SHARPE CONSULTING LLC

# ATTACKS AND DEFENSE OF THE MARITIME INTERMODAL STRUCTURE

17 March 2021

**Greg Wessel**

**Senior Technical Consultant**

# Sea Change

- You are in a global cyber war
  - Stop viewing attacks as isolated incidents
  - Political and economic as much as technical or criminal
- Most of what has been written, reported, and assumed about cyber is wrong
- Our current security approach has led to the adversary getting stronger and better, and information systems becoming weaker and more exposed
- Cyber has gone from a practice of war to a profit industry
- We know how to defend systems, but much of this has become lost in the fog of war and quest for revenue
- Our goal today:  for you to reimagine cyber, understand the battlespace, and set yourself on a war footing to change the tide


SHARPE CONSULTING LLC

# Under Siege

- Maritime attacks up 900% over the last three years; 400% increase since Feb. 2020
- Over 500 major cyber security breaches in 2020, up almost 200 from 2019
- All of the major shipping companies have been victims:
  - CMA CGM (2020): ransomware
  - Mediterranean Shipping Company (2020): unnamed malware
  - COSCO (2018): ransomware
  - Maersk (2017): NotPetya
- Lloyd's of London: report showed cyber attack on Asian ports could cost $110B, paralyze global supply chains
- 92% of total economic costs from an attack are uninsured
- I.H.S. Fairplay Survey: only 66% of maritime respondents had a IT security policy; 44% believe the largest risk is staff; many report no staff IT security training

# Dead in the Water

- 90% of traded goods are carried on the seas
  - Industry generates over half a trillion dollars in income annually
- We are at the proverbial iceberg tip in terms of cyber impacts on maritime
  - Most attacks are financially motivated and not meant to destroy capabilities
  - Future threats of nation-states, activists and terrorists will be based on destruction of infrastructure
  - Quantity of attacks on maritime does not match the value of the target
  - Attack vectors are still very limited
- Cyber will Determine the Balance of Maritime Power by 2030
  - Maritime already part of a global cyber war
  - Easiest way to influence trade is via shipping and port control
  - Economic disruption to US, Europe would be in the trillions of dollars; essentially held hostage
  - China's aggression in South China Seas turns to economic warfare, expands to Southeast Asia, Africa
- New Jack Sparrow
  - Very similar philosophy, tolerance, and trajectory to 17th Century piracy
  - Unconstrained economic warfare; part of proxy nation-state conflicts
  - Difference: we're reaching a point where the genie can't go back in the bottle
  - Unless we realize what governments then did, we are at a point of no return


SHARPE CONSULTING LLC

# Talk Overview and Outcomes

- What this is, and what it is not

- Today's objectives:
  - Explain why we are in this fix
  - Level setting involving cyber
  - Uncover the attackers profile and perspective
  - Allow you to live a Maritime cyber kill chain
  - Walk through the supply chain, examine major nodes, discuss threats, and tech and policy mitigation techniques
  - Demonstrate the byplay between defense and attack, and why the attacker's view is essential to saving your systems
  - Help you reimagine cyber and your response to this existential crisis


SHARPE CONSULTING LLC

# What is Cybersecurity

- The practice of defending your electronic systems, networks, computers, mobile devices, programs and data from malicious digital attacks.
  - Computer Network Attack (Disrupt, deny, degrade or destroy information within computers and networks)
  - Computer Network Exploit (Enabling actions and intelligence collection via computer networks that gather data from target systems or networks)
  - Computer Network Defend (Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity in computers and networks)
  - Policies and Procedures (Built for people)
  - Risk Management (Assessing risk for Defend)
  - Threat and Vulnerability Assessments (Examination)
  - Legal (What can we do)


SHARPE CONSULTING LLC

# Basic Cyber Definitions

- Vulnerability - weakness on a network or its systems devices including servers, firewalls, computers, routers, switches, printers, phones
- Threat - any malicious act that attempts to gain access to a computer network or systems devices without authorization or permission from the owners.
- Risk - the potential exposure to loss or harm stemming from an organization's information or communications systems. (Cyber attacks or data breaches). Also encompasses theft of intellectual property, productivity losses, and reputational harm.
- Hacking - practice of using a computer to break the security of another computing system or network by modifying software and hardware to steal data, corrupt systems or files, commandeer the environment or disrupt data-related activities in any way. 80% of attacks are from hacking.


SHARPE CONSULTING LLC

# Cyber Weapons: Malware

- Virus - programs that infect and can replicate itself to spread from file to file on a computer and from one to another. Attaches to other files
- Trojan Horse - a program that pretends to be legitimate software but when launched performs harmful actions. Do not spread, installed secretly
- Spyware - software that is designed to collect data and send it to a third party without your knowledge or consent. Keyloggers, confidential info, harvest email addresses, track browsing habits
- Adware - launch advertisements, popup banners, toolbars bring these onto computers
- Worms - subset of viruses. Replicates but does not infect other files. Looks to spread to other computers. Stand alone code
- Rootkits - used to evade detection to gain unauthorized access. Stealthy, invisible downloaded from web pages and in memory
- Keylogger - records what is typed on the keyboard of your computer

# Basic Attack Categories

- Malware
- Distributed Denial of Service - overwhelm the server or network with more traffic than it can accommodate
- Phishing - specific type of attack, usually email that tricks you into disclosing valuable information or opening malware thru attachments or websites. Largest attack vector being used today.
- Ransomware - software that requires the victim to pay a ransom to access encrypted files
- Zero Day - cyber attack that occurs on the same day a weakness is discovered in software with no fix available yet
- Subversion – for our talk, other tradecraft that has cyber consequences
- Botnet - network of computers to launch malware or attacks


SHARPE CONSULTING LLC

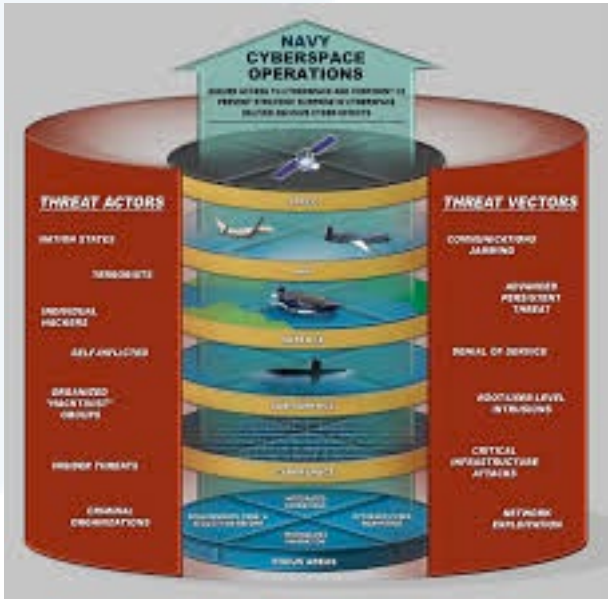
# Attacker Profiles

- Nation State - hackers target government agencies, critical infrastructure and any and all industries known to contain sensitive or intellectual data or property
- Organized Crime - criminals that engage in a variety of cybercrimes, including fraud, hacking, malware creation and distribution, DDoS attacks, blackmail, and stealing intellectual property
- Activists - process of using Internet-based socializing and communication techniques to create, operate and manage activism to promote a cause, product, company, politician or a revolution;
- Script Kiddies - an unskilled individual who uses software or programs to run attacks
- White/Black Hat – attackers who use their skills for good or evil hacking
- Insiders - a malicious, careless or negligent threat to an organization that comes from people within the organization


SHARPE CONSULTING LLC

# Attacker Characteristics

- Motivation
  - More varied than ever
- Skills
  - More available than ever
  - Most attacks are low tech/high volume
- Resources
  - Cost is lower than ever
  - Reward is highest in history
- Goals
  - Depends on which attacker profile



# Attacker Motivations

- Financial Gain
- Disruption
- Deception
- Steal/Leak Information
- Idealism/Political
- Revenge
- Spying
- Deface/Destroy/Sabotage
- Loss of Intellectual Property
- Data/Revenue Loss

# Attack Outcomes

- Espionage
  - Ex. Cozy Bear on SolarWinds, multiple Ministries of Foreign Affairs, US State Dept., White House, etc.
  - Ex. Chinese attack against US satellite firms, many others
- Information Stealing
  - Ex. F-35 Joint Strike Fighter
  - Ex. North Korea and the COVID-19 vaccine
- Disrupt, Destroy, Denigrate, Damage, Deny
  - Ex. Russian attack on Ukraine power grid
  - Ex. Maersk
- Hearts and Minds
  - Ex. Russian and French groups conducting political information operations in Africa
  - Ex. Iranian voter intimidation campaign against US citizens

# Anatomy of a Cyber Attack

- Reconnaissance - the use of cyber capabilities to obtain information about activities, information resources, or system capabilities
- Access - ability to gain permission and enter a network or information system or its assets
- Execution - ability to run software on a network or information system or its assets
- Escalation and Credential Access - thru software or social engineering, gain privileged access
- Movement - the ability to move between different networks or information systems or assets without being detected
- Collection/Disruption/Destruction/Denigration/Damage
- Command and Control - ability to direct software on a network from afar
- Exfil, Change Data, Deny Access etc.

# Virtual Tabletop:

# How an Attacker Would Approach the Port of LA/LB

# Cyber Challenges Facing the Maritime Business Function

- Accepting the Digital Culture - stakeholders are conservative and new technologies and cyber are not a priority. Older technology being used or none at all, manual or paper
- Awareness and Training regarding Cybersecurity - Used to rely on safety and physical security to address risks. IT and OT bring new challenges with regards to cybersecurity that port stakeholders often do not fully anticipate and master. Educating workers and employees is not an easy task
- Budgets - a consequence of poor cybersecurity awareness, especially of top management with regards to cybersecurity challenges. Processes have not caught up to include HW/SW to defend and money for education is spent elsewhere
- Cybersecurity Human Resources for IT and OT - Not enough people in IT and OT staff to manage all projects. Need for hiring cybersecurity resources that are expensive and scarce for securing networks, IT and OT systems


SHARPE CONSULTING LLC

# Cyber Challenges Facing the Maritime Information Technology (IT) Function

- Balance of Cybersecurity and Business Efficiency - guaranteeing the continuity of services while keeping IT and Operational Technology (OT) secure, such as disconnecting critical systems and updating systems without any business impacts
- Regulatory requirements for Cybersecurity NIS Directive 1st one - to implement cybersecurity measures, but only concerns some of the stakeholders in the maritime sector and not the entire port ecosystem
- Keeping up with latest Threats - especially in view of the diversity of stakeholders operating in the ports, the processes, the systems implemented
- Technical complexity of Port IT and OT - the port stakeholders use different systems and technologies that are developed, managed and maintained either by port IT teams, by third-parties or by IT providers
- IT and OT convergence - Usually OT systems, more vulnerable than IT systems, are protected because they are separated from IT systems and networks. But, increasingly, IT and OT systems and networks, become more and more dependent and interconnected, exposing OT systems to higher risks
- Lack of effective tools and talent – budgets for cyber tools and software not there, hiring talent is tough
- New Cyber Risks - ports launching projects to digitalize port processes, (SmartPort concept). Risks should be taken to account in the initial phases of those projects.

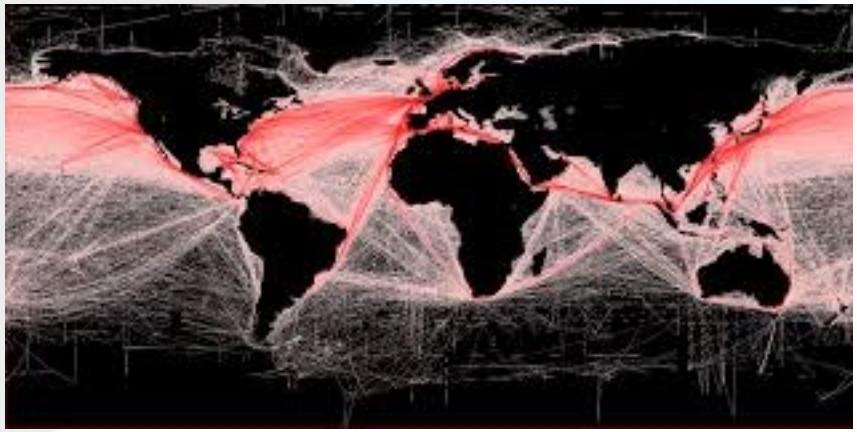

SHARPE CONSULTING LLC

# Cyber Challenges Facing the Maritime Supply Chain

- Supply Chain Overview
  - lack of cybersecurity certifications for port products and services.
  - security risks related to supplier remote access to the port networks/systems
  - long patching cycles for certain types of systems (e.g. ICS)
  - Contractors do not have control over the cybersecurity level of their suppliers and over the cyber risks they involve (supply chain attacks)
- Complexity of the Maritime Port ecosystems - due to the number and diversity of stakeholders taking part in port operations. This ecosystem is built from companies of various sizes, with various levels of cybersecurity capabilities and can even be direct competitors among themselves. No cybersecurity control at the port level
- Interdependencies Port services and external services - from other sectors (e.g. energy) that introduce interdependency cybersecurity risks
- Communications systems for Vessels, Trains and Trucks - especially regarding systems managing navigation data and OT systems which can be very old and vulnerable

# View of the Attack Battlespace

- Almost impossibly complex
- Facing nearly every type of threat actor
- Adversaries have nearly limitless options to accomplish objectives
- Currently, sophisticated attacks will succeed over 90% of the time
- Culture and business elements of cyber not well understood in maritime
- Current technology tools and methods largely will not work



# Do we have a Cyber Midway

- Defeat and hopelessness into victory
- Starts with cultural shift – war versus business
- Classic problem: undermanned and outgunned
- Three steps to changing the trajectory of cyber:
  - People – better gunslingers not better weapons (tools)
  - Agility and Adaptability – must take this from the adversary and stop being a monolith (also involves innovation and smartly using innovation)
  - Superior Knowledge of Your Elements– you should know your domain, system and business better than your adversaries (not maritime experts) and therefore you need to maximize this advantage in defense


SHARPE CONSULTING LLC

# Achieving Victory

- The following will look at the vectors of the maritime constellation and show:
  - Various risks and threats
  - Attacks that could be carried out
  - How to defend against the attacks
  - Policies and Procedures to implement for future protection

# Port Facility Access

- What type of attacker - Nation State, Organized Crime, Activists, Script Kiddies, Insiders
- What kind of attacks - Malware, Phishing, DDos, Subversion
- What can be gained
  - Degrade or disrupt systems used to identify and direct cargo, truck drivers, and facility personnel.
  - Deny access to port facilities
  - Significant congestion or the closure of terminal
- How to defend against
  - Install Antivirus, Firewalls, Intrusion Detection/Prevention
  - Keep software and Operating Systems up-to-date
  - Redundancy of systems
  - Training and Education
  - Contingency Plans, Respond and Recover
  - Training and Education
  - Hire Cyber Personnel
  - Better understanding and mapping of supply chain and risk

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

SHARPE CONSULTING LLC

# Terminal Headquarters

- What kind of attacker - Nation State, Organized Crime, Activists, Script Kiddies, Insiders
- What kind of attacks – Malware, Phishing, Ransomware, DDos, Subversion
- What can be gained –
  - Access sensitive client and cargo information. Steal cargo or smuggle illicit cargo through the terminal.
  - Loss of intellectual property
  - Manipulation or destruction of data
  - Can disrupt operations within a facility
  - Information stealing or spying
  - Financial and business losses
- How to defend against
  - Install Antivirus, Firewalls, Intrusion Detection/Prevention
  - Encrypt data in Transit and at rest
  - Keep software and Operating Systems up-to-date
  - Dual Factor Authentication
  - Redundancy of systems
  - Backup data
  - Training and Education
  - Contingency Plans, Respond and Recover
  - Training and Education
  - Hire Cyber Personnel
  - Better understanding and mapping of supply chain and risk

# Operational Technology Systems

- What kind of attacker - Nation State, Organized Crime, Script Kiddies, Insiders
- What kind of attacks – Malware, Ransomware, DDos, Subversion
- What can be gained
  - Changes to cargo movements
  - Disrupt port operations
  - Espionage
  - Damage to equipment
  - Safety risks for personnel
- How to defend against
  - If connected to IT systems, Install Antivirus, Firewalls, Intrusion Detection/Prevention
  - Updates or patches must be carefully designed and implemented
  - Redundancy of systems
  - Lack of computer memory makes difficult to implement security
  - Training and Education
  - Contingency Plans, Respond and Recover
  - Training and Education
  - Hire Cyber Personnel
  - Better understanding and mapping of supply chain and risk

# Position, Navigation and Timing Services

- What kind of attacker - Nation State, Organized Crime, Script Kiddies, Insiders
- What kind of attacks – Malware, DDos
- What can be gained
  - Disrupt vessel movement
  - Deny logistical support at port facilities
  - Collisions causing damage to vessels
- How to defend against
  - Install Antivirus, Firewalls, Intrusion Detection/Prevention
  - Redundancy of systems
  - Backups
  - Training and Education
  - Contingency Plans, Respond and Recover
  - Training and Education
  - Hire Cyber Personnel
  - Better understanding and mapping of supply chain and risk

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

SHARPE CONSULTING LLC

# Vessels, Trucks, Trains

- What kind of attacker - Nation State, Organized Crime, Activists, Script Kiddies, Insiders
- What kind of attacks - Malware, Ransomware, DDos, GPS hacks
- What can be gained
  - GPS spoofing or jamming
  - Disrupt, Deny, Denigrate Access to Wi-Fi, LTE
  - Access to USB storage devices
  - Change routes or cargo loads
  - Compromise vessels/trucks/trains can gain access to other IT networks at the port
  - Divert ships, trucks or trains
  - Clog up shipping lanes to the ports
- How to defend against
  - Install Antivirus, Firewalls, Intrusion Detection/Prevention
  - Dual Factor Authentication
  - Training and Education
  - Contingency Plans, Respond and Recover
  - Training and Education
  - Hire Cyber Personnel
  - Better understanding and mapping of supply chain and risk


SHARPE CONSULTING LLC

# Constructing Your Art of War: Essential Policies and Procedures

- Risk Assessment of OT and IT – Assess where your OT and IT are vulnerable
- Contingency Plans – What happens if you have a cyber attack
- Response and Recover Plans – How to recover from a cyber attack
- Test Systems and Networks for Vulnerabilities - also keep all operating system and other software up-to-date
- Install Firewalls, Antivirus Software And other Tools – protection from malware and other viruses
- Multi-factor Authentication - for all employee accounts
- Implement Intrusion Prevention Technology - detect reconnaissance attempts
- Encrypt Sensitive Data - both in transit and at rest
- Alerting and Logging - incoming and outgoing data
- Hardware and Software Audits - monitor the strength of your IT systems
- Training and Education - educate them on how to prevent and respond to cyber attacks
- Supply Chain – perform an audit better than two layers deep and categorize risk

# Conclusions

- Maritime Intermodal needs to reimagine cyber security
  - You are in a war. Your adversaries have made cyber a top priority. So should you.
  - This is not an IT problem. A nation goes to war, not a department. Commit everyone.
  - Ultimately, people, not technology, will be the difference. Hire and train accordingly.
- Technology and the Cyber Security Industry will NOT solve the security problem
  - Cyber security is a $150B industry, with incredible growth every year
  - Yet attacks and breaches are at an all-time high, and seemingly easier
- Understand security from the perspective of an attacker
  - Don't secure for security's sake, or because of compliance – you have people attacking you!
  - Perform assessment on your entire network
  - Gain full knowledge of your supply chain
  - Know your adversaries, and their motivations, capabilities, and tools
- Security is an outcome, not a checkbox
  - The point of security is to mitigate or stop threats…not to earn a certificate
  - Commit the necessary resources (money, time, people, technology)
  - Develop policies, plans, and strategies NOW
  - Develop a culture of security, place yourselves on war footing
- This is a "Midway Moment": commit to change and a fight, or Maritime as we know it will not exist in 2030


SHARPE CONSULTING LLC

# Do not hesitate to contact us

**Greg Wessel**

Sharpe Consulting LLC

www.SharpeLLC.com

glwessel@comcast.net

Free Consultation

We promise you two good ideas

# SHARPE CONSULTING LLC

BIG ENOUGH TO DO THE JOB

AGILE ENOUGH TO DO IT *RIGHT*

THANK YOU.