TEXAS A&M UNIVERSITY GALVESTON CAMPUS

MANAGEMENT OF PORT FACILITIES AND INFRASTRUCTURE

4. Safety, Security, and Cybersecurity

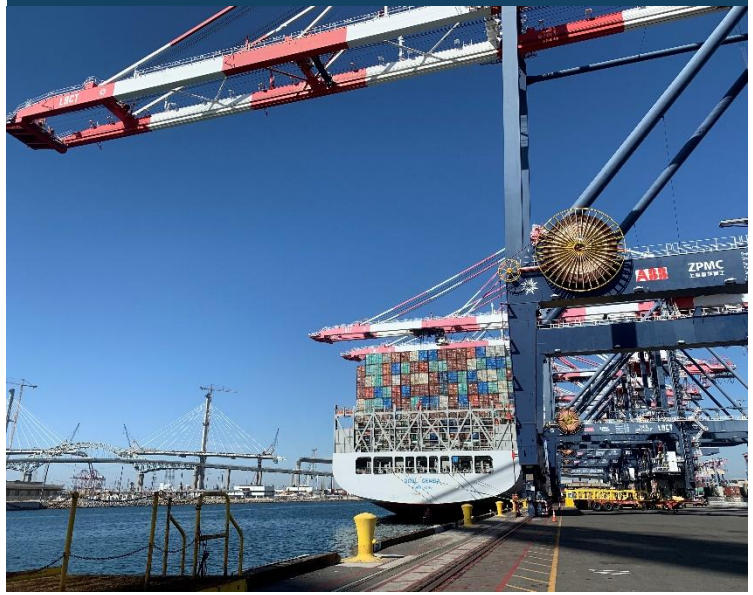
MARA 616

Professor: Dr. Jean-Paul Rodrigue

Table of Contents

TEXAS A&M UNIVERSITY GALVESTON CAMPUS

MANAGEMENT OF PORT FACILITIES AND INFRASTRUCTURE



A. Typology of Crime Affecting Ports

Read this section

Trafficking of Illicit or Counterfeit Goods

- Illicit goods
  - Ports can be used to export or import goods that are judged to be illicit by global or national organizations (customs).
  - Stolen goods, such as cars.
  - Embargoed goods that, under normal circumstances, would be part of regular trade networks.
  - Oil or grains may be embargoed due to conflict or geopolitical tensions.
  - Ports can act as illicit distribution platforms.

Stolen Car in a Shipping Container bound for Ghana

Trafficking of Illicit or Counterfeit Goods

- Drug trafficking
  - Major entry and exit points for illegal drugs.
  - Hidden within shipping containers or other bulk cargo.
  - Drug cartels may bribe or intimidate port officials, customs agents, dock workers, or security personnel to help drugs pass through undetected, or to facilitate the collection of drugs in port areas.
- Trafficking of counterfeit goods
  - Common entry points for smuggling counterfeit goods.
  - Fake luxury items, pharmaceuticals, electronics, and industrial products.
  - Infringe on intellectual property rights.
  - Counterfeit goods, particularly in sectors like pharmaceuticals, toys, or automotive parts, pose risks to consumer safety and health.

Trafficking of Illicit or Counterfeit Goods

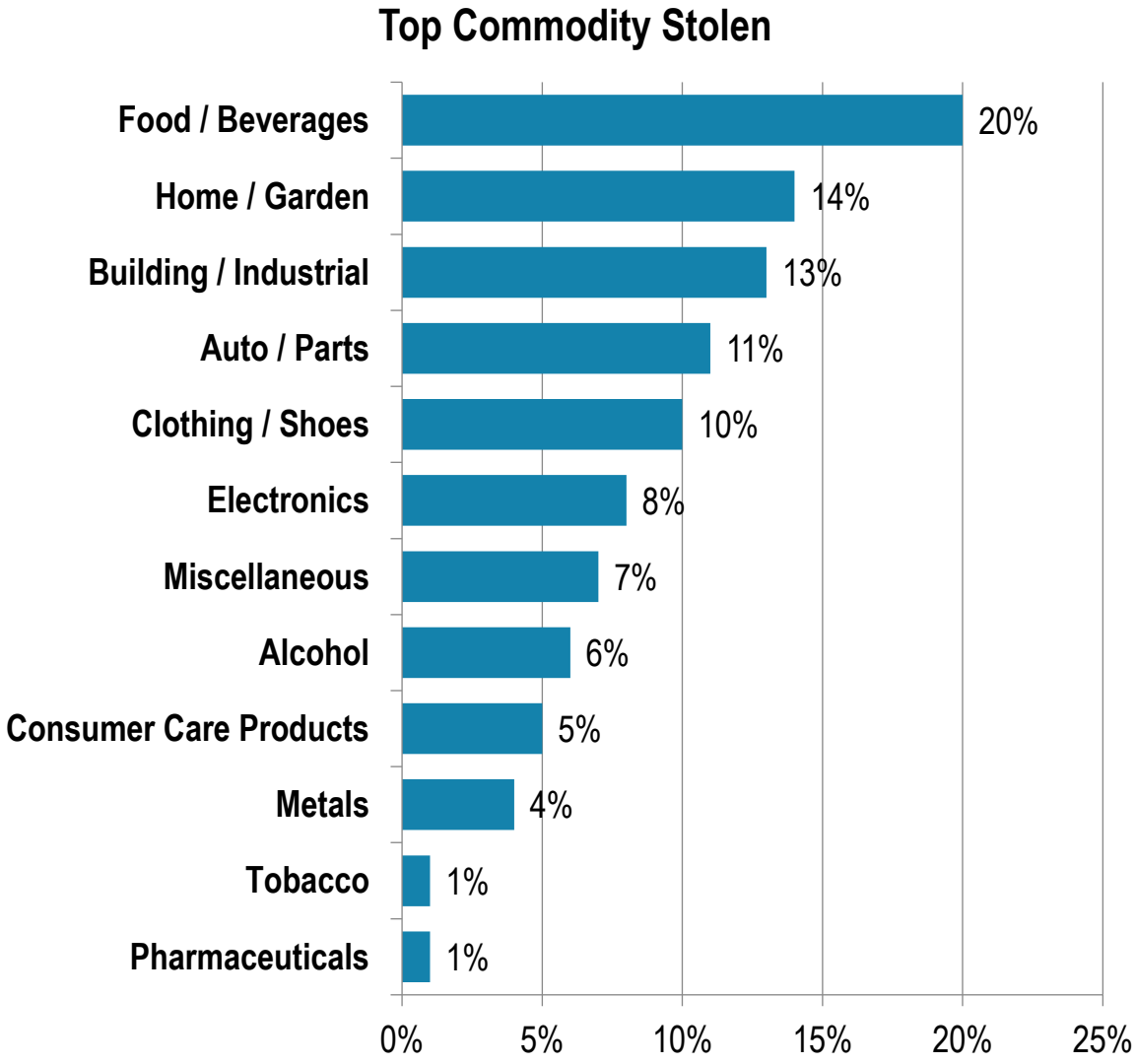
- Arms trafficking
  - Entry points for illegal weapons and ammunition, often concealed within regular shipments.
  - Firearms, explosives, and military-grade weaponry.
  - Forged or fake shipping documents to obscure the true contents of containers.
  - Terrorist organizations or organized crime groups.
  - During regional conflicts, the parties involved try to access weapon supplies, leading to trafficking.
- Illegal wildlife and fish trafficking
  - Trafficking endangered wildlife and illegal animal products, like ivory or exotic pets.
  - Illegal fishing industry; forged documentation to disguise its origin.
- Waste trafficking
  - Hazardous waste exported to countries with looser environmental regulations.

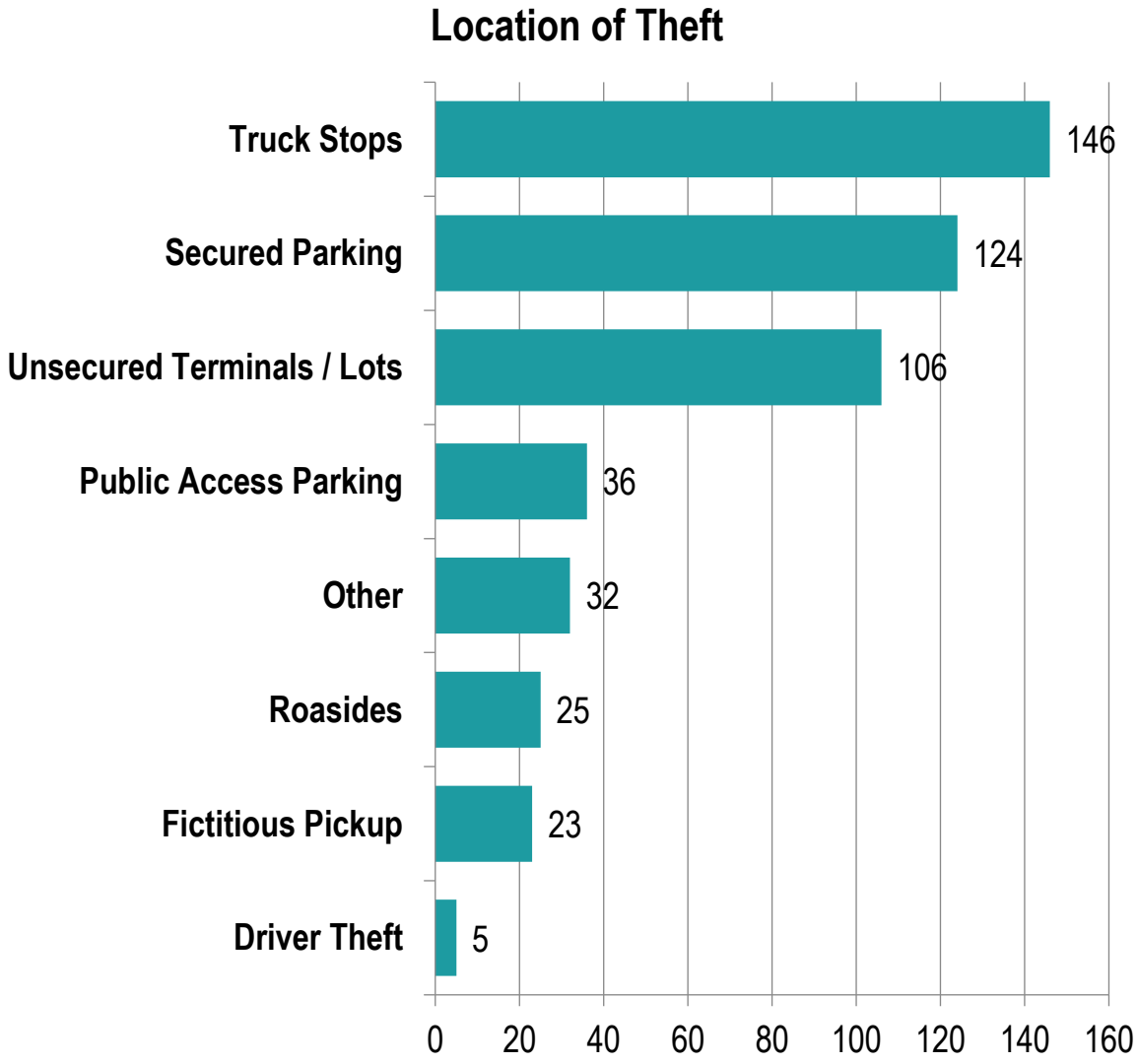
Typology of Crime Affecting Ports

- Cargo theft
  - Vulnerable to cargo theft.
  - Criminal networks often target high-value cargo (electronics, luxury goods, pharmaceuticals, cars, and consumer products).
  - Involves inside knowledge, with criminals bribing or collaborating with port workers or truck drivers.
  - Hijack trucks or other transport modes, leaving ports or even intercept entire containers before they reach their final destination.
- Trade-Based Money Laundering (TBML)
  - Laundering money by manipulating shipping documents, invoices, and the valuation of goods.
  - Shell companies create fake cargo shipments, which can facilitate the movement of illegal funds.
  - Underreport the value of goods to evade customs duties and taxes.
  - Misclassifying cargo to lower tax rates or avoid import restrictions.

Thefts by Type of Cargo and Location, United States, 2016

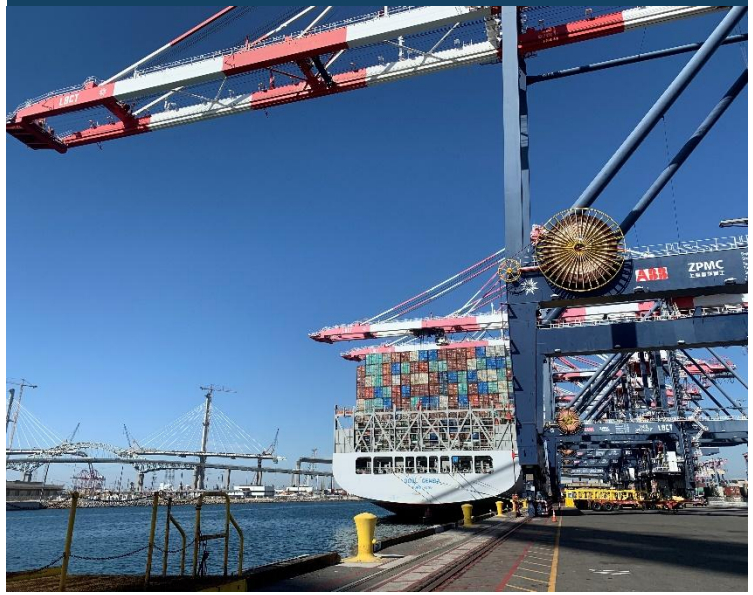
Read this content





TEXAS A&M UNIVERSITY GALVESTON CAMPUS

MANAGEMENT OF PORT FACILITIES AND INFRASTRUCTURE



B. Tackling Security in Ports

Read this section

Context

- Strong culture of security in ports
  - Originates from the protection against cargo theft.
  - Most ports have their own police and security forces.
- Events of September 11, 2001
  - Transportation facilities perceived at risk.
  - Physical protection of terminal facilities against unauthorized entry and intentional damage.
- New expansion phase of port security (2010s)
  - Include cybersecurity concerns.
  - Ports are adapting to security concerns and threat changes.

Port Security

- Advanced remote sensing technologies
  - CCTV, motion sensors, container-scanning technologies, drones (flying and submersible), biometric access control, and automated monitoring.
- Smart fencing (geofencing)
  - Setting virtual geographical boundaries around facilities.
  - Combined with AIS data generated ships or RFID installed on containers to trigger a notification.
  - Entering or exiting a geofenced port area triggers a notification.
  - Individual assets, such as containers, can also be tracked, including through the mobile device of a truck driver.
  - This allows for a better visibility of maritime transport and supply chains.

Geofencing at Port Terminals

Read this content

Transportation Worker Identification Credential (TWIC)

- Maritime Transportation Security Act (2002)
  - Maritime facilities such as terminals considered essential for national security.
  - Areas to be fenced and restricted (port secure area).
  - Tamper-resistant biometric credentials for maritime workers.
  - Mainly for merchant mariners, port facility employees, longshoremen, and truck drivers.
  - Each undergoes a security threat assessment (TSA background check).
- Goals
  - Authorized individuals for unescorted access to port secure areas.
  - Define eligibility for unescorted access to port secure areas.
  - Unauthorized individuals are denied unescorted access to port secure areas.

International Ship and Port Facility Security Code (ISPS Code)

- International Ship and Port Facility Security Code (ISPS Code)
  - USA: “Maritime Transportation Security Act of 2002” (MTSA); Implemented July 2004.
  - IMO adopted the ISPS Code in December of 2002 as part of the 1974 Safety of Life at Sea Convention (SOLAS),
  - Goal is to enhance maritime security on board ships and at ship/port interface areas.
- Secure port areas
  - Fenced and monitored.
  - Access cannot take place without identification.
- Compliance
  - Mandatory for ships to comply with the ISPS Code.
  - Contains detailed security-related requirements for Governments, port authorities, and shipping companies (mandatory).
  - Three levels (1 to 3). Normal to emergency (imminent attack).

International Ship and Port Facility Security Code (ISPS Code)

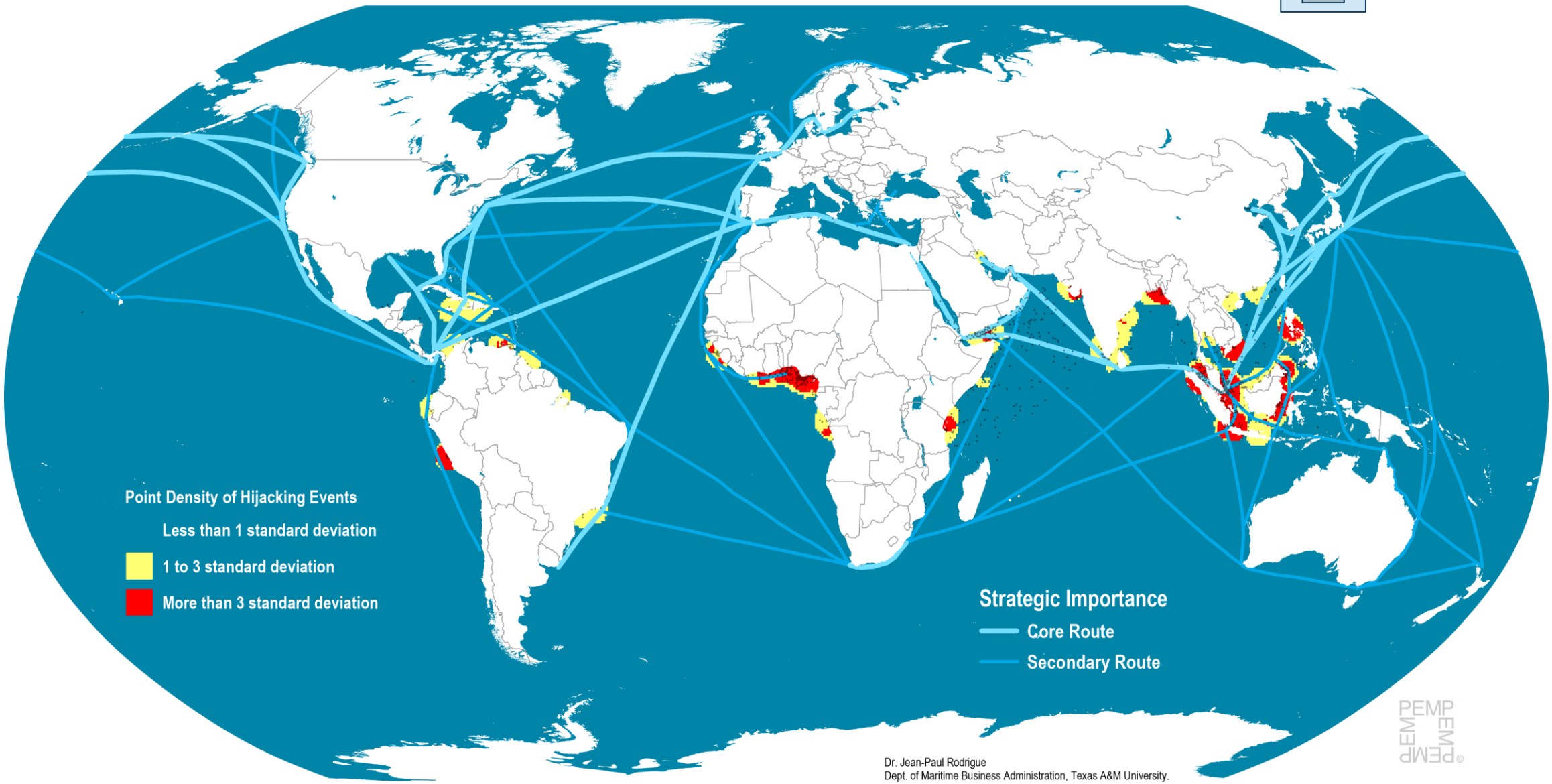
- ISPS Code has a strong interface between the port control facility and the port facility.
- When a ship is at a port or is proceeding to a port of a contracting government:
  - Right to exercise various control and compliance measures with respect to that ship.
  - Ships may be subject to port state control inspections.
  - Authorities may request information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port.
  - Port entry may be denied.

ISPS Code: Port Certificate of Compliance

- ISPS Code has an equal responsibility on both the ship and port
  - Contracting government has to select the port facilities.
  - A Port Facility Security Officer (PFSO) has to be appointed and trained.
  - A Port Facility Security Assessment (PFSA) has to be made and agreed by the contracting government.
  - A Port Facility Security Plan (PFSP) must be produced based on the recommendations of the PFSA.
  - The plan has to be implemented and tested.
  - If all is correct, the port is issued a Certificate of Compliance.

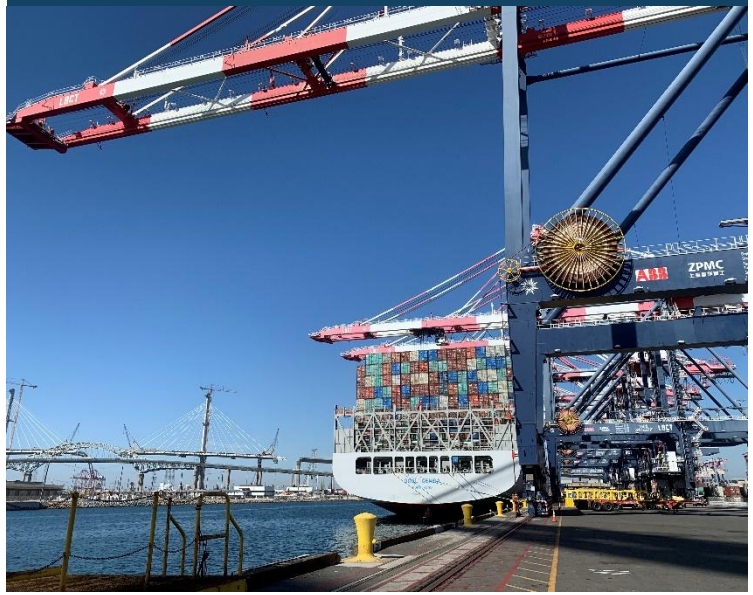
Global Maritime Piracy, 1993-2020

Read this content



TEXAS A&M UNIVERSITY GALVESTON CAMPUS

MANAGEMENT OF PORT FACILITIES AND INFRASTRUCTURE



C. Ports and Military Defense

Read this section

Context

- Recurring geopolitical tensions
  - Some regions around the world are regularly confronted with security issues due to military conflicts and security risks.
  - Renewed attention for investments in defense.
  - Attention to the role of seaports for national security.
  - Port infrastructure, location, and capacity at the foundation for national or regional defense.
  - Role of ports in military logistics:
    - Increases the threat of possible forms of undermining the existing infrastructure and superstructure
    - Cyber attacks, physical sabotage, and targeted attacks by air, water, or land.

The Role of Ports in Military Defense

- Naval bases
  - Near critical locations in the international maritime network:
    - Djibouti near the Red Sea and the Gulf of Aden.
    - Domestic ports (e.g., San Diego and Norfolk as homeports for the US naval fleet at the US West Coast and US East Coast).
  - Ports in the Persian Gulf and South China Sea have become focal points for naval operations due to their proximity to areas of strategic interest.
  - Presence of a strong naval force at a strategic port can act as a deterrent to adversaries.
  - Ports serve as command hubs where defense operations can be coordinated, managed, and monitored.

Naval Station Norfolk, 2012

Chinese Naval Base, Fiery Cross Reef, Spratly Islands, South China Sea

The Role of Ports in Military Defense

- Reserve fleets and sealift capabilities
  - Can be activated to support national defense and the deployment of troops, materiel, and relief.
  - The United States, through its Department of Transportation, maintains a ready reserve force of about 50 cargo vessels.
- Dry docks and maintenance facilities
  - Play a role in constructing, repairing, and overhauling military vessels.
- Logistical role in facilitating military operations and exercises
  - Joint training and multinational exercises, showcasing allied strength and enhancing interoperability.
  - Large seaports are capable of handling heavy military equipment (like tanks, helicopters, and missiles).
  - Troop deployment or redeployment.
  - Supplies such as fuel, ammunition, food, and medical supplies.

USNS Guan – Rapid Deployment Vessel

The Role of Ports in Military Defense

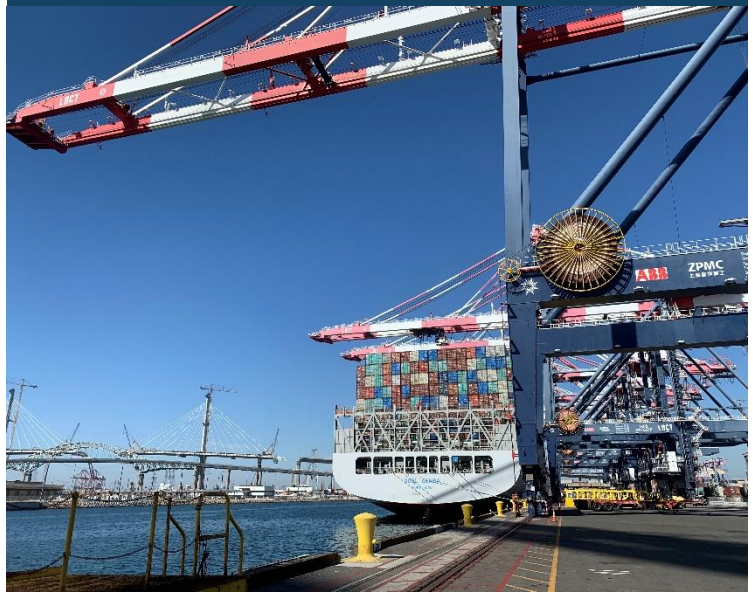
- Coastal defense
  - Batteries, anti-aircraft systems, and fortifications.
  - Mines or other defensive measures can be deployed in harbor approaches to deter hostile ships.
  - Some strategic ports are equipped with systems to detect and counteract submarine and missile threats.
- Protecting critical trade routes
  - Acting as hubs in naval and other operations.
  - Securing international shipping lanes against threats like piracy and terrorism

Coastal Fortifications Protecting Access to New York Harbor

Galveston Coastal Battery, c1940

TEXAS A&M UNIVERSITY GALVESTON CAMPUS

MANAGEMENT OF PORT FACILITIES AND INFRASTRUCTURE



D. Cybersecurity and Ports

Read this section

Context

- Diffusion of information technologies
  - Communication, managerial, and operational considerations.
  - Characteristics, such as digital network access and connectivity, have opened the door to a new range of vulnerabilities and risks.
- Cybersecurity
  - Protection of information technology systems (hardware and software) and their infrastructure from unauthorized access, misuse, and damage.

Vulnerabilities of the Maritime Industry to Cybersecurity

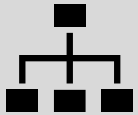
Read this content

TRANSACTIONS

- Transaction-intensive industry.
- Multiple document exchanges.
- Multiple information systems.
- Chain of custody.

ASSET VALUE

- High cargo value.
- Capital-intensive assets (ships, equipment, facilities).
- Limited substitution.



TRANSNATIONALISM

- Represent national interests.
- Multiple jurisdictions of fixed and mobile assets.
- Complex procurement of software and IT.

LIFE CYCLE

- Long life cycle of assets.
- Lagging effect in IT upgrade.
- Legacy systems.

Dimensions of Data Cybersecurity

- Confidentiality
  - Information technologies accessible only to authorized personnel.
  - Layers to confidentiality:
    - Public access (such as a company informational web page).
    - Restricted information (such as financial accounts) only available to key employees in upper management.
- Integrity
  - Information stored and distributed protected from any unauthorized modification or deletion.
  - Data version monitoring and backup systems.
- Availability
  - Information made available at the moment needed to access.
  - Telecommunication systems, such as Wi-Fi, can be compromised and disrupted, impairing operations.
  - Network redundancy allows for mitigating potential disruptions.

Most Common Causes of Cyberattacks

Read this content

Weak/Stolen Credentials

Simple passwords, common passwords, same password for multiple accounts.

Application Vulnerabilities

Technical vulnerability (usually discovered by hackers), slow and inconsistent release of patches.

Malware

Purposely designed software such as keyloggers and ransomware.

Malicious Insiders

Disgruntled employees (recently fired, disciplined or demoted). Still have credentials or physical access.

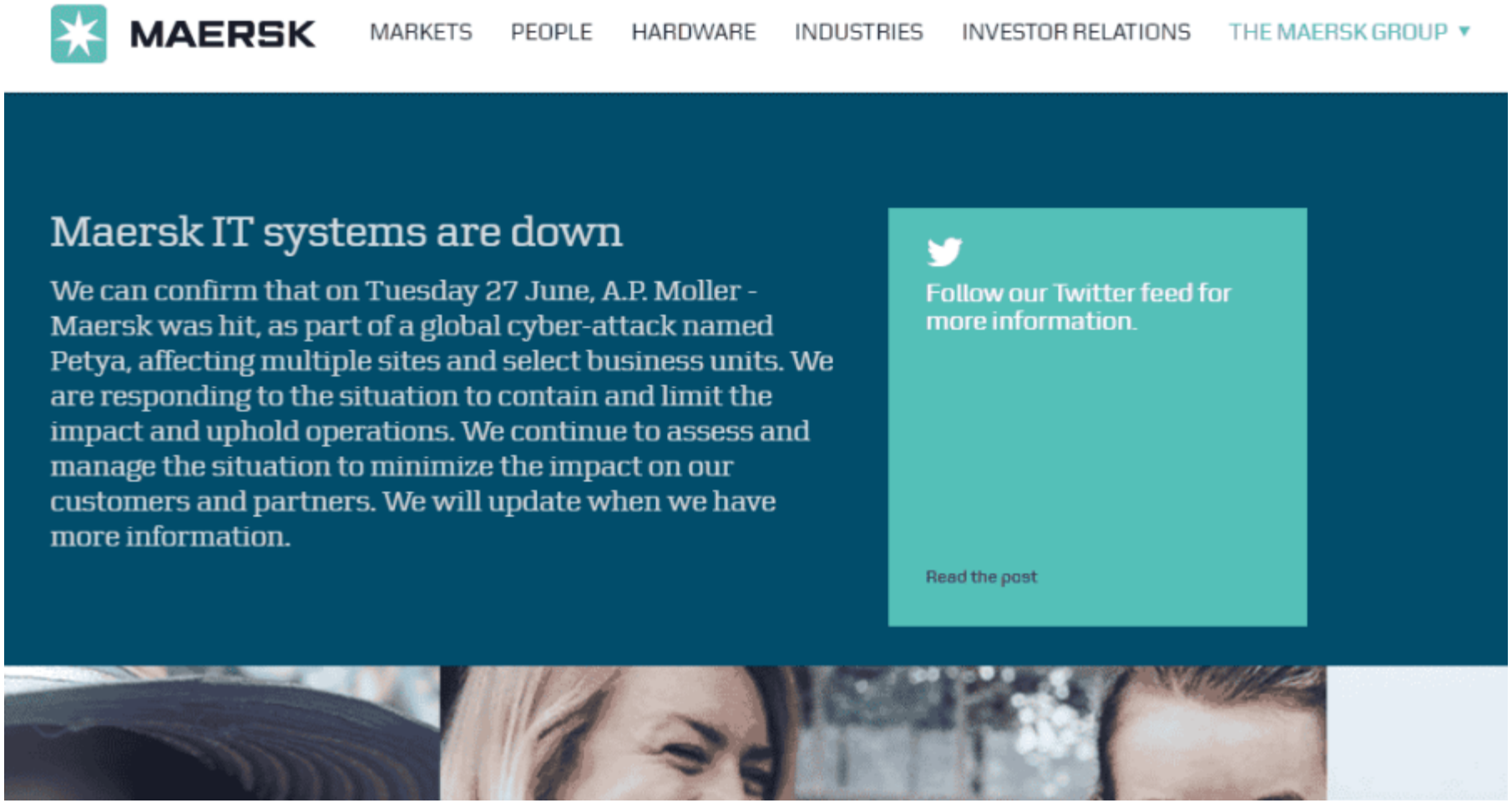
Insider Error

Activate clickbait/phishing, sent wrong file/wrong CC, Lost laptop or USB.

Leading Causes in Ransomware Attacks

Petya Ransomware Cyber-Attack on Maersk, 2017

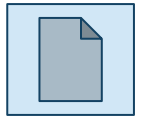
Read this content



Port of Shahid Rajaee (Iran), 2021 Cyber-Attack (Cyber warfare)

Port of Durban Cyber-Attack, 2021 (Ransomware on Terminal Operating System)

Cyber-Resilience Measures for Information Technologies



Read this content

ACCESS CONTROL

- Identity and access management.
- Roles and privilege management.
- Password conventions.
- Multi-factor identification.
- Reviews of accounts and access rights.

DATA SECURITY

- Data encryption protocols.
- Data classification.
- Controls for removable media.
- Disposal of old equipment and media.
- Integrity check for software and firmware.

NETWORK SECURITY

- Network segmentation.
- Firewalls.
- Protection of critical IT systems.
- Remote access (VPN).
- Malware protection.
- System hardening.

OPERATIONAL SECURITY

- Patch and update management.
- Vulnerability monitoring.
- Fraud prevention.
- Cyber intelligence.

Issues of Cyber-Resilience in Ports

- Labor and skill issues
  - Maritime industry competing for IT talent with other industries.
  - Operational and managerial workforce needs to be trained with new sets of skills.
- Software development
  - Software and technologies that can be considered “legacy”.
  - Not designed in circumstances where cybersecurity is an issue.
  - Some terminals use in-house software that is particularly prone to vulnerabilities.
  - Software development undertaken by third parties can be subject to risks such as back-doors.
- Terminal infrastructure
  - Port terminals composed of a multiplicity of information technologies, automated assets, and telecommunication networks.
  - Each represent a potential point of entry for a cyberattack.
  - Terminal infrastructure (ship-to-shore cranes, gantries, trucks) rely on software to operate.
  - Terminal equipment can represent a cybersecurity risk.

Most Common Cyber-Attacks at Ports

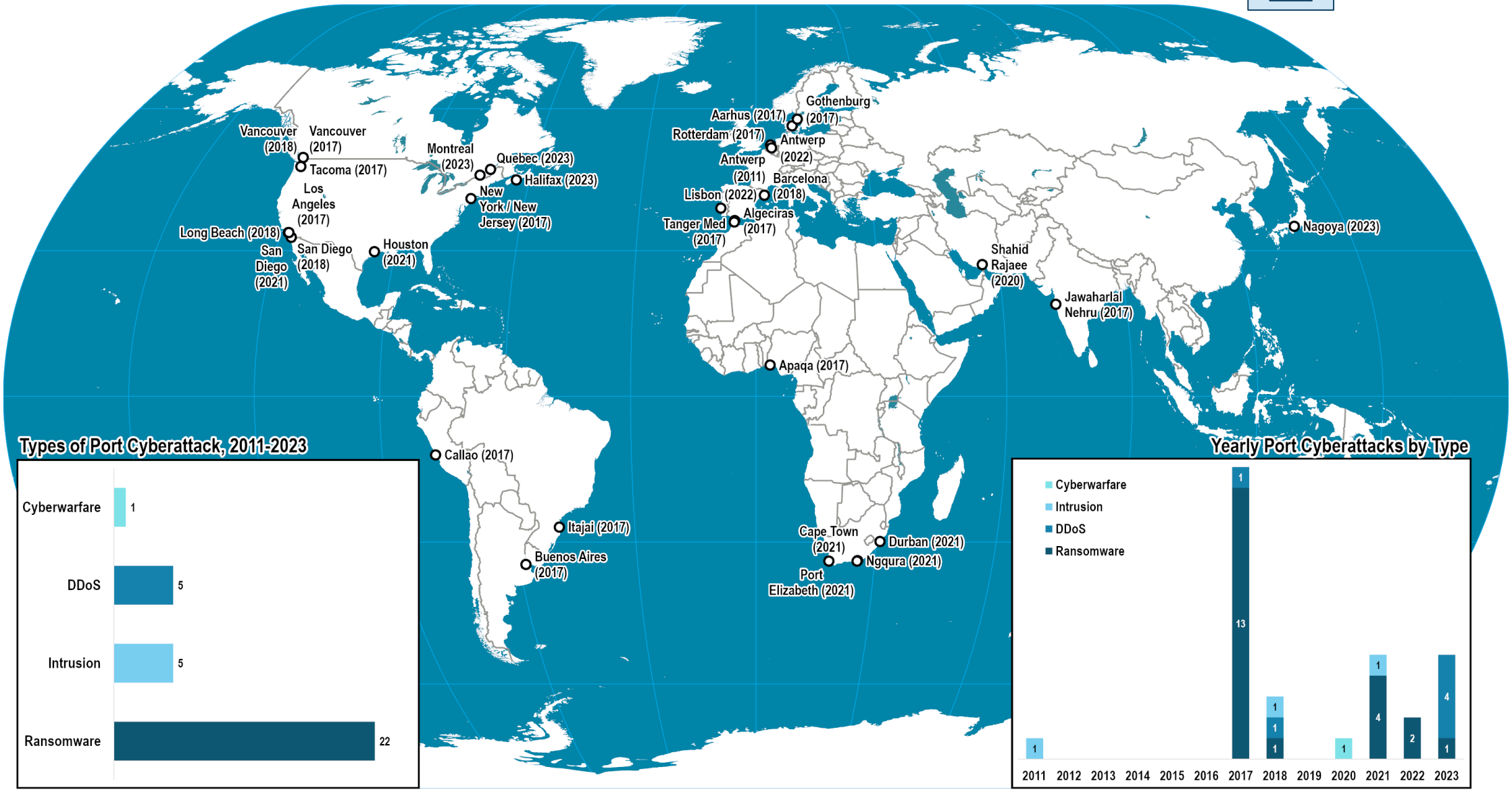
- E-mails
  - Most common vector of a cyberattack.
  - Wide use and diffusion within organizations.
  - Installing malware within the compromised network or stealing login credentials by fooling the recipient into a fake login page.
  - A salient strategy remains a constant and improved monitoring of phishing attempts.
- Denial of service attacks (DDoS).
  - Common in attempts to disrupt networks to extract a ransom or to undermine operations.
  - Networks can be hardened with real-time firewall rules that block IPs subject to suspicious activity.

Most Common Cyber-Attacks at Ports

- Typosquatting
  - Mimics the names of websites.
  - Users are fooled into believing they are using a genuine site and providing, for instance, login credentials and private information.
  - Can be mitigated with firewall rules and rapid take-down notices for typosquatting sites.
- Brute force attacks
  - Used to break in using combinations of well-known passwords across multiple accounts.
  - Mitigated by well-established complex password policies with periodic changes.

Port Cyberattacks, 2011-2023

Read this content



Cybersecurity and Port Resilience

- Trend
  - Growth in the number of attacks but inconsistent breaches.
  - Complex interplay between hackers and port cybersecurity actors.
- Adaptation of the governance structure
  - Entirely new set of risks that have no precedent.
  - Changes in the governance structure with clear roles and chain of authority concerning cybersecurity.
  - Chief cybersecurity officer (CCO) or chief information security officer (CISO).