-building activities, previously served as a director of the Supreme People’s Procuratorate, the PRC agency overseeing legal prosecutions and investigations.

CMG's ownership of the ports of Houston and Miami are managed through Terminal Link, a joint venture established in 2001 between CGM and CMA GGM, the France-based shipping company. CMG holds a 49% stake in Terminal Link, which it acquired in a May 2013 agreement.³⁶

- Port of Houston: Terminal Link, a joint venture between CMA CGM and China Merchants Port, operates the Port of Houston Bayport container terminal.
- Port of Miami: Terminal Link, a joint venture between CMA CGM and China Merchants Port, operates the South Florida Container Terminal at Miami

Figure 1 – PRC Ownership of U.S. Ports



D. U.S. Policymaker Concerns with PRC Economic Influence

U.S. policymakers have implemented various measures to push back against China's economic influence. Throughout many sectors, these efforts have found success. Since 2017, PRC investment and manufacturing dominance in the United States has dropped precipitously to only a fraction of its 2016 levels.³⁷ Federal policymakers have also pursued multilateral responses to China's economic coercion. The G7, which accounts for more than half the global economy, has been urged to publicly unite to denounce China's actions and retaliate economically in a coordinated manner against China.³⁸ There has been a shift in U.S. government awareness and policy towards a more secure economic policy, leading to the investment in coordination efforts, such as those managed by DHS' Supply Chain Resilience Center.³⁹

White House attention to the issue has also increased. The Biden administration promised in February 2024 to provide \$20 billion to strengthen maritime infrastructure cybersecurity, specifically with the goal of addressing software and hardware vulnerabilities in ZPMC cranes. The Biden administration also announced plans to phase out Chinese-made port equipment and fully return crane making to the United States to deal with 200 Chinese-made cranes⁴⁰ at U.S. ports

and facilities.⁴¹ This bipartisan chorus of concern regarding PRC economic influence—especially regarding transportation infrastructure—highlights the level of concern that this issue has reached within the American policymaking community.

E. ZPMC Subcontracting of Crane Control Systems

While ZPMC makes its own internal crane components, the company relies heavily on third-party companies such as ABB⁴²—a Swedish company—and TMEIC⁴³—a Japanese company—and Siemens⁴⁴—a German company—to build the internal systems for the majority of U.S. cranes. These internal components include programmable logic controllers, control systems, crane guidance systems, and other electronic systems—essentially the “brain” of the crane. These companies help ZPMC maintain its market share in the United States and globally by leveraging these companies’ expertise and specialization, global networks, customer confidence, and strategic cooperation.

“[B]y using ABB, TMEIC, and Siemens to make the internal components, ZPMC seeks to provide U.S. ports and terminal operators with the false assurance that they are a more secure option.”

However, by using ABB, TMEIC, and Siemens to make the internal components, ZPMC seeks to provide U.S. ports and terminal operators with the false assurance that they are a more secure option than ZPMC internal components since they are not Chinese companies. ZPMC appears to use these companies’ cooperation as a buffer from policymaker scrutiny and concerns. The investigation found that these companies allow for long periods of time outside of operational control in China highlighting the continued vulnerability of companies that work with the PRC.⁴⁵

In the United States, ABB and TMEIC are the primary providers of control systems for STS cranes. In recent years, Siemens has played a very small part in the industry at U.S. ports. For all these companies, STS port cranes represent a very small percentage of their manufacturing and engineering capabilities.

“The investigation found that [ABB, TMEIC, & Siemens] allow for long periods of time outside of operational control in China highlighting the continued vulnerability of companies that work with the PRC.”

F. Role of U.S. Federal Agencies in the Maritime Sector

The U.S. Coast Guard is responsible for enforcing maritime security regulations, conducting port security assessments, and ensuring compliance with the International Ship and Port Facility Security Code.⁴⁶ The Coast Guard also provides law and maritime safety enforcement, marine and environmental protection, and military naval support. The Coast Guard administers facility security plans and

safeguards fisheries and marine protected resources by enforcing living natural resource authorities.

The maritime sector is a crucial component of the United States' transportation system. Several federal agencies have jurisdiction over maritime sector security. The Office of Maritime Security (MAR-420), which is part of MARAD, is responsible for developing and implementing effective maritime security policies, procedures, practices, statutes, and training to protect U.S. citizens and maritime interests from security threats such as piracy, terrorism, and cyberattacks.⁴⁷

The Department's CISA is actively involved in maritime sector security. In March 2023, CISA and the U.S. Army Corps of Engineers, Engineer Research and Development Center, released the co-developed Marine Transportation System Resilience Assessment Guide (MTS Guide) for use by federal agencies, local governments, and industry decisionmakers that manage risk and enhance resilience to critical infrastructure systems and functions through conducting resilience assessments.⁴⁸

The FBI is responsible for investigating maritime security threats and incidents.⁴⁹ The FBI works closely with international and interagency partners to facilitate maritime security information-sharing with maritime industry stakeholders. U.S. Maritime Alerts and U.S. Maritime Advisories have been established through a U.S. government - U.S. maritime industry partnership to communicate information on threats in the maritime domain to maritime industry stakeholders and mariners.

The DoD is responsible for providing military support to civilian authorities in the event of a maritime security threat. The DoD, through United States Transportation Command (TRANSCOM) and its component commands, has a fleet of commercially viable, militarily useful merchant ships active in international trade available to support DoD sustainment sealift requirements during times of conflict or in other national emergencies.⁵⁰ Six DoD equities – TRANSCOM, United States Northern Command (NORTHCOM), Military Sealift Command (MSC), U.S. Army Forces Command (FORSCOM), Surface Deployment and Distribution Command (SDDC), and the Army Corps of Engineers – manage the National Port Readiness Network jointly with MARAD, the Coast Guard, and the Transportation Security Administration (TSA). The National Port Readiness Network facilitates the readiness of commercial ports in the United States for use by the military during national defense emergencies.⁵¹

G. Alternatives to ZPMC Cranes

Within the United States, there are currently no manufacturing alternatives for STS cranes, though at least two companies are considering or actively pursuing establishing a manufacturing presence in the United States. The Biden administration identified PACECO/Mitsui E&S Co—a company from Japan—to onshore its manufacturing capabilities so that it can produce STS cranes in the United States.⁵²

Additionally, the Committees were made aware that Kiewit, a U.S. company based out of Omaha, Nebraska, is considering entering the STS crane market. Konecranes—a Finnish company—and Liebherr—a German company—currently sell STS cranes, though they are more expensive than ZPMC. Within the PRC itself, there are several other STS crane manufacturers, such as Xuzhou Heavy Machinery (XCMG), Zoomlion, and Sany.⁵³ These PRC-based manufacturers obviously present a similar security concern as ZPMC and would not serve as a viable alternative.

II. THE COMMITTEES' INVESTIGATIVE PROCESS

A. Scope of Investigation

To inform the legislative process—including legislation designed to harden and secure the U.S. maritime industry—the Committees conducted oversight of both public and private shareholders. Over the last eight months, the Committees met with, received documents and information from, and questioned—both in-person and virtually—the following key stakeholders in the U.S. maritime industry:

- Department of Homeland Security
- Department of Transportation Maritime Administration (TMA)
- Department of Defense
- Coast Guard
- Department of the Navy
- United States Indo-Pacific Command
- United States Southern Command
- United States Cyber Command
- Federal Bureau of Investigation
- Cybersecurity and Infrastructure Security Agency
- National Security Agency (NSA)
- National Oceanic and Atmospheric Administration (NOAA)
- Sandia National Laboratories
- 10 U.S. Commercial Strategic Seaports
- 3 international port equipment manufacturers
- Other relevant government agencies and industry stakeholders

In March 2023, Select Committee Chairman Mike Gallagher and Rep. Carlos Gimenez—Chairman of the Homeland Committee's Transportation and Maritime Security Subcommittee—visited the Port of Miami to learn about the security of critical infrastructure and the pervasive threat of PRC-linked technology in port infrastructure. Additionally, Chairmen Gallagher and Gimenez visited the United States Southern Command headquarters to learn about PRC influence in the Western hemisphere. In June 2023, staff from both Committees visited the Port of New York and New Jersey to learn about the cybersecurity risks related to PRC-linked port infrastructure and ZPMC's presence at the port.

Under House Rule X, the Homeland Committee's jurisdiction includes "Overall homeland security policy" and "Functions of the Department of Homeland Security" regarding:

- A. Border and port security (except immigration policy and non-border enforcement)
- B. Customs (except customs revenue)
- C. Integration, analysis, and dissemination of homeland security information
- D. Domestic preparedness for and collective response to terrorism

- E. Research and development
- F. Transportation Security
- G. Cybersecurity

The Select Committee has broad authority to “investigate and submit policy recommendations on the status of the Chinese Communist Party’s economic, technological, and security progress and its competition with the United States” under H. Res. 11.

B. Investigative Process

In June 2023, the Committees launched their investigation. The Committees focused their investigative work on the PRC’s stake and influence within the operations of U.S. port facilities, seeking to understand the nature of their involvement, and on identifying and quantifying possible digital threats at U.S. maritime entry points.

i. PRC Operational and Strategic Dynamics

Equally pivotal is the understanding of the operational and strategic dynamics of ports under significant PRC influence abroad, offering insights into the global reach of China’s maritime strategies. The Committees are incredibly attentive to concerns surrounding proprietary technology theft, particularly in relation to container-scanning devices, a critical component of maritime security infrastructure. This aspect of the investigation aimed to unravel the complex web of relationships and contributions of PRC-based firms to the U.S. port equipment ecosystem, highlighting dependencies and potential vulnerabilities.

ii. Software Integrity and Safety

Another crucial area of focus is assessing the safety and integrity of software with PRC origins employed at U.S. maritime facilities. This encompasses thoroughly evaluating digital infrastructures and systems, and recognizing the potential risks embedded within software solutions integral to maritime operations. The Committees’ approach to this investigation was multi-dimensional, involving collaborative data sourcing from a diverse range of stakeholders, including domestic agencies, maritime bodies, industry experts, and allied nations. This comprehensive collection of data encompassed operational metrics, financial trails, technology blueprints, and transactional data.

Digital security formed a cornerstone of this investigation, with cybersecurity specialists playing a crucial role in identifying and addressing potential vulnerabilities. Moreover, establishing communication channels with international maritime entities has been instrumental in gaining shared intelligence on the PRC’s naval endeavors outside its borders. This collaborative approach not only enhances the depth of the investigation but also fosters a more comprehensive understanding of the global maritime landscape influenced by the PRC.

iii. Engagement with Maritime Sector Stakeholders

Additionally, the Committees engaged directly with key players in the maritime sector, including port administrators, logistics specialists, and technology vendors, to garner a ground-level perspective of the current landscape. This engagement was complemented by the dispatch of evaluation teams to primary U.S. maritime points to directly appraise PRC equipment and infrastructure components, providing an on-the-ground assessment of the situation.

Through this detailed and thorough examination, the Committees aimed to develop a nuanced understanding of the PRC's involvement in the U.S. maritime sector and to formulate effective strategies to mitigate any associated risks, ensuring the security and integrity of the nation's critical maritime infrastructure.

III. FINDINGS OF THE INVESTIGATION INTO ZPMC AND ABB

A. ZPMC Poses a Risk to U.S. National Security

The Committees' investigation into ZPMC has revealed significant national security concerns due to its deep ties with the Chinese military and state-controlled entities. As a wholly owned subsidiary of China Communications Construction Group (CCCC), ZPMC has transitioned from a maritime heavy-machinery manufacturer to a dominant player in the port-container sector. The company's board includes senior members of the Chinese Communist Party (CCP) and individuals with roles in defense contracting, highlighting its strategic alignment with Beijing's ambitions. ZPMC's operations have included collaboration with the People's Liberation Army Ground Force (PLAGF) and other military entities, and it has entered into agreements with sanctioned entities involved in human rights abuses. The company's partnerships with tech firms, such as Microsoft, to develop real-time port activity monitoring tools, further intensify national security concerns. Additionally, ZPMC's role in the Belt and Road Initiative and the development of "Smart Cities" underscores its strategic importance in advancing China's global influence.

Given ZPMC's status as the largest provider of port infrastructure and associated software, it is highly likely that the PRC government has embedded access into its source code, suppliers' source code, and potentially its partners' systems, through mandatory backdoors. Under China's Cybersecurity Law, particularly Article 35, critical infrastructure operators like ZPMC must allow

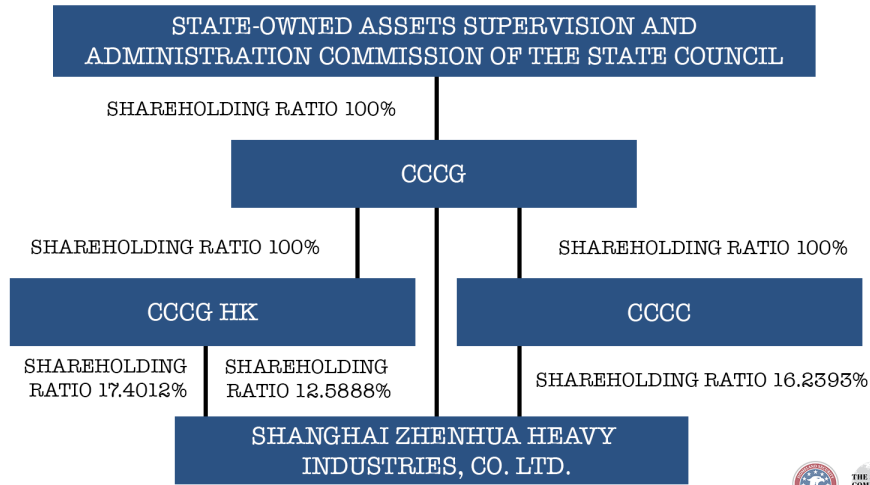
"[I]t is highly likely that the PRC government has embedded access into [ZPMC's] source code, suppliers' source code, and potentially its partners' systems, through mandatory backdoors."

PRC authorities to review source code, granting access to sensitive data and control systems. Additionally, the PRC mandates the storage of certain data within China and permits comprehensive inspections by Chinese authorities. Despite these requirements, PRC cybersecurity databases fail to report vulnerabilities for ZPMC products, compromising system integrity and risking U.S. partners' security. PRC-run services, such as Zoomeye, conceal ZPMC-related vulnerabilities while U.S. platforms like Shodan show numerous entries for ZPMC within China. This selective reporting creates significant security risks for U.S. firms interacting with ZPMC. With ZPMC operating a substantial number of cranes at U.S. ports and providing comprehensive "smart" port infrastructure, the potential vulnerabilities pose a serious national security threat.

The Committees' investigation into ZPMC uncovered numerous national security concerns and vulnerabilities.

ZPMC is a wholly owned subsidiary of China Communications Construction Group (CCCC), aka, China Communications Construction Company (CCCC), a company with significant involvement in militarizing the South China Sea.⁵⁴ In August 2020, CCCC was named a “Communist Chinese Military Company” by the DoD.⁵⁵

Figure 2 – ZPMC Ownership^{56,57,58}



ZPMC is a long-time heavy-equipment operator and component manufacturer headquartered in Shanghai, China. ZPMC originally started as a maritime heavy-machinery manufacturer but has since become the most dominant player in the port-container machinery and crane sector.⁵⁹ ZPMC was founded in 1992 by Guan Tongxian,⁶⁰ who in 2019 was nominated for Shanghai’s “Most Beautiful Revolutionary.” As with most state-owned enterprises, ZPMC’s current board contains senior members of the Chinese Communist Party (CCP),⁶¹ and individuals with senior positions in PRC defense contractors and other malign organizations.

ZPMC has a fleet of approximately 20 large vessels, some designed for dredging operations to make islands in the South China Sea, and other larger cargo vessels and semi-submersible heavy-lift ships. The ZPMC ship Zhen Hua 28 has conducted training with the People’s Liberation Army Ground Force (PLAGF) helicopter squadrons in exercises, using their semi-submersible heavy-lift ships as flight decks for military aircraft.⁶² The PRC media attempted to hide the identity

“ZPMC ship Zhen Hua 28 has conducted training with the People’s Liberation Army Ground Force helicopter squadrons in exercises, using their semi-submersible heavy-lift ships as flight decks for military aircraft.”

of the ship; however, an expert from the U.S. Air Force Academy confirmed the Zhen Hua 28 provided its services as a sizeable civilian flight deck for military operations.⁶³ The PRC uses civilian ships as cover for other operations, as evidenced by their maritime militia in the South China Sea and off the coast of Japan.⁶⁴ PLAN is specifically looking to

leverage the capital markets to invest in its long-term ambitions to develop a capable blue-water navy.⁶⁵ As one of the largest Chinese maritime champions, ZPMC has likely benefited from the PLAN infusion of capital and has announced rounds of investment that are likely downstream effects of investment by PLAN in its naval capacity growth.⁶⁶ In this way, ZPMC serves as a critical component to the PRC's strategy of global logistics dominance through PLAN expansion and growth.

Figure 3 – ZPMC Participation in PLA Exercises



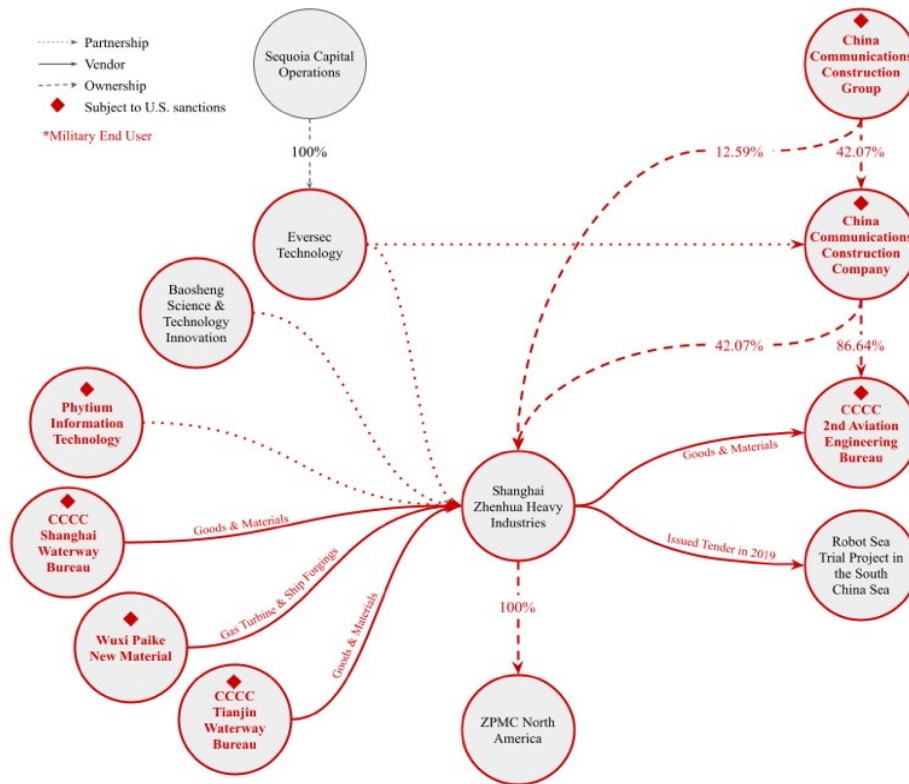
According to documents obtained by the Committees, the most recent president of ZPMC and CCP member, Ou Huisheng, is also the chairman of the state-owned heavy industry firm Tongyu Heavy Industry Company Limited.⁶⁷ The Committees have found that as recently as 2023, Tongyu Heavy Industry Company Limited has sent shipments of goods to Magnitogorskiy Metallurgicheskiy Kombinat (MMK),⁶⁸ a sanctioned Russian steelmaker which is owned by Viktor Filippovich Rashnikov, a sanctioned Russian Oligarch.⁶⁹ This example follows the broader trend of Chinese engineers and steel manufacturing enabling Russian heavy industry to keep producing iron and steel necessary to support Russia's invasion of Ukraine and its wartime economy.⁷⁰

“ZPMC was [listed as] a ‘ccooperation partner’ of Eversec Technologies[, which is] using AI to develop PLA early-warning platforms.”

In 2021 Eversec Technology Co., Ltd., listed ZPMC as a “cooperation partner.”⁷¹ Eversec is a PRC firm and state security contractor in the communications networking and big-data intelligence and security business. Eversec serves as a national-level “cybersecurity emergency service support unit” for the PRC's National Computer Network Emergency Response Technical Team/ Coordination

Center (CNCERT).⁷² Eversec is also using AI to develop PLA early- warning platforms and taking sizeable investment from Sequoia Capital China.⁷³

Figure 4 – ZPMC Partnerships and Affiliations



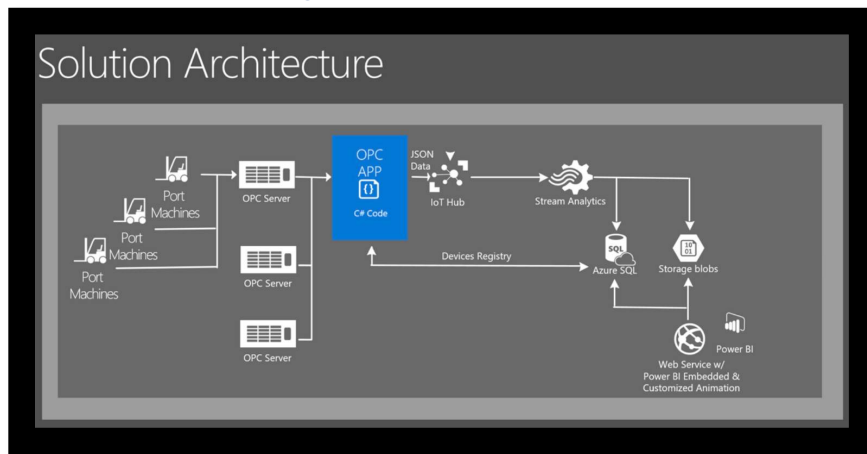
In 2017, ZPMC partnered with Microsoft to develop a suite of tools to connect machinery and analyze real-time port activity and cargo movement, wherein the data is then passed back to a central hub for analysis.⁷⁴ That year, then-ZPMC chairman, Hailiang Song, proclaimed, “We used to sell equipment, but now we are selling systems... Through our main office in Shanghai, you can monitor all the cranes.”⁷⁵ This statement alone has raised grave national security concerns with the Committees. Song also stated, “We used to sell hardware, now we are selling software and service... The automation terminal is the main product in our future.”⁷⁶

“In 2017, ZPMC partnered with Microsoft to develop a suite of tools to ... [pass] real-time port activity and cargo movement ... [data] to a central hub for analysis.”

ZPMC has been instrumental in developing the Belt and Road Initiative and helping build the Smart Cities program for the PRC.⁷⁷ ZPMC also partnered with

Microsoft China, Navis, and infrastructure advisory firm Moffat & Nichol to explore opportunities and automation solutions to incorporate into their “smart” port offerings.⁷⁸ The extent to which this partnership has developed is unclear, though efforts by ZPMC to connect port infrastructure to the cloud have continued and seem to have integrated solutions from Microsoft Azure and Microsoft Power BI.⁷⁹

Figure 5 – Solution Architecture



i. Mandatory Access for PRC Law Enforcement and Intelligence

Since ZPMC is one of the largest providers of port infrastructure and the accompanying software to run it, the PRC government is entitled to access ZPMC’s source code, the source code of its suppliers and potentially its partners. Furthermore, Chinese law enforcement has mandatory backdoors known as embedded and reserved interfaces that are legally required in all domestically created devices.⁸⁰ This vulnerability coincides with China’s totalitarian laws and regulations, which include the requirement that companies comply with intrusive measures for “national security.”⁸¹

Under the Cybersecurity Law of the People’s Republic of China, particularly Article 35,⁸² critical information infrastructure operators such as ZPMC are mandated to allow reviews on the provision of source code.⁸³ These reviews allow the PRC to access sensitive data and control systems. These cybersecurity requirements are further bolstered by the Multi-Level Protection Scheme,⁸⁴ which requires network operators to store specific data within China and permits Chinese authorities to conduct on-site or remote checks on the networks.⁸⁵ This includes examining documentation that reveals the construction of the system, thus exposing source code.⁸⁶

Because the PRC government has legally obligated access to ZPMC’s source code—including integrated software offered by suppliers—sensitive information

about critical port infrastructure software is accessible to the PRC government. With access to source code, there is a high risk that the PRC government could manipulate these systems for strategic reasons, including the disruption of U.S. critical infrastructure. Additionally, this access could be used as a tool for espionage, as the information and data of ports using ZPMC infrastructure could be compromised.

“With access to source code, there is a high risk that the PRC government could manipulate these systems [...] U.S. critical infrastructure [or conduct] ... espionage.”

ii. PRC Hides ZPMC Cybersecurity Vulnerabilities

The PRC’s national cybersecurity vulnerability database returns zero results for ZPMC products,⁸⁷ whereas U.S.-based companies have identified and published dozens of entries on ZPMC vulnerabilities.⁸⁸ Because all cybersecurity vulnerabilities must be disclosed to the PRC government under the Multi-Level Protection Scheme⁸⁹ lack of public reporting on these vulnerabilities suggests an effort by the PRC government to cover up or purposefully obscure any such vulnerabilities.⁹⁰

PRC-sponsored services such as Zoomeye, owned and operated by the PRC military cyber contractor KnownSec, are designed to find and catalog web-facing vulnerabilities so that they can be remediated before adversaries compromise them.⁹¹ These same companies appear to hide ZPMC and ZPMC-related site vulnerabilities, whereas U.S. firms such as Shodan have numerous entries for ZPMC within China. The PRC laws surrounding cybersecurity mandate that only the PRC is aware of the problems associated with companies like ZPMC. This creates a national security issue for U.S. firms who deal with ZPMC or their partners because they are not receiving a wholistic or accurate perspective.

iii. Hidden Cellular Modems on ZPMC Cranes

Throughout the course of the investigation, the Committees uncovered that cellular modems—connected to Linux computers on port cranes—were found on some ZPMC cranes delivered from China to the United States.⁹²

“These modems—although not necessary for the operation of the cranes—created an obscure method to collect information, and bypass firewalls in a manner that could potentially disrupt port operations.”

Figure 6 – Cellular Modem



According to contract documents⁹³ and port operators familiar with the orders, these unknown modems were believed to be installed under the auspices of collecting usage data for the equipment.⁹⁴ These modems—although not necessary for the operation of the cranes—created an obscure method to collect information, and bypass firewalls in a manner that could potentially disrupt port operations.⁹⁵

Technicians at the ports were aware of these modems and understood them to be for diagnostic purposes only; however, the modems were not part of an existing contract, and their services were declined at the time of purchase of the cranes.⁹⁶ These modems were intended to allow for a mobile diagnostic and monitoring add-on—a feature the ports chose not to include.⁹⁷ In at least one case, modems were installed during the manufacturing and assembly process in 2017.⁹⁸ Notably, when the ports first inspected the cranes in the PRC, the modems were already in place.⁹⁹

The Committees were told by security stakeholders that it is an open secret among ports and terminal operators that throughout the process of procuring a ZPMC crane, they will be pressured to provide remote access—under the auspices of monitoring and diagnostics. Some ports insist on securing their assets, but many cave to the pressure.¹⁰⁰ In speaking with industry and security stakeholders, the Committees found that pushing back on ZPMC demands—including allowing for remote access—is difficult for customers who are looking to get the lowest price or guarantee a robust warranty policy.¹⁰¹

“[I]t is an open secret among ports and terminal operators that throughout the process of procuring a ZPMC crane, they will be pressured to provide remote access.”

The exact identity of those responsible for installing the modems, while likely ZPMC, remains unclear.¹⁰² Although the modems were discovered when the cranes were first inspected at a ZPMC manufacturing facility in the PRC, ZPMC has denied responsibility for the modems.¹⁰³ Indeed, non-PRC manufacturers—including ABB—admitted that their hardware is outside of their control while in the PRC and that ZPMC engineers install the components, thereby adding a level of inherent vulnerability to the process.¹⁰⁴ Finally, the non-PRC companies denied knowledge of the cellular modems and agreed that these components introduce an additional vulnerability to the crane.¹⁰⁵

B. ABB’s Role in Port Infrastructure and National Security Risks Arising from Partnership with ZPMC

ABB, a multinational corporation, holds extensive contracts with numerous U.S. government agencies, including the Navy, NASA, and the Defense Logistics Agency. It has produced equipment critical to U.S. national security, such as the U.S. Arleigh Burke class destroyer and the Raven Rock Mountain Complex. That being said, ABB also maintains a long-standing partnership with ZPMC,

beginning in 1992, and has involved significant collaborations in crane automation, energy-efficient propulsion for deep-sea vessels, and certain automation services. ABB stores products in China for up to 18 months, shares design schematics, and allows for ZPMC engineers to finalize product assembly before shipment to the United States. Although ABB claims it is confident with its internal protections against attacks, ABB suffered a ransomware attack in May 2023—potentially compromising sensitive data. And as late as November 2023, a Russia cybercriminal was reported to be selling access to ABB’s systems and those of its PRC supplier, indicating unresolved cybersecurity vulnerabilities.

i. ABB Contracts with U.S. Government

ABB’s operations in the United States include extensive contracts with multiple government agencies such as the United States Navy, NASA, Tennessee Valley Authority, Bureau of Reclamation, Southeastern Pennsylvania Transport Authority, Department of Agriculture, Department of Commerce, Defense Logistics Agency, Department of State, Department of Treasury, Environmental Protection Agency, Federal Aviation Administration, National Oceanic and Atmospheric Administration, Electrify America, Army Corp of Engineers, Coast Guard, and the United States Air Force.¹⁰⁶

ABB has contracted to produce equipment for the Navy’s Arleigh Burke-class guided missile destroyer, as well as the power management system for the Raven Rock Mountain Complex, otherwise known as Site R or “the underground Pentagon,” which is a strategic national facility site crucial to U.S. continuity of government.¹⁰⁷

ii. ABB’s Extensive Partnership with ZPMC

ABB’s partnership with ZPMC has a long history, starting in 1992, and continuing through Collaboration on Crane Automation and Support Systems in 2007, when ABB contributed significantly to ZPMC’s development of container cranes by providing a complete set of crane automation and support systems for 74 ZPMC-developed container cranes.¹⁰⁸ This package included controllers, software, low-voltage AC motors and inverters, power transformers, and switchgear.¹⁰⁹ In 2009, ABB and ZPMC expanded their cooperation to develop energy-efficient propulsion solutions for deep-sea offshore vessels.¹¹⁰ This collaboration created equipment for vessels requiring deep operating draught, such as heavy carriers or drilling platforms.¹¹¹ The partnership focused on utilizing ABB’s Compact Azipod technology, known for its unique design, lifecycle availability, excellent station-keeping capabilities, and compact size.¹¹²

In 2014, ABB and ZPMC signed a Memorandum of Cooperation in port automation services.¹¹³ This agreement aimed to strengthen cooperation in the port machinery transformation service sector, covering technical support, information sharing, spare parts supply, and more.¹¹⁴ The goal was to optimize workflow and achieve beneficial results and to set up 15 port machinery service and spare parts

centers worldwide to transition from equipment manufacturing to service providing.¹¹⁵ Correspondingly, ABB, with a focus on developing its service sector, had already established multiple integrated service centers in China, its second-largest market.

“ABB does, in fact, work hand in hand with ZPMC within the PRC.”

ABB does, in fact, work hand in hand with ZPMC within the PRC. For example, ABB stores its software products in the PRC for up to 18 months following shipment from Europe and before the cranes are delivered to the United States.¹¹⁶ During that time, the hardware is accessible to ZPMC. ABB also provides ZPMC personnel with design schematics, which would allow ZPMC to create a backdoor in the hardware. In addition, ABB works closely with ZPMC engineers on product

“ZPMC engineers—not ABB personnel—assemble the final product and integrate the ABB software before the cranes are shipped to US ports.”

specifications to ensure that its software is interoperable with ZPMC hardware and firmware.¹¹⁷ Finally, ZPMC engineers—not ABB personnel—assemble the final product and integrate the ABB software before the cranes are shipped to U.S. ports.

iii. ABB’s Ransomware and Unreported Cybersecurity Incidents

In May of 2023, reports revealed that ABB had fallen victim to a ransomware attack from the cybercriminal organization BlackBasta, which exposed many customers’ data.¹¹⁸ ABB is likely to have paid between \$1.2 and \$9 million in ransom to have their systems restored.¹¹⁹ It is unknown whether nation-state actors purchased the data from the criminal organization in a secondary market.

According to a cybersecurity report,¹²⁰ in November 2023, a Russian cybercriminal was selling access to ABB’s internal systems as well as access to their PRC supplier “TPV Technology,” an affiliate of the PRC military company China Electronics Corporation, which is also sanctioned by the Treasury Department for contributing to civil-military fusion in the PRC.¹²¹

IV. COMMITTEE INVESTIGATION ENGAGEMENT

A. ABB Engagement

ABB initially conveyed its intent to work with the Committees to address concerns with their partnerships with PRC-connected firms like ZPMC.¹²² ABB asked the Committees to work with them and identify areas of concern they could remediate to better address U.S. national security and counterintelligence concerns.¹²³ Their initial document production included hundreds of pages that were publicly available on their website and did not directly answer the Committees' questions.¹²⁴ The Committees specifically requested information on the following:

1. The a West Coast port crane agreement, specifically section 3.5, titled, "Limit Switches and Sensors" (reference number 01-000412), outlines the necessity for component compatibility between ABB and ZPMC. Considering ABB's previous declaration of not sharing coding with China, the Committees were interested in the methods employed to achieve this compatibility in hardware and software compliance with the China's Cybersecurity Law.
2. The approach to compatibility in other areas of the supply scope for multiple cranes. This query particularly pertains to elements such as the CCTV system, the spreader, the power-cable reel assembly, and the previously identified vulnerabilities in the Profibus and Profibus interface. This question is even more important in light of ZPMC's role in providing the communication gateway for these components (reference number 01-000419).
3. The document exchange plan between ZPMC and ABB (reference number 01-000426). The Committees seek clarity on the extent of detail shared with ZPMC during the "Remote Control Station (RCS) layout and functional description" phase.
4. Information on the nature and depth of data exchanged in other phases of this collaboration process.

After meeting multiple times with ABB, the Committees documented substantial stalling techniques.¹²⁵ ABB claimed that they were undergoing a review of the concerns and wanted to help in any way they could. ABB conveyed multiple times that they do not share any software or code with the PRC and have somehow "found a way" to circumvent PRC national security laws that mandate source-code sharing in order to do business in China. Proof of this was never given, and the Committee received information from ZPMC¹²⁶ and other

"ABB conveyed multiple times that they do not share any software or code with the PRC ... [but] proof of this was never given, and the Committee received information ... that suggests all software was provided for testing at manufacturing sites in China."

manufacturers¹²⁷ that suggests all software was provided for testing at manufacturing sites in China.

Table 1 – Timeline of ABB Interactions with Committees

JUNE 15, 2023 Email from CHS staff to ABB requesting a briefing to discuss ABB’s commercial engagement with U.S. seaports, U.S. government agencies, and their presence in the PRC.	JUNE 16, 2023 Email from ABB to CHS staff confirming ABB will provide a briefing.
JUNE 20, 2023 CHS staff and ABB speak on the phone.	JUNE 19, 2023 Email from ABB asking for a call to discuss the briefing request.
JUNE 26, 2023 CHS and China Select officially launch a joint investigation.	JUNE 23, 2023 Sidley Austin LLP places a call to CHS staff noting they have been retained as counsel for ABB and we should communicate through them going forward.
JULY 11, 2023 CHS and China Select hold a call with Sidley Austin LLP.	Sidley Austin LLP sends an email to CHS staff after calling earlier in the day and asking to schedule a follow-up call the week of July 10-14.
JULY 25, 2023 CHS/China Select transmit a letter to ABB requesting documents and information by no later than August 8, 2023.	JULY 19, 2023 In-person meeting between CHS/China Select staff and Sidley Austin LLP to discuss the ABB inquiry.
SEPTEMBER 6, 2023 China Select emails Sidley Austin LLP asking for a second in-person meeting to discuss the document production.	AUGUST 8, 2023 Sidley Austin LLP delivers the document production to China Select staff.
SEPTEMBER 27, 2023 CHS/China Select meet with Sidley Austin LLP to discuss the ABB document production as well as remedial action to address the security vulnerabilities identified by committee staff. CHS/China Select staff ask for ABB’s response by (11/23).	SEPTEMBER 12, 2023 Sidley Austin LLP does not respond to China Select’s 9/6 email, prompting CHS staff to send a follow-up email requesting a meeting the week of September 25th. Sidley Austin LLP responds and agrees to meet on September 27th.
OCTOBER 23, 2023 Squire Patton Boggs (SPB) contacts Chairman Gallagher’s personal office to discuss the ABB inquiry. In an email, SPB notes they have been retained by ABB as lobbyists. Several other Member offices reach out to the committees informing staff that Squire Patton Boggs is requesting information about the joint investigation/ABB inquiry.	OCTOBER 11, 2023 CHS/China Select staff meet with Sidley Austin LLP to further discuss the security vulnerabilities identified and potential remedial action by ABB.
OCTOBER 23, 2023-JANUARY 17, 2024 The Committees receive no further outreach from Sidley Austin LLP or their client, ABB.	OCTOBER 25, 2023 Sidley Austin LLP meets with China Select staff.
JANUARY 18, 2024 The Committees send a public letter to ABB, outlining the company’s disregard for the investigation and requesting their American executives presence at a CHS hearing.	OCTOBER 27, 2023 Sidley Austin LLP requests a second meeting to discuss the committee’s investigation. During the meeting, CHS/China Select staff reiterate the request for a response from ABB about potential remedial action by November 23, 2023. Sidley Austin LLP suggested they could provide a response by the stated deadline.
JANUARY 26, 2024 Sidley Austin LLP communicates to CHS and China Select staff that ABB is unable to agree to participate in a hearing.	JANUARY 23, 2024 Sidley Austin LLP contacts CHS and China Select staff to discuss the January 18, 2024 letter. Sidley Austin LLP tells Committee staff that the letter “got Sweden’s attention”
FEBRUARY 21, 2024 CHS staff email Sidley Austin LLP reiterating the committee’s request for public testimony from ABB’s U.S. Country Holding Officer, Mr. Michael Gray.	FEBRUARY 7, 2024 CHS and China Select staff meet with senior executives from ABB Headquarters and Sidley Austin LLP to discuss the committees’ January 18, 2024 letter, the ongoing investigation, and the request for ABB’s participation in a CHS hearing that was tentatively scheduled for February 29, 2024.
FEBRUARY 23, 2024 Sidley Austin LLP hand delivers a letter to CHS/China Select staff responding to lines of inquiry discussed during the February 7, 2024 in-person meeting with ABB senior executives.	FEBRUARY 23, 2024 Sidley Austin LLP emails CHS/China Select staff acknowledging the committee’s February 21, 2024 email requesting ABB’s participation in a hearing.
This is the last form of communication between the committees and Sidley Austin LLP relating to the investigation.	FEBRUARY 24, 2024 – MARCH 28, 2024 The Committees receive no further outreach from Sidley Austin LLP or their client, ABB.

Through extensive briefings with various national security community agencies and departments, the Committees found even more reason for concern. ABB sponsors at least one individual with a government security clearance who is responsible for ABB's physical security in the United States. The Committees discussed with ABB the idea of bringing the individual to a secure space so they could better understand the national security threats to which they were exposing U.S. critical infrastructure.¹²⁸ ABB made various excuses for why this was not possible.

First, they claimed the individual did not have the necessary expertise to have an informed conversation with the Committees. Second, they claimed the individual would be unable to do anything with the classified information and therefore would put the company at risk by being made aware of the classified information.¹²⁹ When asked why ABB sponsored a security clearance, ABB admitted it was so that they could discuss security concerns with law enforcement and intelligence.¹³⁰

When asked if ABB had joint ventures in the PRC, ABB did not answer directly and instead pointed to the fact that all the company's sectors were segmented and had no impact on the crane industry.¹³¹ When asked if the PRC had ever leveraged its national security laws to request information from ABB, the company's counsel could not provide a clear answer—leaving the Committees with the impression that ABB probably does provide information pursuant to the PRC's national security laws.¹³²

When ABB was asked to show any actionable deliverables that coincided with their statements to help safeguard the nation and its critical infrastructure, they continued to stall with no results, and offered no plan to solve their internal cybersecurity and supply chain issues.¹³³ Instead, they insisted that their components were secure and their processes and procedures follow the practices of every other company that works with ZPMC.¹³⁴

B. TMEIC and Siemens Engagement

Following extensive engagement with ABB, the Committees spoke with Siemens¹³⁵ and TMEIC¹³⁶ to understand whether ABB's methods were abnormal. Siemens explained that it has a very small portion of this market, which is primarily owned by TMEIC and ABB. Both TMEIC and Siemens confirmed that their companies make internal components for ZPMC cranes and ships and send these components to the PRC for installation. As subcontractors, TMEIC and Siemens explained they have little control over the contracts between ZPMC and the U.S. ports; however, they agreed that a vulnerability exists in the supply chain. Both companies explained that the cost would increase if the cranes' internal components were installed in the United States. In addition to optimizing labor costs, the ZPMC cranes are constructed in a specialized manufacturing site that integrates all the engineers and components—allowing final testing to take place before shipment. Installing internal components in the United States would likely increase the price of the crane—though it could be done.

Throughout the investigation, TMEIC and Siemens were helpful and constructive. The Committees were able to gain valuable insight into the challenges inherent to manufacturing internal crane components. When involved, their counsels were forthcoming and did not attempt to obstruct the work of the investigation.

C. Crane Manufacturers Engagement

The Committees also spoke with crane manufacturers that compete with ZPMC. Konecranes—based in Finland¹³⁷—and Liebherr—based in Germany,¹³⁸ with manufacturing in Ireland—can create STS cranes on par with ZPMC. While more expensive, these crane manufacturers believe that their components last longer than ZPMC’s products and provide more security through supply-chain resilience and avoid the cybersecurity vulnerabilities associated with manufacturing in the PRC. Konecranes pointed to the Port of Savannah in Georgia that relies exclusively on Konecranes as an example of a U.S. port that has spent more on STS cranes because of their longevity and superior security.¹³⁹ Liebherr provides STS cranes to the Port of Newark Container Terminal in New Jersey and Penn Terminals in Eddystone, Pennsylvania.¹⁴⁰

Outside of STS cranes, both Konecranes¹⁴¹ and Liebherr¹⁴² possess significant manufacturing presence in China. On a call with the Committees, Liebherr admitted that currently even its STS cranes would have some components from China. Furthermore, these companies are susceptible to pressure from PRC-based influences that could threaten their market share. While both provide a measure of separation from the direct supply-chain and cybersecurity vulnerability inherent to doing business in and with the PRC, there are still ways for the PRC to exercise soft power and potentially coerce action by these companies.

The Committees are also aware that Mitsui—a Japan-based company—with its U.S.-based subsidiary PACECO, is pursuing STS crane manufacturing in the United States.¹⁴³ Additionally, Kiewit, a construction and manufacturing company based out of Omaha, Nebraska, is considering entering the maritime crane market. Both companies have the potential to completely manufacture the STS crane in the United States; however, building the capacity and creating the expertise will take years. Additionally, these cranes will be more expensive due to the higher labor and material costs in the United States.




































D. ZPMC Engagement

On February 29, 2024, the Committees sent a letter to ZPMC Chairman and President Liu Chengyun and ZPMC USA President Richard Pope expressing concerns about ZPMC’s close ties with the PRC.¹⁴⁴ The letter requested written answers to several questions regarding ZPMC’s connections to the PRC and how their ties to the PRC government impact its work overseas.

In their initial correspondence with the Committees following receipt of the February 29 letter, ZPMC communicated their unwillingness to provide written answers before consultation with the PRC government. On March 19, 2024, a

lawyer contracted by ZPMC contacted Committees staff requesting that the Committees sign a non-disclosure agreement before ZPMC provides information to the Committees. After the Committees declined to sign a non-disclosure agreement, ZPMC’s contracted counsel at Baker McKenzie, provided a letter to the Committees stating that ZPMC’s response to the Committees’ “may trigger data cross-border transfer requirements under applicable Chinese laws.”¹⁴⁵ The laws are detailed in the Table 1 below.

Table 2 – ZPMC Legal Objections to Committees’ Investigation Requests

APPLICABLE CHINESE DATA RESTRICTION LAWS	ISSUES RAISED BY COMMITTEES’ INVESTIGATION		
DATA SECURITY LAW: ARTICLE 36	   		
CYBERSECURITY LAW: ARTICLES 2 AND 37 SECURITY PROTECTION REGULATIONS FOR CRITICAL INFORMATION INFRASTRUCTURE: ARTICLES 2, 8 AND 9 MEASURES ON SECURITY ASSESSMENT FOR CROSS-BORDER TRANSFER OF DATA: ARTICLES 4 AND 19	 		
MEASURES ON SECURITY ASSESSMENT FOR CROSS-BORDER TRANSFER OF DATA: ARTICLE 4 PERSONAL INFORMATION PROTECTION LAW: ARTICLES 3, 4, 38, 39, 55, 56 AND 73	     		
THE LAW OF THE PEOPLE’S REPUBLIC OF CHINA ON GUARDING STATE SECRETS			
DATA SECURITY LAW: ARTICLE 21 MEASURES FOR THE ADMINISTRATION OF DATA SECURITY IN THE FIELD OF INDUSTRY AND INFORMATION TECHNOLOGY (FOR TRIAL IMPLEMENTATION): ARTICLE 21	 		
EXPORT CONTROL LAW: ARTICLES 2 AND 32 DATA SECURITY LAW: ARTICLE 25	 		
LEGEND <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;">  ZPMC RELATIONSHIP WITH CCP INTELLIGENCE  ZPMC PRC SUBSIDIES AND GRANTS TO SUPPORT ZPMC ACTIVITY IN THE UNITED STATES  ZPMC AND ABB REMOTE ACCESS & CCP INTELLIGENCE AGENCIES REQUESTS TO REMOTE ACCESS </td> <td style="width: 50%; vertical-align: top;">  ZPMC RELATIONSHIPS AND ENGAGEMENTS WITH PRC ENTITIES  ZPMC INTERNAL CCP INFLUENCE  ZPMC ONGOING ENGAGEMENT WITH U.S. DEPARTMENT OF COMMERCE ENTITY LIST </td> </tr> </table>		 ZPMC RELATIONSHIP WITH CCP INTELLIGENCE  ZPMC PRC SUBSIDIES AND GRANTS TO SUPPORT ZPMC ACTIVITY IN THE UNITED STATES  ZPMC AND ABB REMOTE ACCESS & CCP INTELLIGENCE AGENCIES REQUESTS TO REMOTE ACCESS	 ZPMC RELATIONSHIPS AND ENGAGEMENTS WITH PRC ENTITIES  ZPMC INTERNAL CCP INFLUENCE  ZPMC ONGOING ENGAGEMENT WITH U.S. DEPARTMENT OF COMMERCE ENTITY LIST
 ZPMC RELATIONSHIP WITH CCP INTELLIGENCE  ZPMC PRC SUBSIDIES AND GRANTS TO SUPPORT ZPMC ACTIVITY IN THE UNITED STATES  ZPMC AND ABB REMOTE ACCESS & CCP INTELLIGENCE AGENCIES REQUESTS TO REMOTE ACCESS	 ZPMC RELATIONSHIPS AND ENGAGEMENTS WITH PRC ENTITIES  ZPMC INTERNAL CCP INFLUENCE  ZPMC ONGOING ENGAGEMENT WITH U.S. DEPARTMENT OF COMMERCE ENTITY LIST		

On April 7, 2024, ZPMC through Baker McKenzie, provided a letter with responses to individual questions raised in the Committees' February 29 letter. The letter emphasizes that "ZPMC USA operates independently from its parent companies."¹⁴⁶ However, many of the responses provided to the Committees cited the PRC laws listed above in detailing that the firm would require permission by the PRC to share information responsive to the Committees' questions.

In response to the Committees' questions regarding its engagement with ABB, ZPMC's letter detailed that ZPMC contacted ABB requesting information regarding remote access to STS cranes and "other maritime infrastructure components" in the United States. While the letter stated that ZPMC had not yet received a response from ABB, the letter asserted that Article 36 of the PRC *Data Security Law* would require ZPMC to obtain permission from the PRC to share ABB's response to ZPMC if content is covered by Article 36.¹⁴⁷

The letter also detailed that ZPMC took internal action to follow up on questions raised in the Committees' letter. According to the letter, ZPMC contacted suppliers regarding "the installation of cellular modems or equipment, component, and system on U.S.-bound cranes."¹⁴⁸ The letter stated that ZPMC was also in the process of reviewing "subsidy-related information in [ZPMC's] financial statements" to determine what grants or subsidies the company received from the PRC government.¹⁴⁹ Additionally, the letter stated that ZPMC had started an "internal review of the possible transactions with entities listed on the [U.S. Department of Commerce's Bureau of Industry and Security] Entity List."¹⁵⁰ However, the letter argued that ZPMC would be required to obtain permission from the PRC to share the findings of these reviews and investigations with the Committees.

ZPMC currently maintains an internal Communist Party Committee. The Committee, according to ZPMC, is established internally and is "involved in the assessment and discussion of ZPMC's significant operational matters

"ZPMC's chairman and president, serves as the party secretary for the Internal Communist Party Committee."

prior to the decision-making process by the board of directors and management level."¹⁵¹ You Ruikai, ZPMC's chairman and president, serves as the party secretary for the Internal Communist Party Committee, and Committee members are elected by "the plenary meeting of the Party members of ZPMC."¹⁵² At the time of writing, ZPMC had not explained to the Committees to whom the Internal Communist Party Committee reports within the PRC government and what information is shared.

Table 3 – Members of ZPMC’s Internal Communist Party Committee

**MEMBERS OF THE ZPMC INTERNAL
COMMUNIST PARTY COMMITTEE:**

- YOU RUIKAI (CHAIRMAN, PRESIDENT, AND PARTY SECRETARY)
- OU HUI SHENG
- ZHU XIAOHUAI
- WANG CHENG
- LIU FENG
- LI RUI XIANG
- SUN LI
- LI YI MING
- MO XIAO JIAN

On June 4, 2024 ZPMC said that there was no evidence suggesting that a PRC entity—including CCP intelligence agencies or security services—had ever requested ZPMC to modify its US-bound maritime equipment.¹⁵³ Despite this fact, ZPMC said that it could not disclose the nature of its relationships or engagements with the Ministry of State Security because of its compliance with *The Law of the People’s Republic of China on Guarding State Secrets*.¹⁵⁴ ZPMC also noted it had conducted an internal review regarding U.S.-bound STS cranes and other onshore maritime infrastructure.¹⁵⁵ During the course of its review, ZPMC claimed it contacted 86 engineers, all of whom advised that no ZPMC modifications were ever requested for US-bound maritime equipment.¹⁵⁶

ZPMC noted that during the course of its internal investigation, the company had communicated with ABB to clarify whether the Swedish company had ever received a request from ZPMC or a PRC entity for remote access to STS cranes or maritime infrastructure.¹⁵⁷ ABB confirmed to ZPMC that this had never taken place, but at the time of the letter had not provided ZPMC with the consent to disclose contact information regarding this request.¹⁵⁸

E. U.S. Ports Engagement

Throughout the investigation, the Committees engaged U.S. ports, asking questions and requesting documentation regarding cranes and cybersecurity practices. Each port has unique requirements due to its geography and merchandise; however, common vulnerabilities exist, and some ports engage the security concerns effectively, while others do not.

i. Port Authority and Terminal Operator Delineation

In the Committees’ engagements, some of the port authorities deferred to their terminal operators for security procedures, because of the way they had written their contracts. One of the ports told the Committees that they had asked the Coast

Guard to do a “cyber hunt” mission at their port to ensure best cybersecurity practices and the terminal operator had declined to participate despite possessing ZPMC cranes. Throughout the investigation, the Committees often had to reach out separately to the terminal operators to gain access to the appropriate information concerning the cranes and the contracts secured with ZPMC. The Committees are encouraged that the Coast Guard captain of the port is specifically addressed in the executive order to bolster cybersecurity at the ports.¹⁵⁹

The Committees remain concerned that the port authorities have often structured their legal agreements with terminal operators in such a way as to pass off risk and are unable or unwilling to address the cybersecurity challenges in some cases.

ii. Attempts to Mitigate Vulnerabilities Posed by ZPMC Cranes

Due to the cost difference between ZPMC cranes and those offered by other providers such as Konecranes or Liebherr, many ports purchase ZPMC cranes. Some of these ports understand the security implications and arrange for the FBI to come investigate the crane electronics before connecting cranes to the broader port network. Additionally, many of these ports contract with outside cybersecurity companies to perform penetration testing and a cybersecurity policy audit. Some of these ports request a Coast Guard cybersecurity analysis by cyber protection teams. These actions can significantly reduce the vulnerabilities posed by the PRC, but some ports do not engage in any of these actions, and the original manufacturing and installation takes place in the PRC, outside the purview of the internal component manufacturers, and therefore carries inherent cybersecurity risk.

The ZPMC crane manufacturing process takes place in the PRC and all components—even those components made in the United States—are shipped to the PRC for installation and testing by ZPMC engineers. Upon arrival at the U.S. port, Chinese ZPMC engineers help install and test the crane. Internal component manufacturers such as TMEIC and ABB will inspect their products during the testing phase in the PRC and upon delivery to the U.S. port; however, these components are left in the PRC for extended periods of time and are installed by ZPMC engineers.

Ports have admitted to the Committees that the use of ZPMC engineers is part of the contract and helps keep crane costs low. When asked if the contract could stipulate that internal components are installed in the United States, ports said the contracts do not typically allow for that option and that it would increase the cost of the crane.

V. GUAM'S STRATEGIC SIGNIFICANCE AND THE NEED FOR ENHANCED INFRASTRUCTURE AMID RISING TENSIONS IN THE INDO-PACIFIC

During the investigation, the Committees conversed extensively with representatives from Guam, the civilian port on the island, MARAD, DoD, and various other stakeholders. The Committees discovered that due to poor management from the port authority, MARAD, and DoD, Guam is unable to consistently receive grant funding, obtain strategic port status, maintain or improve its cyber security posture, and avoid the pitfalls of installing PRC-made equipment in its port.

A. Guam's Geopolitical Significance

As the geopolitical landscape in the Indo-Pacific undergoes rapid shifts and the PRC continues to escalate tensions in the South China Sea and the Taiwan Strait, the strategic importance of Guam has come into sharper focus.¹⁶⁰ This has highlighted its geographical and military importance, burdened by the current state of its critical infrastructure and its unique position as a territory inhabited by American citizens.

Guam and the Northern Mariana Islands' location as the waypoint to Taiwan, Japan, and the Philippines is critical for U.S. military operations and strategic interests.¹⁶¹ Home to significant Navy and Air Force assets, Guam serves as a forward operating base for the United States, playing a crucial role in monitoring and potentially countering PRC activities.¹⁶² Its value as a strategic outpost cannot be overstated, especially in the context of the PRC's growing military presence, assertiveness, and even destabilizing behavior in the Indo-Pacific. In the event of a crisis in the Indo-Pacific, Guam will be a critical trans-shipment point for supplies and other critical items and personnel.

B. Guam's Critical Infrastructure Vulnerabilities

Despite its strategic importance, there are growing concerns about Guam's critical infrastructure, particularly its ports, airfields, and electric grid, which are essential for military operations and the island's civilian population and economy.¹⁶³ The Committees have found that the current levels of investment in and maintenance of these resources must be increased to meet the demands of a potential emergency scenario in the Indo-Pacific. This neglect poses significant risks to U.S. military capabilities in the region and the safety and well-being of Guam's residents. Moreover, as American citizens, the residents of Guam are entitled to the same level of protection and

“Current levels of investment in and maintenance of [Guam's critical infrastructure and military facilities] must be increased to meet the demands of a potential emergency scenario in the Indo-Pacific.”

infrastructure development as those in the mainland United States. Our findings emphasize that strategic planning for Guam must balance military needs with the welfare of its residents, ensuring that their rights and needs are not overlooked amidst broader geopolitical concerns.

In early 2023, a state-sponsored hacking group connected to the PRC known as “Volt Typhoon” targeted and attacked Guam’s critical infrastructure, as well as other critical infrastructure in the United States.¹⁶⁴ These PRC-led critical infrastructure attacks exposed a significant gap in Guam’s cyber security protocols and continue to this day.¹⁶⁵

“In early 2023, a state-sponsored hacking group connected to the PRC known as “Volt Typhoon” targeted and attacked Guam’s critical infrastructure.”

The Committees discovered a highly complex process to get skilled cybersecurity personnel who are able to work on Guam’s critical infrastructure. According to documents provided to the Committees, there are crucial gaps in cybersecurity standards on the island of Guam due to a lack of financial resources and experts in the field readily available from the United States. This means cybersecurity experts from Australia and other nearby countries are used first. Guam’s ability to increase the cybersecurity of its critical infrastructure is crucial to Guam’s survival and essential to its ability to act as a strategic basing option in the event of a crisis.

“According to documents provided to the Committees, there are crucial gaps in cybersecurity standards on the island of Guam due to a lack of financial resources and experts in the field readily available from the United States.”

C. Disagreement Between Department of Transportation, MARAD, and Department of Defense on Guam’s Strategic Importance

During the Committees’ investigation, we discovered that while the Port of Guam is listed as a Commercial Strategic Seaport under MARAD, the DoD does not extend the same recognition, limiting its ability to receive the same resources as other U.S. mainland Commercial Strategic Seaports.

Figure 7 – U.S. Commercial Strategic Seaports

STRATEGIC SEAPORTS IN THE UNITED STATES AND ITS TERRITORIES:		
■ ANCHORAGE, AK	■ GULFPORT, MS	■ PHILADELPHIA, PA
■ BEAUMONT, TX	■ HAMPTON ROADS, VA	■ PORT ARTHUR, TX
■ CHARLESTON, SC	■ JACKSONVILLE, FL	■ SAN DIEGO, CA
■ CORPUS CHRISTI, TX	■ LONG BEACH, CA	■ SAVANNAH, GA
■ PORT OF EVERETT, WA	■ MOREHEAD CITY, NC	■ TACOMA, WA
■ GUAM	■ OAKLAND, CA	■ WILMINGTON, NC

The Military Surface Deployment and Distribution Command (SDDC), which falls under the United States Transportation Command, is responsible for all origin-to-destination distribution operations and plans and executes the surface delivery of equipment and supplies globally. Since 2016, and because it does not have a designated surge deployment mission, SDCC has held the Port of Guam in special status, which means that MARAD does not issue it a Port Readiness Plan, nor ask it to participate in other voluntary planning or readiness reporting activities.¹⁶⁶ SDDC has determined that the Port of Guam currently has no significant deployment or operational role that would typically coincide with a Commercial Strategic Seaport designation; nevertheless, it has retained Guam in the program due to its unique strategic location and importance to DoD.¹⁶⁷

“DoD does not ... recogn[ize Guam as a strategic seaport], limiting its ability to receive the same resources as other U.S. mainland strategic seaports.”

The Committees have reviewed the port readiness plans and the SDDC Commercial Strategic Seaport Infrastructure requirements and found a lack of cybersecurity requirements necessary to be considered a Commercial Strategic Seaport. The post-9/11 counterterrorism requirements are still critical; however, there needs to be a statutory expansion to include a more robust cybersecurity requirement to meet the threats faced in the modern environment.

The strategic significance of Guam, particularly in terms of contingency operations, calls for a reassessment of its role in military planning. Its location in the Indo-Pacific endows it with high military value, serving as a critical point for power projection and facilitating rapid response within the Indo-Pacific theater. This geographic advantage positions Guam as a launchpad for military initiatives and a central hub for ongoing sustainment and redeployment during significant contingency operations.

There must be immediate and sustained action to enhance Guam's infrastructure, particularly its ports, to ensure they can support both military and civilian needs in times of crisis. It is also necessary for a strategic re-evaluation of Guam's role in Indo-Pacific policy, one that considers the island's dual importance as a military asset and a home to American citizens. Failing to address these issues could have dire consequences for U.S. strategic interests in the region and the people of Guam.

“There must be immediate and sustained action to enhance Guam's infrastructure, particularly its ports, to ensure they can support both military and civilian needs in times of crisis.”

CLASSIFIED ANNEX

The Committees are primarily concerned with ZPMC cranes in U.S. ports; the global influence of the company and the implications are far-reaching. Appropriately cleared parties can read the analysis on file with the Homeland Committee.

ENDNOTES

-
- ¹ Chasing the dragon, Chasing the dragon, THE ECONOMIST, <https://www.economist.com/united-states/2013/04/13/chasing-the-dragon> (last visited Feb 22, 2024).
- ² China's "going out" strategy, China's "going out" strategy, THE ECONOMIST, <https://www.economist.com/free-exchange/2009/07/21/chinas-going-out-strategy> (last visited Feb 22, 2024).
- ³ The COSCO Danger Looms Large For The Global Supply Chain, <https://www.forbes.com/sites/loracecere/2022/12/30/the-cosco-danger-looms-large-for-the-global-supply-chain/> (last visited Aug 14, 2024).
- ⁴ Mike Yeo, *China Reportedly Converted Civilian Ferries for Amphibious Assault Operations*, DEFENSE NEWS (2021), <https://www.defensenews.com/naval/2021/08/04/china-reportedly-converted-civilian-ferries-for-amphibious-assault-operations/> (last visited Feb 22, 2024).
- ⁵ ZPMC and America's Ship-to-Shore Crane Industry: Recommendations for Improving Port Security | The Foundation for American Innovation, <https://www.thefai.org/posts/zpmc-and-america-s-ship-to-shore-crane-industry-recommendations-for-improving-port-security> (last visited Feb 15, 2024).
- ⁶ Aruna Viswanatha, Gordon Lubold & Kate O'Keeffe, *WSJ News Exclusive | Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools*, Wall Street Journal, Mar. 5, 2023, <https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade> (last visited Feb 14, 2024).
- ⁷ Leah Wils-Owens, *China's Status as a Non-Market Economy*, 28 (2017), <https://enforcement.trade.gov/download/prc-nme-status/prc-nme-review-final-103017.pdf>.
- ⁸ Viswanatha, Lubold, and O'Keeffe, *supra* note 6.
- ⁹ Wils-Owens, *supra* note 7 at 28.
- ¹⁰ ZPMC USA, *ZPMC USA*, ZPMC USA, <https://zpmcusa.com/who-we-are> (last visited Feb 14, 2024).
- ¹¹ Shusheng Yang, Lijuan Chen & Xianjin Bi, *Overtime Work, Job Autonomy, and Employees' Subjective Well-Being: Evidence from China*, 11 FRONT PUBLIC HEALTH 1077177 (2023).
- ¹² Jude Blanchette et al., *Hidden Harbors: China's State-Backed Shipping Industry* (2020), <https://www.csis.org/analysis/hidden-harbors-chinas-state-backed-shipping-industry> (last visited Feb 14, 2024).
- ¹³ What Grade Steel Is Used For Cranes?, ZOKE CRANE, <https://www.zoke-crane.com/posts/8526/> (last visited Feb 15, 2024).
- ¹⁴ Kevin Dempsey, *Steel Market Update Column: US Trade Laws Must Be Upgraded to Address China's Belt and Road Initiative*, AMERICAN IRON AND STEEL INSTITUTE (Jan. 26, 2024), <https://www.steel.org/2024/01/steel-market-update-column-us-trade-laws-must-be-upgraded-to-address-chinas-belt-and-road-initiative/> (last visited Feb 15, 2024).
- ¹⁵ Blanchette et al., *supra* note 12.
- ¹⁶ Viswanatha, Lubold, and O'Keeffe, *supra* note 6.
- ¹⁷ ALEXANDER WOOLEY ET AL., *HARBORING GLOBAL AMBITIONS: CHINA'S PORTS FOOTPRINT AND IMPLICATIONS FOR FUTURE OVERSEAS NAVAL BASES* (2023), <https://scholar.google.com/scholar?cluster=1965649976175512556&hl=en&oi=scholar> (last visited Mar 25, 2024).
- ¹⁸ Terminals | COSCO SHIPPING North America, <https://na.coscoshipping.com/terminals/> (last visited Mar 13, 2024).
- ¹⁹ Isaac Kardon, *Research & Debate—Pier Competitor: Testimony on China's Global Ports*, 74 NAVAL WAR COLLEGE REVIEW (2021), <https://digital-commons.usnwc.edu/nwc-review/vol74/iss1/11>.
- ²⁰ Charlie Lyons Jones, *The Port Operators behind China's Naval Expansion*, THE STRATEGIST (2021), <https://www.aspiratelist.org.au/the-port-operators-behind-chinas-naval-expansion/> (last visited Mar 13, 2024).
- ²¹ EXPANDING GLOBAL PRESENCE AND IMPLEMENTING LEAN OPERATIONS | ACCELERATING HIGH-QUALITY DEVELOPMENT BY INCREASING EFFICIENCY, (2022), <https://doc.irasia.com/listco/hk/coscoship/annual/2022/ar2022.pdf>.
- ²² Yeo, *supra* note 4.

-
- ²³ RO-RO Ferries and the Expansion of the PLA's Landing Ship Fleet | Center for International Maritime Security, <https://cimsec.org/ro-ro-ferries-and-the-expansion-of-the-plas-landing-ship-fleet/> (last visited Mar 13, 2024).
- ²⁴ COSCO: China's shipping giant expands its global influence - Nikkei Asia, <https://archive.is/20220513182431/https://asia.nikkei.com/Business/Business-Spotlight/COSCO-China-s-ship-ping-giant-expands-its-global-influence#selection-2791.428-2791.610> (last visited Mar 13, 2024).
- ²⁵ COSCO SHIPPING and the Hellenic Republic Asset Development Fund (HRADF) Signed a Letter Confirming the Acquisition of 67% Equities of PPA, https://bulker.coscoshipping.com/col10718/art/2016/art_10718_82350.html (last visited Aug 14, 2024).
- ²⁶ The series of activities of "Joining Hands with Central Enterprises to Dialogue with the World" approached COSCO SHIPPING and entered Xiamen, Fujian Province_Ministry of Foreign Affairs of the People's Republic of China, https://www.mfa.gov.cn/web/wjw_673085/zzjg_673183/wsgls_674701/xgxw_glj_674703/202309/t20230915_11143537.shtml (last visited Mar 13, 2024).
- ²⁷ The United States Imposes Sanctions on Chinese Companies for Transporting Iranian Oil, UNITED STATES DEPARTMENT OF STATE, <https://2017-2021.state.gov/the-united-states-imposes-sanctions-on-chinese-companies-for-transporting-iranian-oil/> (last visited Mar 13, 2024).
- ²⁸ China Merchants Group, https://www.cmhk.com/home/a/2021/d08/a42239_44399.shtml?4 (last visited Mar 13, 2024).
- ²⁹ Did China's Belt and Road Initiative destroy Sri Lanka? — Radio Free Asia, <https://www.rfa.org/english/commentaries/china-srilanka-07182022103112.html> (last visited Mar 13, 2024).
- ³⁰ Doraleh Multipurpose Port (I), THE PEOPLE'S MAP OF GLOBAL CHINA, <https://thepeoples-map.net/project/doraleh-multipurpose-port-phase-i/> (last visited Aug 14, 2024).
- ³¹ Peter Dutton, Isaac Kardon & Conor Kennedy, *China Maritime Report No. 6: Djibouti: China's First Overseas Strategic Strongpoint*, CMSI CHINA MARITIME REPORTS (2020), <https://digital-commons.usnwc.edu/cmsi-maritime-reports/6>.
- ³² Chinese military ship leaves Sri Lanka after controversial visit, REUTERS, Aug. 22, 2022, <https://www.reuters.com/world/asia-pacific/chinese-military-ship-leaves-sri-lanka-after-controversial-visit-2022-08-22/> (last visited Mar 13, 2024).
- ³³ Shihar Aneez, *Exclusive: Sri Lanka's Cabinet "clears Port Deal" with China Firm after Concerns Addressed*, REUTERS, Jul. 25, 2017, <https://www.reuters.com/article/idUSKBN1AA0PI/> (last visited Mar 13, 2024).
- ³⁴ DP World wins another ruling in battle over Djibouti port, AP NEWS (2022), <https://apnews.com/article/middle-east-africa-china-hong-kong-e01b827fd55dd5fba9d13f5e5baabade> (last visited Mar 13, 2024).
- ³⁵ China Merchants Group, *supra* note 28.
- ³⁶ CHINA MERCHANTS PORT HOLDINGS COMPANY LIMITED, <https://www.cmport.com.hk/EnTouch/business/Infor.aspx?id=10000819> (last visited Mar 13, 2024).
- ³⁷ Chinese Investments in the US—Handout, AMERICAN ENTERPRISE INSTITUTE - AEI, <https://www.aei.org/multimedia/chinese-investments-us-handout/> (last visited Feb 22, 2024).
- ³⁸ The White House, *G7 Hiroshima Leaders' Communiqué*, THE WHITE HOUSE (2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communicue/> (last visited Feb 22, 2024).
- ³⁹ The White House, *FACT SHEET: President Biden Announces New Actions to Strengthen America's Supply Chains, Lower Costs for Families, and Secure Key Sectors*, THE WHITE HOUSE (2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/27/fact-sheet-president-biden-announces-new-actions-to-strengthen-americas-supply-chains-lower-costs-for-families-and-secure-key-sectors/> (last visited Feb 22, 2024).
- ⁴⁰ Jenna McLaughlin, *Chinese-Made Cranes at U.S. Ports May Pose a National Security Threat*, NPR, Feb. 21, 2024, <https://www.npr.org/2024/02/21/1232998691/chinese-made-cranes-at-u-s-ports-may-pose-a-national-security-threat> (last visited Aug 14, 2024).
- ⁴¹ The White House, *FACT SHEET: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports*, THE WHITE HOUSE (2024), <https://www.whitehouse.gov/briefing-room/statements->

-
- releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/ (last visited Feb 24, 2024).
- ⁴² ABB joins ZPMC in developing overseas port service business, NEWS (2014), <https://new.abb.com/news/detail/45497/abb-joins-zpmc-in-developing-overseas-port-service-business> (last visited Feb 23, 2024).
- ⁴³ Crane Systems | TMEIC, (2017), https://www.tmeic.com/sites/default/files/assets/articles/ZPMC_Orders_TMEIC_Crane_Automation_Systems.pdf (last visited Feb 23, 2024).
- ⁴⁴ Siemens technology for Africa's first automated container terminal, <https://press.siemens.com/global/en/pressrelease/siemens-technology-africas-first-automated-container-terminal> (last visited Aug 14, 2024).
- ⁴⁵ China Select Committee and Committee on Homeland Security staff interviews with Crane manufacturers.
- ⁴⁶ U.S. DEP'T OF HOMELAND SEC., International Ship and Port Facility Security Code and aritime Transportation Security Act, <https://www.dco.uscg.mil/ISPS-MTSA/> (last visited Jan 22, 2024).
- ⁴⁷ Office of Maritime Security | MARAD, <https://www.maritime.dot.gov/ports/office-security/office-maritime-security> (last visited Jan 22, 2024).
- ⁴⁸ Press Release, Cybersecurity & Infrastructure Security Agency, CISA Releases the Marine Transportation System Resilience Assessment Guide | CISA, (2023), <https://www.cisa.gov/news-events/news/cisa-releases-marine-transportation-system-resilience-assessment-guide> (last visited Jan 22, 2024).
- ⁴⁹ OFFICE OF THE INSPECTOR GENERAL - AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF MARITIME TERRORISM THREAT, (2019), <https://oig.justice.gov/reports/2019/a1918.pdf>.
- ⁵⁰ U.S. DEP'T OF TRANSP., MARITIME SECURITY PROGRAM FLEET 2024 | MARAD, [HTTPS://WWW.MARITIME.DOT.GOV/NATIONAL-SECURITY/STRATEGIC-SEALIFT/MARITIME-SECURITY-PROGRAM-FLEET-2024](https://www.maritime.dot.gov/national-security/strategic-sealift/maritime-security-program-fleet-2024) (LAST VISITED JAN 22, 2024).
- ⁵¹ National Port Readiness Network (NPRN), U.S. DEPARTMENT OF TRANSPORTATION MARITIME ADMINISTRATION. <https://www.maritime.dot.gov/ports/national-port-readiness-network-nprn> (last visited Mar. 28, 2024).
- ⁵² House, *supra* note 41.
- ⁵³ ICM20: World's largest crane manufacturers, CRANE & TRANSPORT BRIEFING (2023), <https://www.cranebriefing.com/news/icm20-world-s-largest-crane-manufacturers/8033529.article> (last visited Mar 7, 2024).
- ⁵⁴ SHANGHAI ZHENHUA HEAVY INDUSTRIES CO., LTD. ANNUAL REPORT, (2022), <https://q.stock.sohu.com/newpdf/202354741674.pdf>.
- ⁵⁵ DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA, U.S. DEPARTMENT OF DEFENSE, <https://www.defense.gov/News/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/> (last visited Feb 24, 2024).
- ⁵⁶ 2020 SEMI-ANNUAL REPORT [上海振华重工 (集团) 股份有限公司 2020年半年度报告], (2020), https://static.sse.com.cn/disclosure/listedinfo/announcement/c/2020-08-29/600320_20200829_2.pdf.
- ⁵⁷ TENDER NOTICE [招标公告], (2019), <https://cn.zpmc.com/Img/zhaobiao/201906251643155944379.pdf>.
- ⁵⁸ INITIAL PUBLIC OFFERING PROSPECTUS, (2020), http://static.sse.com.cn/disclosure/listedinfo/announcement/c/2020-08-12/605123_20200812_1.pdf.
- ⁵⁹ Tim Reiterman, *Cranes Lift Upstart Above Competition*, LOS ANGELES TIMES (2002), <https://www.latimes.com/archives/la-xpm-2002-jan-27-fi-cranes27-story.html> (last visited Aug 14, 2024).
- ⁶⁰ A Late Bloomer: ZPMC CEO Guan Tongxian, HARVARD BUSINESS PUBLISHING, <https://hbsp.harvard.edu/product/TU0042-PDF-ENG> (last visited Feb 25, 2024).
- ⁶¹ ZPMC Board Members, ZPMCMED.COM, <https://zpmcmed.com/corporate/zpmc-board-members> (last visited Feb 25, 2024).
- ⁶² Exercise demonstrates PLA Army Aviation ability to use commercial ships as temporary flight decks, JANES.COM, <https://www.janes.com/defence-news/news-detail/exercise-demonstrates-pla-army-aviation-ability-to-use-commercial-ships-as-temporary-flight-decks> (last visited Feb 29, 2024).
- ⁶³ *Id.*

-
- ⁶⁴ China using civilian ships to enhance navy capability, reach, AP NEWS (2022), <https://ap-news.com/article/space-launches-taiwan-science-technology-asia-e8b45f49d3d29851210983d0a399ccba> (last visited Feb 29, 2024).
- ⁶⁵ Simon Rabinovitch, *China Navy Plots Course to Stock Market*, (2013), <https://www.ft.com/content/4f27d80a-1abb-11e3-a605-00144feab7de> (last visited Feb 25, 2024).
- ⁶⁶ ZPMC plans to invest 1.9 billion yuan in the purchase of ships_信德海事网-专业海事信息咨询服务平台, <https://www.xindemarinenews.com/en/market/2023/0526/48083.html> (last visited Mar 2, 2024).
- ⁶⁷ Proprietary trade records made available to Committee staff. (January 1, 2023).
- ⁶⁸ *Id.*
- ⁶⁹ Treasury Sanctions Elites and Companies in Economic Sectors that Generate Substantial Revenue for the Russian Regime, U.S. DEPARTMENT OF THE TREASURY (2024), <https://home.treasury.gov/news/press-releases/jy0905> (last visited Feb 25, 2024).
- ⁷⁰ Chinese Engineers Are Keeping Russia’s Metal Furnaces Firing, BLOOMBERG.COM, Jan. 28, 2024, <https://www.bloomberg.com/news/articles/2024-01-28/china-s-engineers-are-keeping-russia-s-metal-furnaces-firing> (last visited Aug 14, 2024).
- ⁷¹ Hengan Jiaxin (Beijing) Technology Co., Ltd. – Builder of national cyberspace security basic capabilities and leader of cyberspace security ecosystem, (2021), <https://web.archive.org/web/20211026002346/http://eversec.com.cn/partner/> (last visited Aug 21, 2024).
- ⁷² Ryan Fedasiuk, Jennifer Merlot & Ben Murphy, *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence*, CENTER FOR SECURITY AND EMERGING TECHNOLOGY, <https://cset.georgetown.edu/publication/harnessed-lightning/> (last visited Aug 20, 2024).
- ⁷³ This investment was made by then-Sequoia arm Sequoia Capital China. In 2023, Sequoia split off its international investing arms and the resulting PRC entity rebranded as HongShan. Sequoia China Rebranding Is High-Stakes Leadership Test, BLOOMBERG.COM, Nov. 9, 2023, <https://www.bloomberg.com/news/articles/2023-11-09/sequoia-china-rebranding-is-high-stakes-leadership-test> (last visited Mar 2, 2024).
- ⁷⁴ Viswanatha, Lubold, and O’Keeffe, *supra* note 6.
- ⁷⁵ DISRUPTION DEFINED: ZPMC, (2018), <https://www.youtube.com/watch?v=QKjqBlJhRKE> (last visited Mar 2, 2024).
- ⁷⁶ *Id.*
- ⁷⁷ Chinese and foreign enterprises explore dual strategies under Belt and Road framework - Global Times, <https://www.globaltimes.cn/page/201904/1148012.shtml> (last visited Aug 15, 2024).
- ⁷⁸ Navis, ZPMC, Microsoft China and Moffatt & Nichol to Explore Potential Business Opportunities, *Turnkey Solution for Automation*, (2017), <https://www.businesswire.com/news/home/20171115006462/en/Navis-ZPMC-Microsoft-China-and-Moffatt-Nichol-to-Explore-Potential-Business-Opportunities-Turnkey-Solution-for-Automation> (last visited Mar 2, 2024).
- ⁷⁹ Microsoft, *Port Machinery Manufacturer ZPMC Transforms Its Business with Azure IoT*, CODEPROJECT (2017), <https://www.codeproject.com/Articles/1193764/Port-machinery-manufacturer-ZPMC-transforms-its> (last visited Aug 5, 2024).
- ⁸⁰ Pointe Bello | Insights | Beijing’s backdoors into infrastructure and technology, POINTE BELLO, <https://www.pointebello.com/insights/reserved-interfaces> (last visited Mar 2, 2024).
- ⁸¹ Laurie Chen & Laurie Chen, *China Broadens Law on State Security to Include “Work Secrets,”* REUTERS, Feb. 28, 2024, <https://www.reuters.com/world/china/china-broadens-law-state-secrets-include-work-secrets-2024-02-28/> (last visited Aug 15, 2024).
- ⁸² Full text of the Cybersecurity Law (Draft)_Chinese National Congress, https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (last visited Mar 2, 2024).
- ⁸³ RecordedFuture, *China’s Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers Over Foreign Technology* | Recorded Future, <https://www.recordedfuture.com/research/china-cybersecurity-law> (last visited Aug 15, 2024).
- ⁸⁴ Multi-Level Protection Scheme (MLPS) 2.0 | Protiviti Hong Kong SAR, <https://www.protiviti.com/hk-en/whitepaper/chinas-cybersecurity-law-multiple-level-protection-scheme> (last visited Mar 2, 2024).

-
- ⁸⁵ Kevin Townsend, *China Police Get Power to Remotely “Inspect” Company Networks in China*, SECURITYWEEK (2019), <https://www.securityweek.com/china-police-get-power-remotely-inspect-company-networks-china/> (last visited Mar 2, 2024).
- ⁸⁶ China’s cyber security law rattles multinationals, <https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996> (last visited Mar 2, 2024).
- ⁸⁷ ZoomEye Search - ZPMC and China, <https://www.zoomeye.org/searchResult?q=zpmc%20%2Bcountry:%22CN%22&t=all> (last visited Mar 3, 2024).
- ⁸⁸ Shodan Search, <https://www.shodan.io/search?query=zpmc> (last visited Mar 3, 2024).
- ⁸⁹ Multi-Level Protection Scheme (MLPS) 2.0 | Protiviti Hong Kong SAR, *supra* note 84.
- ⁹⁰ China National Vulnerability Database (CNVD), CNVD (2023), <https://archive.ph/o54ok> (last visited Mar 3, 2024).
- ⁹¹ The Chinese Private Sector Cyber Landscape, MARGIN RESEARCH (2022), <https://margin.re/2022/04/the-chinese-private-sector-cyber-landscape/> (last visited Mar 3, 2024).
- ⁹² Briefing from U.S. government agency to Committee staff. (January 11, 2024).
- ⁹³ U.S. seaport contract document with ZPMC. (December 19, 2023).
- ⁹⁴ Briefing from U.S. seaport to Committee staff. (January 4, 2024).
- ⁹⁵ *Id.*
- ⁹⁶ U.S. government agency, *supra* 89.
- ⁹⁷ U.S. Seaport, *supra* note 91.
- ⁹⁸ U.S. government agency, *supra* 89.
- ⁹⁹ U.S. Seaport, *supra* note 91.
- ¹⁰⁰ *Id.*
- ¹⁰¹ Briefing from industry and security stakeholders to Committee staff. (March 7, 2024).
- ¹⁰² Email from U.S. government agency to Committee staff. (January 11, 2024).
- ¹⁰³ Letter from ZPMC to Committee staff. (April 7, 2024).
- ¹⁰⁴ Briefing from Senior ABB staff to Representative Gimenez. (February 7, 2024).
- ¹⁰⁵ Briefings from ship-to-shore crane internal component manufacturers to Committee staff. (February 22 and 26, 2024).
- ¹⁰⁶ ABB SOLUTIONS FOR THE U.S. FEDERAL GOVERNMENT, https://new.abb.com/docs/librariesprovider15/campaigns/abb_federal-government-brochure-2022.pdf?sfvrsn=7fbc309_2.
- ¹⁰⁷ ABB, document submission to Committees (.).
- ¹⁰⁸ ABB wins \$65 million in orders for crane systems, NEWS (2007), <https://new.abb.com/news/detail/13293/abb-wins-65-million-in-orders-for-crane-systems> (last visited Mar 5, 2024).
- ¹⁰⁹ *Id.*
- ¹¹⁰ ABB And ZPMC To Jointly Develop Energy Efficient Propulsion Solutions For Deep Sea Offshore Vessels, <https://www.plantaautomation.com/doc/abb-and-zpmc-to-jointly-develop-energy-0002> (last visited Mar 5, 2024).
- ¹¹¹ ABB, ZPMC to Develop Efficient Propulsion, MARINELINK (2009), <https://www.marinelink.com/news/propulsion-efficient330334> (last visited Mar 5, 2024).
- ¹¹² Azipod® electric propulsion | ABB Marine & Ports, <https://new.abb.com/marine/systems-and-solutions/azipod> (last visited Mar 5, 2024).
- ¹¹³ ABB joins ZPMC in developing overseas port service business, *supra* note 42.
- ¹¹⁴ *Id.*
- ¹¹⁵ *Id.*
- ¹¹⁶ Committee staff meeting with ABB, February 7, 2024.
- ¹¹⁷ ABB joins ZPMC in developing overseas port service business, *supra* note 42.
- ¹¹⁸ Multinational tech firm ABB hit by Black Basta ransomware attack, BLEEPINGCOMPUTER, <https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/> (last visited Mar 5, 2024).
- ¹¹⁹ More than \$100 million in ransom paid to Black Basta gang over nearly 2 years, <https://therecord.media/blackbasta-ransom-payments> (last visited Mar 5, 2024).
- ¹²⁰ MANDIANT THREAT ACTIVITY ALERT: WEDNESDAY, NOV. 15, 2023, (2023).

¹²¹ Communist Chinese Military Companies Listed Under E.O. 13959 Have More Than 1,100 Subsidiaries, UNITED STATES DEPARTMENT OF STATE, <https://2017-2021.state.gov/communist-chinese-military-companies-listed-under-e-o-13959-have-more-than-1100-subsidiaries/> (last visited Mar 5, 2024).

¹²² ABB meeting with Committee staff. (Jul 18, 2023).

¹²³ *Id.*

¹²⁴ ABB documents provided to Committee staff. (Sep 5, 2023)

¹²⁵ Chairmen Green, Gallagher, Gimenez, and Pfluger Request Testimony from Swiss Company with Concerning Ties to Chinese State-Owned Enterprises – Committee on Homeland Security, <https://homeland.house.gov/2024/01/18/chairmen-green-gallagher-gimenez-and-pfluger-request-testimony-from-swiss-company-with-concerning-ties-to-chinese-state-owned-enterprises/> (last visited Aug 21, 2024).

¹²⁶ Letter from ZPMC to the Committee staff (Mar 21, 2024).

¹²⁷ Briefings from ship-to-shore crane internal component manufacturers to Committee staff. (February 22 and 26, 2024).

¹²⁸ ABB meeting with Committee staff. (Sep 29, 2023).

¹²⁹ Briefing from Senior ABB staff to Representative Gimenez. (February 7, 2024).

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ Siemens meeting with Committee staff. (Feb 22, 2024).

¹³⁶ TMEIC meeting with Committee staff. (Feb 26, 2024).

¹³⁷ Ship-to-Shore Crane | Konecranes USA, <https://www.konecranes.com/en-us/port-equipment-services/container-handling-equipment/konecranes-ship-to-shore-cranes> (last visited Mar 10, 2024).

¹³⁸ Ship to Shore Container Cranes, <https://www.liebherr.com/en/int/products/maritime-cranes/port-equipment/container-bridges/ship-to-shore-container-cranes.html> (last visited Mar 10, 2024).

¹³⁹ Georgia Ports Authority orders a fleet of 22 Konecranes container cranes | Corporate press releases | Konecranes USA, <https://www.konecranes.com/en-us/press/releases/2022/georgia-ports-authority-orders-fleet-of-22-konecranes-container-cranes> (last visited Mar 10, 2024).

¹⁴⁰ Liebherr Container Cranes delivers in the US, <https://www.ajot.com/news/liebherr-container-cranes-delivers-in-the-us> (last visited Mar 10, 2024).

¹⁴¹ Liebherr in the People's Republic of China, <https://www.liebherr.com/en/usa/about-liebherr/liebherr-worldwide/china/liebherr-in-china.html> (last visited Mar 11, 2024).

¹⁴² Konecranes supports Jingjin Equipment's business expansion with 35-crane order | Trade press releases | Konecranes, <https://www.konecranes.com/press/releases/2023/konecranes-supports-jingjin-equipments-business-expansion-with-35-crane-order> (last visited Mar 11, 2024).

¹⁴³ Katherine Schulte, *Biden Executive Order on Chinese Cranes Affects Port of Va.*, VIRGINIA BUSINESS (Feb. 21, 2024), <https://www.virginiabusiness.com/article/biden-executive-order-on-chinese-cranes-affects-port-of-va/> (last visited Mar 10, 2024).

¹⁴⁴ House Homeland, China Select Committee Republicans Demand Answers from CCP-Backed Company Operating at U.S. Ports Amid Shocking Joint Investigation Findings – Committee on Homeland Security, <https://homeland.house.gov/2024/03/07/house-homeland-china-select-committee-republicans-demand-answers-from-ccp-backed-company-operating-at-u-s-ports-amid-shocking-joint-investigation-findings/> (last visited Apr 29, 2024).

¹⁴⁵ Letter from ZPMC to the Committee staff (Mar 21, 2024).

¹⁴⁶ Letter from ZPMC to the Committee staff (Apr 7, 2024).

¹⁴⁷ *Id.*, p. 6.

¹⁴⁸ *Id.*, p. 2.

¹⁴⁹ *Id.*, p. 4.

¹⁵⁰ *Id.*, p. 6.

¹⁵¹ *Id.*, p. 5.

¹⁵² *Id.*

¹⁵³ Letter from ZPMC to the Committee staff (Jun 4, 2024)

¹⁵⁴ *Id.*, p. 3.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*, p. 4.

¹⁵⁸ *Id.*

¹⁵⁹ House, *supra* note 41.

¹⁶⁰ ANDREW TILGHMAN, *Guam: Defense Infrastructure and Readiness*, (2023), <https://crsreports.congress.gov/product/pdf/R/R47643> (last visited Mar 12, 2024).

¹⁶¹ TOPIC: DEFENSE OF GUAM AND THE COMMONWEALTH OF THE NORTHERN MARIANA ISLANDS (CNMI), (2023), https://www.pacom.mil/LinkClick.aspx?fileticket=UUf_gsxkuPQ%3D&portalid=55 (last visited Mar 12, 2024).

¹⁶² U. S. Government Accountability Office, *The Evolving U.S. Military Presence on Guam* | U.S. GAO, <https://www.gao.gov/blog/2017/06/15/the-evolving-u-s-military-presence-on-guam> (last visited Mar 12, 2024).

¹⁶³ Admin, *Infrastructure Gaps at the Port Posing a Setback to Guam's Military Readiness*, PACTIMES (2023), <https://www.pacificislandtimes.com/post/infrastructure-gaps-at-the-port-posing-a-setback-to-guam-s-military-readiness> (last visited Mar 12, 2024).

¹⁶⁴ Microsoft Threat Intelligence, *Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques*, MICROSOFT SECURITY BLOG (2023), <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/> (last visited Mar 12, 2024).

¹⁶⁵ Andy Greenberg, *China Hacks US Critical Networks in Guam, Raising Cyberwar Fears*, WIRED, <https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/> (last visited Mar 12, 2024).

¹⁶⁶ Jose Leon, Regular Meeting of the Board of Directors, (2016), https://www.portofguam.com/sites/default/files/112316_pag_boardmeetingmaterials.pdf (last visited Mar 12, 2024).

¹⁶⁷ Briefing from Port of Guam to Committee staff. (June 29, 2024).