Cybersecurity Issues in Modern Transportation Infrastructure Age: Development of Prototype Maritime and Cargo Security Supply Chain

Abstract: Since the September 11 attack on the United States, efforts to improve the security of infrastructures and citizens have been given serious attention. The national security agencies in the United States have since initiated several international partnerships and anti-terrorism initiatives. Major areas that still require urgent attention are the sea ports in general and maritime cargos in particular. Cybersecurity is the follow of protective systems, networks, and programs from digital attacks. Computers and communication play an important role in all modes of maritime transportation. The purpose of this paper is to develop prototype maritime and cargo technology system for tracking and tracing shipment from foreign ports to the United State of America and increase information and trade data sharing. Specifically, the objective of this paper is to increase our understanding and awareness on issues of cybersecurity in the maritime transportation system and proposes a conceptual framework for maritime and cargo industry based on an overview review of the existing literature. The conceptual framework comprises two major tracking product identifications, namely bar coding (BC) and radio frequency identification (RFID) The paper concludes that a secure transportation system is critical to overall national security from terrorism. Groups or individuals motivated to terrorize or injure people or the economy may well utilize transportation facilities as a target and/or a tool. Most assuredly, they will utilize transportation elements in an overall plan of terrorism. The aim of maritime transportation security is to understand and resolve threats early in the process and strengthen the safety of physical infrastructures, conveyances and information assets while seeking to maximize trade through modernizing provide chain infrastructures and processes. Thus, securing the transportation system is a critical consideration in overall security planning and it is envisaged that this theoretical model provides a useful tool for decision-makers in developing a more comprehensive overall tracking Maritime and Cargo Security Supply Chain.

Keywords: Cybersecurity, Maritime security, Supply chain, Bar code, RFID.

INTRODUCTION

Since the September 11 attack on the United States, efforts to improve the security of infrastructures and citizens have been given serious attention. The national security agencies in the United States have since initiated several international partnerships and anti-terrorism initiatives. Major areas that still require urgent attention are the sea ports in general and maritime cargos in particular.

Tougher trading conditions, occasioned by the demand for security of goods and personnel moving between nations has compelled organizations and border protection agencies to strive to attain process and logistics efficiencies that will enable them to drive down costs, provides competitive advantage and offer security to the citizenry. Trans-Atlantic trading involves a supply chain that moves goods using containers, throughout the supply chain, from manufacturer to retailer across continents. There is therefore the need to implement container security to forestall unauthorized exchange of cargo content, diversion of goods and products and provide security for port personnel and trading nations.

Wawruch (2003) reported that ship borne Automatic Identification System (AIS) is an excellent tool for shore based ships monitoring, providing a automatic manner and without time delay information about ships in area of coverage of the shore based VHF radio stations (in so called A1 sea area of the Global Maritime Distress and Safety System (GMDSS)) . However, there is a common growing demand from various maritime authorities and regional and national agencies for global ships monitoring system, so called Long-Range Identification and Tracking (LRIT) system to enable them to fulfill their individual tasks ranging from navigation safety, search and rescue (SAR) service to environmental protection, prevention of crime and security acts at sea and in ports. (IALA, 2005).

Our effort, which is pioneered on the foregoing, aim to employ the use of bar codes and Radio Frequency Identification (RFID) systems as mechanisms of choice to aid Trans-Atlantic movement of exports between the United States and her international partners. This will enhance customs and border protection thus aiding the safety and movement of goods and personnel across the Atlantic. The use of barcodes can be traced back as far as the 1960s, in some cases as a means to identify railroad cars. Common linear barcodes started appearing on grocery shelves in the early 1970s as the UPC barcode to automate the process of identifying grocery items. 1982 brought a major boost to bar code technology as the U.S. Department of Defense started to require all suppliers to ship their goods with attached bar code labels. Since then, both the grocery and auto industries have stepped up their efforts requiring bar code labels on every item moved between plants and organizations. The utilization of barcode technology in business processes, procedures are automated to increase productivity and reduce human error.

Cybersecurity is the observation of protecting systems, networks, and programs from digital attacks. A booming cybersecurity approach has multiple layers of protection unfold across the computers, networks, programs, or information that one intends to stay safe (www.cisco.com). The safety of the planet provides chain is perceived as inconsistent with the target of...
facilitating international trade. Security is incredibly a part of a thought supply-chain paradigm whereas security will even become a driver for trade facilitation. While pilotless ships and autonomous ports area unit are technologically possible, it'll be quite a while before the world maritime community overcomes the worry and uncertainty related to removing all human control of vital safety, security, and environmentally sensitive shipping operations. However, stand on a drop-off wherever technology has become a vital component of the many aboard and shore-based systems that may still revolutionize the means shipping operations are conducted.

Furthermore, while the transition to multiplied dependence on cyber-enabled technologies happens, the maritime business should be proactive to take care of the outstanding safety record it's attained.

The safety culture embedded within the deoxyribonucleic acid of our business was developed over decades of rigorously implementing risk management principles into all aspects of sea life. In the face of such fast technological growth, it's this culture of risk management that may offer for a secure transition from the age of diesel to the age of the computer.

Organizations and governments have responded with policies and practices aiming at reducing the exposure of providing chains to voluntary acts of the breach and intentional chain disruptions. The applying of policies, procedures and technologies aiming at reducing such exposure and at protective, people, goods, facilities and instrumentality within the chain, still as preventing malicious interferences on the standard flow of product and data with the target of allowing contraband or thieving, area unit noted as provide chain security (Closs & McGarrell, 2004).

**Maritime Business**

In the maritime business, there are many problems that build cybersecurity for the maritime business notably tasking. Firstly, there are many alternative categories of the vessel, all of that operate in terribly completely different environments. These vessels tend to have altogether completely different portable computer systems designed into them.

Considerably, several of those systems are designed to last over thirty years. In alternative words, several ships run superannuated and unsupported operative systems, that are typically those most susceptible to cyber-attacks. Furthermore, the users of those maritime laptop systems are perpetually in flux. Ship crews are extraordinarily dynamic, typically ever-changing at short notice. As a result, the crew members are typically victimization systems they are unknown, increasing the potential for cybersecurity incidents relating to human error. Further, the maintenance of aboard systems, as well as steering ones, is usually shrunk to a range of third parties. It’s completely realizable that a ship’s crew has very little understanding of but aboard systems move with each other.

Notwithstanding, another issue is that the linkage between aboard and terrestrial systems. Several maritime companies detain constant communication with their vessels. The cybersecurity of the ship is to boot dependent, then, on the cybersecurity of the land-based infrastructure that creates this attainable. Figure 1 below shows the entire fleet that was delayed because of a cyber-attack in 2017 (Wikimedia/Nils Jepsen).

---

**Figure 1:** A.P. Moller-Maersk’s entire fleet CC BY
Issues of Cybersecurity in Transportation

The world depends on maritime commerce to maneuver exceptionally large elements of product, services, and people. Jointly this effort includes the Maritime installation or MTS, a significant component of this discouraging many-sided enterprise area unit cyber networks, and also the infrastructure they manage. From the complicated programs managing the loading and unloading of containers to waiting trucks to the planet navigation systems aboard vessels, to the hydraulic valves designed to safeguard spills into waterways that are set and controlled by cyber systems at intervals chemical, water/wastewater, or fossil fuel plants, the MTS is turning into more and more machine-driven. (Joseph. et al, 2017).

Threats to international Navigation on the provision Chain

The security of the planet provides chain could also be perceived as inconsistent with the target of facilitating international trade. Security is improbably a great deal of a section of thought supply-chain paradigm whereas security may additionally become a driver for trade facilitation. Originally developed to guide Allied convoys safely across the Atlantic, the utilization of synchronic low-frequency radio signals as a direct aid revolutionized stylish maritime navigation within the Forties. These systems were phased go in favor of the satellite-based international Positioning System (GPS) that became operational in July of 1995. The impact of GPS on the economic transportation business has been monumental. Everything that moves e.g., ships, cars, trains, aircraft, etc is currently navigated by GPS or an analogous GNSS system. Today, the first suggests that of Positioning, Navigation and temporal arrangement (PNT) being utilized in maritime applications is GPS; whether or not complete or increased. The vulnerabilities of GPS square measure standard (Grant, et.al.2008. Volpe, 2001), because the signals square measure therefore weak on reception, they're vulnerable to interference and electronic jamming, whether or not intentional or not. As such the GLA are keen to understand the effectiveness of their AtoNs, and the navigation systems being employed by mariners within their waters, under conditions of GPS service denial. The GLA promote the utilization of numerous suggests that of navigation and, as such, square measure taking part in an important role within the institution of eLoran as the associate freelance supply of PNT, with dissimilar failure modes to GNSS (Grant, et.al. 2008; 2020 The Vision, 2004).

The figure below shows three basic segments of Positioning, Navigation and Timing (PNT) namely: the space segment, the control segment, and the user segment, it should be noted that International Navigation Satellite Systems (GNSS) operate as well as GPS as reported by National Coordination workplace for Space Based Positioning, Navigation, and temporal arrangement, 2014.

Figure 2: Source: www.transportation.gov/pnt/what-positioning...Jun 13, 2017 · “A U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services.

Martin (2019) reported about the complexity of the maritime industry and involved several core issues that make cybersecurity for the maritime industry particularly challenging to address.
Issues associated with navigation include:

- **Electronic countermeasures and Interference:** The printed of a stronger signal that deliberately or unintentionally blocks or impacts a GNSS satellite signal.

- **Spoofing:** The broadcast of a false GNSS signal, but at slightly greater power. This deceives the GNSS receiver into lockup onto the spoofed signal. Once the receiver has locked onto the stronger spoofed signal, the false signal gradually phases out of sync with the actual GNSS signal, causing the receiver to report false PNT data (information generated by the spoofer). This incremental phase-out makes a spoofing attack very difficult to detect (The Mitre Corporation, 2014).

- **Meaconing:** The intentional delay and rerun of a GNSS signal meant to introduce error to receivers.

- **Extreme Space Weather (ESW):** Solar activity such as solar flares, coronal mass ejections, high-speed solar radiation, and the impact of energetic particles on the earth’s ionosphere.

**Piracy**

Cyber-attacks fall into three main categories: a criminal using cyber as the facilitator to commit another crime such as fraud; a targeted cyber-attack when the systems of a shipping company/ship are attacked to get specific data/IP or cause the company to lose business and or revenue or a “Hacktivist” who may target a company for personal gratification. Alternatively, the cyber-attack maybe directed towards manipulating cargo handling (Antwerp, 2013) in order to illegally import/export illegal weapons, narcotics, people, etc. There is also significant danger from company employee/’s/crew members unwittingly or purposefully revealing company sensitive information on social media. In summary, the threats are many and diverse but can all be overcome if approached in a pragmatic and methodical way. (www.porttechnology.org).

In 2017, I.H.S. Fairplay conducted a maritime cybersecurity survey, to that 284 folks responded. 34% of them said that their company had experienced a cyber-attack in the previous 12 months. Of those attacks, the majority were ransomware and phishing incidents; exactly the same style of incidents moving firms everywhere, and not in the slightest degree specific to the maritime world.

The good news is that solely half-hour of those responding to the survey had no appointed info security manager or department, meaning that the majority of companies have a resource able to respond and mitigate any attack.

However, the survey did reveal that their area unit still heaps of staff UN agency haven’t received cyber awareness coaching of any kind, which means the shipping industry must try harder, for its own security. Additionally, only 66% of those questioned said that their company had an IT security policy, that could be a serious cause for concern; IT security can’t be approached on a commercial hoc, incident by incident basis. It’s the safety equivalent of plugging holes in a very hull with cardboard.

To underline that, 47% of those questioned believed that their organization’s biggest cyber the vulnerability was the staff. Hardly a glowing endorsement, however, if you don’t train your employees to bear in mind of threats, it’s not shocking (David, 2018).

**Conceptual Framework for Tracking Maritime and Cargo Security**

Burke (1984) states: “Bar codes are messages where information is encoded using widths of wide or narrow bars and spaces (i.e., unique wide or narrow combinations of black and white bars). They provide a means savers due to their ability to support automatic data collection concepts. After the grocery industry reached the point where the number of labeled items proved the practicality of the system, savings of more than 1 ½ percent of the gross profit resulted. This is considered extremely high because of the very low profit margin in this industry. Baker (1984) gives other examples of resulted improvements:(a) Decreased work in process investment has been reported to be up to 65 percent, (b) reduced raw material parts and finished goods inventory are running as high as 50 percent, (c) less paper processing. In some plants this is running as much as 90 percent, (d) increased output from existing capacity is running as much as 35 percent.

These successes have been related to the use of the bar coding technology. Further improvement in overhauling the supply chain in the face of current challenges with terrorism and security at the borders are however constrained by the limitations of bar-coding as a technology for tracking the movement of goods and cargo contents. Bar codes, while representing a significant step forward when first introduced some decades ago, have significant limitations. In addition to being prone to damage, they require human intervention to be read and provide limited information since they only represent a product number. While bar codes have undoubtedly helped to deliver significant supply chain improvements by providing information which drives operational systems, they cannot be programmed and can only provide the most basic product number information. This passive technology is constraining the development of automated processes that can improve supply chain efficiencies and cross-border security.

As far as we know, the United States Custom and Border protection Agency have container security initiative with only two ports in Africa, Durban in South Africa and Alexandria in Egypt signed December 1, 2003 and September 28, 2007 respectively (USCBP, 2008). There have been series of attacks against ocean lined ship by the Mogadishu and Somalia pirates. Incidences of cargo content exchanges at sea have also been reported on Trans-Atlantic ocean liners. Given the precedent that most terrorist attacks against United States infrastructure emanates from resource-poor environment, as well as the particular instance of the Christmas day terrorist attempt on Delta airline flight, it is opportune to begin to initiate and establish measures that will strengthen border protection between the United States of America and its trading partners from Sub-Saharan Africa, Nigeria not being an exemption. Although there are volumes of ocean liners trading between Nigeria and the United States of America, Nigeria is not currently one of the nations that have
container security initiative with the US despite the substantial trade with the US. Despite the existence of computerized paper monitoring systems for cargos and its content in Nigeria, the harbor authority does not have established and standardized bar-coding schemes for tagging containers and contents. Neither is the use of RFID adapted for ports security. This scenario does not provide opportunity for data capture and data sharing at the two ends of the cargo shipment activity.

A secure transportation system is critical to overall national security from terrorism. Groups or individuals motivated to terrorize or injure people or the economy may well utilize transportation facilities as a target and/or a tool. Most assuredly, they will utilize transportation elements in an overall plan of terrorism. Thus, securing the transportation system is a critical consideration in overall security planning.

Analysis of Framework for Proposed System

The framework depicted in Figure 3 takes into consideration the interrelationship between the different factors that must be present for the proposed system to work effectively. These are:

- Data capture and information processing
- Database for data and information storage
- Data verification and updates

It is expected that all containers to be shipped will have product identification codes. This contains the necessary information about the container which includes: the point of origin, content information and specifications, expected date of delivery, destination, and time of dispatch amongst others.

The integrated system will be powered by two different technologies to facilitate both direct and remote monitoring and authentication of the containers and their contents. These include bar-code (BC) and radio frequency identification (RFID) technology. The rationale behind this integrated system is to the problems associated with BC technology. It is no gainsaying to assert that BC can easily be damaged or tampered with or without ulterior motives. Therefore, there is a need to enhance the mode of authenticating the information about any container to further enhance security of lives and properties.

Figure 3: Framework for proposed System
As shown in Figure 3, the same information is encoded into the two technologies but differently. A specific bar coding standard will be adopted among already existing bar coding systems. The BC technology consists of information which is encoded via the use combination of widths of wide or narrow bars and spaces which uniquely identify a particular. The strength of BC lies in its ability to support automatic data collection, simplicity and possibility of not drawing unnecessary attention. With this background, once the product identification has been composed, the system via the administrator generates the barcode and prints the label. Once this is printed, it is rimmed into the container ready for transportation. This operation will usually take place at the source, that is the point of origination of the container.

At the destination, the user/administrator can read the content of the BC, decode and employ the information for necessary processes to be carried out on the container.

However it is important to note that this advantage can be easily rubbed with the slightest tampering on the encoded barcode. Another important factor relating security and forming the crux of this proposal lies in the fact that BC content can only be accessed directly. This passive mode of operation hinders the need for automated processes capable of improving the supply chain efficiencies and cross-border security. With the prevailing rate of pirates attack on containers and possibility of using the seaports in carrying out deadly attacks, the onus therefore requires that an active means of monitoring and accessing the container should be developed.

With the RFID, the product identification is first encrypted to establish data security and the encrypted information is used to populate the RFID tags. The same information is sent over to the destination or out-stations to forewarn and intimate them of incoming goods and services.

Once the RFID has been populated, the transmission link between the source and destination can be established. This development facilitates sharing of information remotely and actively thus securing both the contents and the direction of the containers. The system administrator can easily assess the content of the containers, determine their destination and prepare the landing formalities for incoming goods. Another important contribution is the fact that any form of alteration/tampering on the container can easily be reflected and detected via the scanning and the RFID information.

Figure 4 depicts the link between ‘source’ and ‘destination’ as implemented in the RFID module. It provides the opportunity for communication both remotely and direct aimed at monitoring the content of the container via the RFID tags. Once the container arrives at the port, the system provides a dual mode authentication system. That is, the content of the barcode (if unhampered) is decoded and compared with the decrypted information from the RFID tag. If the two correspond, then there is every possibility that the content is safe and secure, if otherwise, alarm can easily be raised or such container can be treated with caution until they can be validated by other means.

**CONCLUSION**

The aim of maritime security is to understand and resolve threats early in the process and strengthen the safety of physical infrastructures, conveyances, and information assets, while seeking to maximize trade through modernizing provide chain infrastructures and processes. The maritime community has to become additional open-eyed, actively train to acknowledge and respond to both jamming and spoofing attacks and encourage the immediate installation of complementary PNT systems.
The paper concludes that a secure transportation system is critical to overall national security from terrorism. Groups or individuals motivated to terrorize or injure people or the economy may well utilize transportation facilities as a target and/or a tool. Most assuredly, they will utilize transportation elements in an overall plan of terrorism. The aim of maritime transportation security is to understand and resolve threats early in the process and strengthen the safety of physical infrastructures, conveyances and information assets while seeking to maximize trade through modernizing provide chain infrastructures and processes. Thus, securing the transportation system is a critical consideration in overall security planning and it is envisaged that this theoretical model provides a useful tool for decision-makers in developing a more comprehensive overall tracking Maritime and Cargo Security Supply Chain

REFERENCES
4. https://www.securitymagazine.com/articles/87010-the-daily-challenges-
7. International Association of Lighthouse Authorities (IALA) 2005
12. www.cisco.com
13. www_gps.gov