Module 1: The Maritime Transportation System
Structure, Architecture, and Vulnerabilities
The End-to-End Transportation System

The end-to-end transportation system follows the black arrow. In this illustration, the MTS is embedded in the transportation system. What comprises the MTS?

*Customers and Border Protection
Intermodal Connectors - Interconnecting Different Modes of Transportation

Although a shipyard may be very efficient, there must be ways of connecting the yard to interstate transport, i.e., to roads and rails. These connections are called Intermodal Connectors (IC).
The Maritime Transportation System

The MTS extends from red dashed line to red dashed line, indicated by the red arrow. It includes the Intermodal Connectors (IC). An efficient port must have access to adequate ICs to get goods into and out of the port.
Pipelines – Part of the Transportation System

Pipelines are regulated by the Transportation Security Agency (TSA). Liquified Natural Gas Facilities at Ports are MTSA-regulated. LNG port facilities and vessels are shown.
Natural Gas Transportation System (NGTS)

Summary

- NGTS is an example of Operational Technology (OT), i.e., technology that runs some kind of production, such as manufacturing, electrical grid, LNG processing... (see Module 2).

- Liquification of natural gas reduces volume for storage and transport by 600x for a given amount of energy, making it suitable for transport by ship

- LNG port facilities and vessels are MTSA-regulated and are part of the MTS

- LNG port facilities have been cyber-attacked (see Case Study)
MTS Security Evolution

Transportation security has evolved from crime to counterterrorism to a focus on cybersecurity

• Prior to 9/11/2001, MTS security focused primarily on physical security in smuggling and counterfeiting

• After 9/11, focus shifted to counter-terrorism.

• Now, we are concerned with security from multiple threats (terrorism, crime, warfare) in both the Physical and Cyber domains

• Some Physical protections are important parts of Cybersecurity Plans (Facility and Vessel)

• *Discussion Point: Can you name some?*
Physical Security of MTS Components

Physical Security is implemented across all transportation components

1-Customs Trade, Partnership Against Terrorism
2-Transportation Worker Identification Credential (TWIC)
3-Radio Frequency ID Tag (RFID)
Physical Security Examples

Thermal Imaging – Infrared Camera

Radiation Portal Monitor
Access Control in Physical and Cybersecurity

Access control is a key component of both physical and cybersecurity plans

Physical Access Control
- Keeps unauthorized people (and things) out of places they should not be, \textit{while}
- Allowing authorized people and things to enter areas and systems that they are allowed

Relationship to Cyber:
- Physical access control of server rooms, control rooms, open USB ports...
- Good physical access controls are often first step in a good cybersecurity plan

There is often tension between safety and security, and between security and efficiency. Think of any?
Cybersecurity – Some Definitions

• **Cyber Threat**: A potential action that can harm a computer system or resource

• **Cyber Threat Actor**: An individual or entity that has the capability and intent to execute the threat

• **Vulnerability**: A weakness in a system that can be exploited to enable a successful attack

• **Exploit**: The actions that take advantage of a vulnerability and achieve an intrusion or breach

• **Patch**: Software that, when downloaded, removes some vulnerabilities
Types of Cyber Threat Actors
Who are they and what do they want to achieve

• **Nation/State Adversaries**: Hostile states seeking to destroy physical assets (e.g., Stuxnet virus) or perform espionage on their adversaries (e.g., SolarWinds attack). Or attack the electric grid, or other critical infrastructure of US or Ukraine. Might be cyber warfare.

• **Cyber Criminals**: Hackers or organized crime seeking financial benefit through theft of personal data (e.g., phishing) or compromise of cyber systems for profit (e.g., ransomware)

• **Cyber Terrorists/ Cyber Activists (Hacktivists)**: Terrorist seeking to sabotage or destroy assets, such as critical infrastructure, for political or ideological reasons

• **Insider Attackers**: Disgruntled or alienated employees, or enemies, seeking to harm their employers or institutions

• **“Challenge” Hackers**: Just in it for the challenge. Sometimes hired by law enforcement to legally break into a computer or cell phone
Case Study: Cyber Criminal Group KILLNET

US Coast Guard Cyber Command
Maritime Cyber Alert 03-22

August 17, 2022

Information Sharing Protocol: TLP: WHITE [https://www.us-cert.gov/tlp]

Threat from Cyber Criminal Group KILLNET.
The KILLNET Group
Who are they and what do they want to achieve

• The KILLNET Group is a cyber criminal and cyber hacktivist group aligned with Russia

• It has attacked sites in many European countries, and is targeting sites in US

• Group activity has increased since Russian invasion of Ukraine in 2022

• Among its TTP’s (Tactics, Techniques, and Procedures) are:
  • Brute Force Attack: Gaining system entry credentials by exhaustively trying all possibilities
  • Denial Of Service Attack: Overloading a victim’s network by generating traffic overloads; renders user network resources inaccessible to intended users

• Victims in Norway, Lithuania, Italy, US (Lockheed Martin), US Power Grid?
The MTS Target Components

Port cybersecurity potential vulnerabilities, including the intermodal connectors

Ref: NSRI Study Report, Maritime Cyber Security
The MTS Target Components

Vessel cybersecurity and vulnerable systems

Shipboard Systems

- PROPULSION AND STEERING
- NAVIGATION
- POWER
- BALLAST
- COMMUNICATIONS
- CARGO MGT

The diagram illustrates various components and systems related to vessel cybersecurity and vulnerability.
Case Study: Commercial Vessel Attack - Port of NY/NJ
Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel’s network and essential control systems.

USCG Analysis

Essential vessel control systems (OT) were “air-gapped” from impacted network, but...

- Impacted network used various IT functions (cargo data management, voyage planning, updating electronic charts).
- Malware identified as **EMOTET** (modular banking Trojan)
- Malware **slowed** systems operations (Note: This is an “Indicator of Compromise”)
- Unknown source...virus could have been transferred by USB or downloaded by any internet user on board.
- Liberal use of thumb-drive data transfer at all ports of call. No active scanning of networks/external drives.
Findings
Safety Alert 06-19 - Port of NY/NJ

Some findings
- Generic login/password used by all personnel with access to the vessel; no network monitoring or consistent use of anti-virus software

- No “Principle of Least Access”

As we shall see, this means no cyber access control, everybody can access everything
- Note: Recall earlier we said physical access control “Keeps unauthorized people (and things) out of places they should not be”

Also means hard to trace, anyone could have caused it! No forensics.
USCG Recommendations

These USCG strong recommendations from Safety Alert 06-19 will be repeated in most exploits (These are all key Take-Aways for us)

• **Segment Networks.** “Flat” networks allow an adversary to easily maneuver to any system connected to that network (This is called “Lateral Attack”)

• **Per-user Profiles, Passwords, and Privileges.** Limit access/privileges to only those levels necessary to allow each user to do his or her job. (Principle of Least Access)

• **Be Wary of External (Portable) Media.** This incident revealed that it is common practice for cargo data to be transferred at the pier, via USB drive. USB drives can be a vehicle to introduce malware.

• **Install Basic Antivirus Software.**
Case Study: Fragility of the MTS – Suez Canal Accident

On March 21, 2021, the Evergreen *Ever Given* became wedged in the Suez Canal closing it to traffic for six days. Although an accident, it illustrates the profound consequences of a successful attack on MTS choke points. Other choke points are port entry channels and Intermodal Connectors.
Effects of a Successful Choke Point Attack

The Suez Canal *Ever Given* Accident demonstrates the vulnerability of the MTS to a choke point compromise. Choke points include canals, port channels, and intermodal connectors.

The six-day closure resulted in billions of dollars in losses from

- Refloating and recovering the *Ever Given*
- Delay, misrouting, and misplaced containers
  - Shortages of goods and fuel globally
  - Shortages of empty containers at sources of supply
- Overloading nearby ports
- No good alternate routes
- Results the same whether by intent or accident
Module 1 - Summary

- The MTS extends from Intermodal Connector to Intermodal Connector, including port facilities, vessels and MTSA-regulated pipeline facilities.

- Attacks can occur in both facilities and on vessels.

- A serious infrastructure attack may be initiated through a deceitful attack on unsuspecting employees (e.g., phishing), a password attack or by exploiting portable media, among others.

- Choke points are particularly vulnerable to major impacts on supply chains.

- There are many types of Threat Actors with varying motivations.

- Some key cybersecurity take-aways were introduced, including concerns regarding flat networks, per user passwords and privileges, portable media, and up-to-date virus controls.
This material is based upon work supported by the U.S. Department of Homeland Security under Cooperative Agreement No. 2014-ST-061-ML0001.

MSC@stevens.edu
www.stevens.edu/MSC