Identifying Commonalities of Cyberattacks Against the Maritime Transportation System

Rebecca Rohan
Marymount University, Arlington, Virginia, United States of America

rebecca_rohan@marymount.edu

Abstract: The purpose of this study is to identify commonalities in cyberattacks against the civilian maritime transportation system (MTS). For this exploratory study, the researcher analysed documents to identify trends about the cyberattacks impacting and responsible adversaries targeting maritime operations. The MTS can use identified trends to make informed decisions about information technology (IT) and operational technology (OT) requiring new or enhanced cybersecurity measures. Current research examining publicly disclosed cyberattacks impacting MTS companies identifies the trend of increasing cyberattacks against the MTS. However, current research fails to examine adversaries and their social-political needs thoroughly. Knowledge of the adversary based on the Diamond Model of Intrusion Analysis can be augmented by identifying which MTS assets (e.g., shipbuilding, ports) and which aspect of the information security triad—Confidentiality, Integrity, or Availability (CIA)—the adversary targeted. At the conclusion of this limited, exploratory document analysis, the researcher determined the most compromised aspect of the information security triad was Availability and then Confidentiality; there were no identified Integrity compromises. The most targeted MTS assets was shipping companies, followed by ports, administration, shipbuilding, and vessels. Concerning the adversary customer behind MTS cyberattacks, China was first, followed by unknown cyber adversaries, then Russia, Iran, and Israel. Last, in terms of adversary's social-political needs, data exfiltration occurred the most, followed by ransomware, political agenda, and unknown needs.

Keywords: Maritime Transportation System, MTS, Adversary, Information Technology (IT), Operational Technology (OT)

1. Introduction

Over recent years, cybersecurity attacks have increasingly impacted the maritime transportation system (MTS), which plays a critical role in the global economy. The MTS moves over 80 percent of all goods around the globe (Statista, 2022). Cyberattacks, including deployment of malicious software (or malware), have disrupted operations at ports, in shipping companies, and in MTS administration (Dickerson, 2021; Vanguard, 2020). To better secure information technology (IT) and operational technology (OT), the MTS needs to understand better the adversaries behind the cyberattacks impacting maritime operations.

The purpose of this paper is to identify trends in adversaries targeting of the MTS by exploring cyberattacks impacting the MTS, including maritime administration, ports, shipbuilding, shipping companies, and vessels. In Section 2, related work pertaining to cyber adversaries per the Diamond Model of Intrusion Analysis and published research on cyber adversaries attacking the MTS will be reviewed. Section 3 will discuss the methodology and research design. Section 4 will present the results and discuss the findings. Finally, Section 5 will address the conclusion and recommendations for future work.

2. Related Work

Current research addresses concerns about increasing cyberattacks against the civilian MTS but does not provide an in-depth analysis of the adversaries behind those cyberattacks. The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) noted a 30 percent increase in reporting of malicious cyber activities against MTS stakeholders during January-June 2021 (Dickerson, 2021). Other works have examined factors affecting cybersecurity risks in the MTS without looking into the adversaries behind the cyberattacks (Tam and Jones, 2019). Current work has addressed implementing tools for dynamic risk assessments for improving cybersecurity in ports or managing cybersecurity risk using risk analysis models (Tam, Moara-Nkwe, and Jones, 2021; Paté-Cornell et al, 2018).

In the Diamond Model of Intrusion Analysis, the adversary compromises one of four points of the diamond with the three remaining points being victim, capability, and infrastructure. The adversary is an actor/organization employing a capability over an infrastructure against the victim to achieve an effect (Caltagirone, Pendergast, and Best, 2013).

Knowledge of the adversary is usually elusive and likely unknown when a cyberattack is initially identified (Caltagirone, Pendergast, and Best, 2013). Details about the adversary include the adversary operator, the adversary customer, and social-political needs for conducting a cyberattack (Caltagirone, Pendergast, and Best, 2013). The adversary operator is the actor/organization conducting the cyberattack, and the adversary customer

is the entity that will benefit from the cyberattack (Caltagirone, Pendergast, and Best, 2013). In conducting a cyberattack, the adversary can meet their social-political needs, or goals, of the attack (Caltagirone, Pendergast, and Best, 2013). In this study, the adversary's social-political needs fell into one of four categories: data exfiltration, political agenda, ransomware, or unknown. Knowledge of the adversary based upon the Diamond Model of Intrusion Analysis can be augmented by identifying which aspect of the information security triad—Confidentiality, Integrity, or Availability (CIA)—and which MTS asset (e.g., shipbuilding, ports) the adversary targeted during a cyberattack.

3. Methodology and Research Design

For the MTS, publicly available datasets concerning cyberattacks and the adversaries conducting said attacks are lacking. To complete this exploratory research, document analysis was based on two open-source websites:

- The Center for Strategic and International Studies (CSIS) maintains a Significant Cyber Incidents timeline from the year 2006 to the present focusing on cyberattacks against the defense sector, government agencies, high-tech companies, or those economic crimes in excess of one million U.S. dollars (Center, n.d.).
- The Council of Foreign Relations maintains a Cyber Operations tracker from the year 2005 to present involving publicly known state-sponsored cyber incidents (Council, 2022).

To focus on the entries pertaining to the MTS, the researcher:

1. Combined entries from CFR and CSIS into one spreadsheet for a total of 1,319 entries.
2. Deleted duplicate entries.
3. Deleted entries lacking the key terms *maritime, marine, transportation,* or *shipping* (at this point, 46 entries remained).
4. Deleted 20 entries with terminology pertaining to defense or military—*defense, military, naval technologies, navy, submarine, unclassified,* or *warship*.
5. Deleted 11 entries lacking specificity of a target in the MTS and lacking keywords *civilian maritime operations, maritime affairs, shipping,* or *transportation*.

See Figure 1 for a graphical representation noting how the CFR and CSIS entries were filtered.

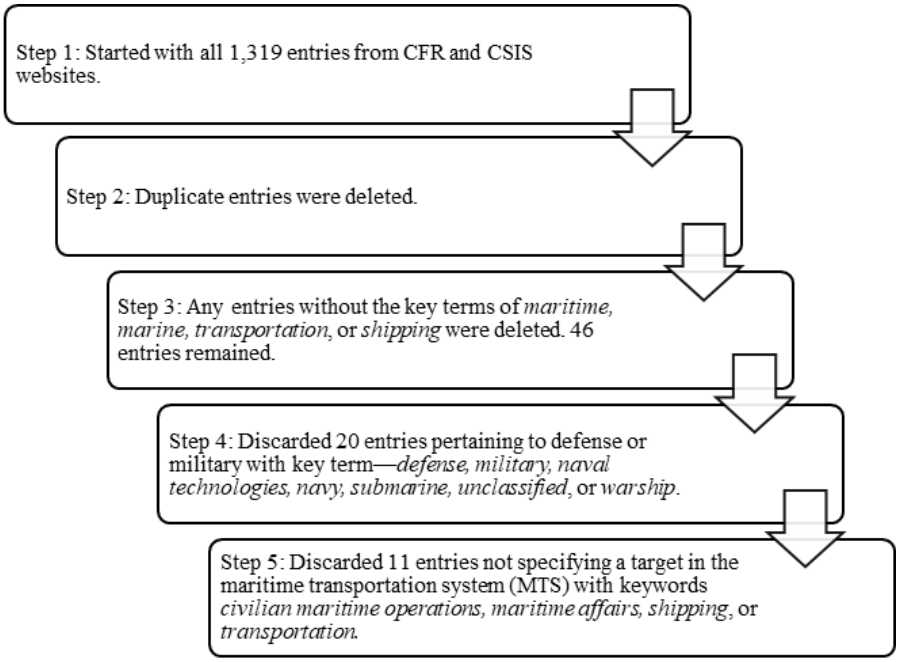

Figure 1: Steps for filtering cyber incident entries from CFR and CSIS.

4. Results and Discussion

Once filtering steps outlined in Section 3 and Figure 1 were completed, 15 entries remained of the original 1,319 entries obtained from CSIS' Significant Cyber Incidents and CFR's Cyber Operations Tracker (CSIS, 2021; CFR, 2021). The researcher created a spreadsheet with the 15 remaining entries to sort the data. The spreadsheet had the following columns:

- Year;
- Incident Description;
- MTS Asset:
    - Administration – maritime agencies or companies providing software used by the MTS;
    - Ports – ports or terminals where cargo is loaded/unloaded;
    - Shipbuilding – companies building ships used in the MTS;
    - Shipping Companies – companies handling the business or physical movement of cargo; or
    - Vessels – ships or merchant vessels transporting cargo.
- Victim of Cyberattack;
- Adversary Operator;
- Adversary Customer;
- Security Fundamental Compromised – Confidentiality, Integrity, or Availability; and
- Social-Political Needs – data exfiltration, political agenda, ransomware, or unknown need.

Arranged chronologically from newest to oldest, the resulting 15 entries on cyber incidents and adversary details are shown in Figure 2.

Year	Incident Description	MTS Asset	Victim of Cyberattack	Adversary Operator	Adversary Customer	Security Fundamental Compromised	Social-Political Need
2020	Iranian hackers compromised an Isareli developer of logistics management software and then accessed data over 40 clients of the developer (CSIS, 2021).	Administration	Unspecified	Unknown	Iran	Confidentiality	Political Agenda
2020	Iran's Ports and Maritime Organization experienced a cyberattack (CSIS, 2021).	Ports	Iran's Ports & Maritime Organization	Unknown	Unknown	Availability	Unknown
2020	The International Maritime Organization (IMO)--the United Nation's maritime agency--experienced a cyberattack impacting its website and networks (CSIS, 2021).	Administration	International Maritime Organization	Unknown	Unknown	Availability	Unknown
2020	CMA CGM SA, a French shipping company, experienced a ransomware attack in two of its Asian subsidiaries; the ransomware significantly disrupted information technology networks but did not impact movement of cargo (CSIS, 2021).	Shipping Companies	CMA CGM SA	Unknown	Unknown	Availability	Ransomware
2020	Operations at Iranian port, Shahid Rajaee, were disrupted for several days due to cyberattacks conducted by Isareli hackers (CFR, 2021; CSIS, 2021)	Ports	Shahid Rajaee Port	Unknown	Israel	Availability	Political Agenda
2019	A merchant vessel coming into the U.S. via interational waters reported a malware incident impacting the vessel's networks. The U.S. Coast received the report and issued a warning (CSIS, 2021).	Vessels	Unspecified	Unknown	Unknown	Availability	Unknown
2017	The Port of Rosario is a suspected victim of NotPetya malware that encrypted data on victim's computers without any means of data decryption (CFR, 2021).	Ports	Port of Rosario	Unknown	Russia	Availability	Ransomware
2017	For two days, Maersk's operations at port terminals were shut down by the NotPetya malware (CFR, 2021).	Ports	Maersk	Unknown	Russia	Availability	Ransomware
2017	For two days, Maersk's shipping operations were shut down by the NotPetya malware (CFR, 2021).	Shipping Companies	Maersk	Unknown	Russia	Availability	Ransomware
2015	OceanLotus has been conducting cyberattacks targeting shipping companies and marine agencies. Qihoo360, a Chinese company, reported OceanLotus has been running an espionage program since 2012 (CSIS, 2021).	Administration	Unspecified	Unknown	China	Confidentiality	Data Exfiltration
2015	OceanLotus has been conducting cyberattacks targeting shipping companies and marine agencies. Qihoo360, a Chinese company, reported OceanLotus has been running an espionage program since 2012 (CSIS, 2021).	Shipping Companies	Unspecified	Unknown	China	Confidentiality	Data Exfiltration
2015	Threat actor, Ocean Lotus, has conducted cyberattacks against maritime construction firms (CFR, 2021)	Shipbuilding	Unspecified	Unknown	China	Confidentiality	Data Exfiltration
2013	Threat actor, IceFog, conducts cyberattacks targeting maritime and shipbuilding groups. Targets have primarily been in Japan and South Korea (CFR, 2021).	Shipping Companies	Unspecified	Unknown	China	Confidentiality	Data Exfiltration
2012	Threat actor, Lucky Cat, conducts cyberattacks against Indian and Japanese shipping industries (CFR, 2021).	Shipping Companies	Unspecified	Unknown	China	Confidentiality	Data Exfiltration
2012	Threat actor, Sneaky Panda, targets cyberattacks against shipping firms in the private sector (CFR, 2021).	Shipping Companies	Unspecified	Unknown	China	Confidentiality	Data Exfiltration

Figure 2: Entries remaining after data filtering and sorted chronologically from newest to oldest

This exploratory document analysis on cyber incidents and associated adversary details are shown in Figures 3 through 6.

Figure 3 shows the cyber incidents per MTS asset:

- The most targeted MTS asset was shipping companies with six incidents.
- The second most targeted MTS asset was ports (four incidents) followed by administration (three incidents), shipbuilding (one incident), and vessels (one incident).

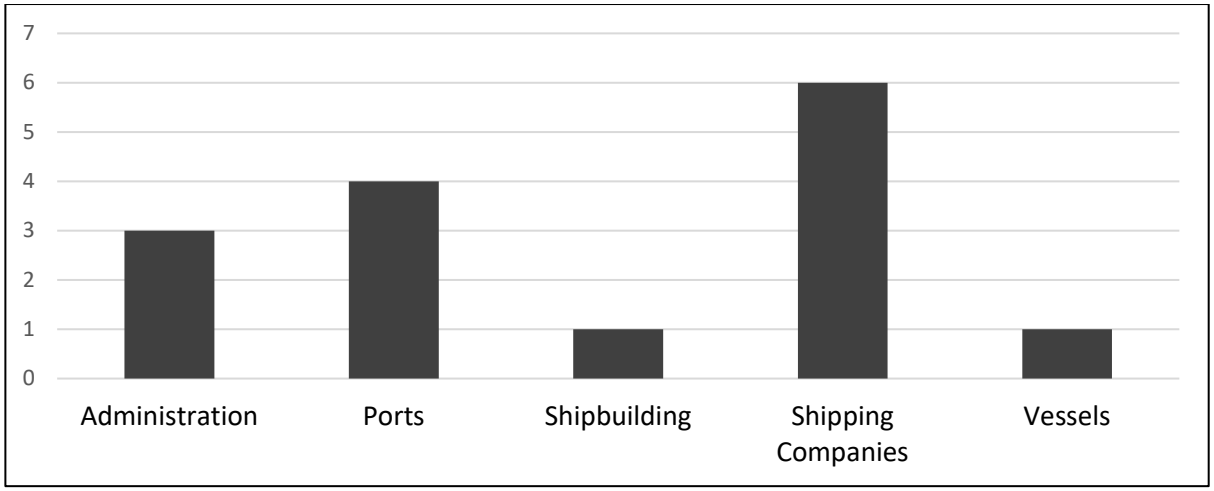

Figure 3: Cyber incidents per MTS asset

As shipping companies, ports, and administration assets incorporate more IT to support their operations, it follows these three MTS assets would be more often targeted in cyberattacks. The shipbuilding and vessels assets of the MTS have more OT deployed and may be harder to target, wittingly or unwittingly, during cyberattacks.

With respect to the adversary customers behind cyberattacks against the MTS assets, Figure 4 shows:

- China was the adversary customer for six of the cyberattacks—four in shipping companies, one in shipbuilding, and one in administration.
- Russia came in second as an adversary customer with three total cyberattacks, including two cyberattacks against ports and one cyberattack against shipping companies.
- Iran was an adversary customer for one cyberattack in administration.
- Israel was an adversary customer for one cyberattack in ports.
- Adversary customers were not known for one incident each in administration, ports, shipping companies, and vessels.

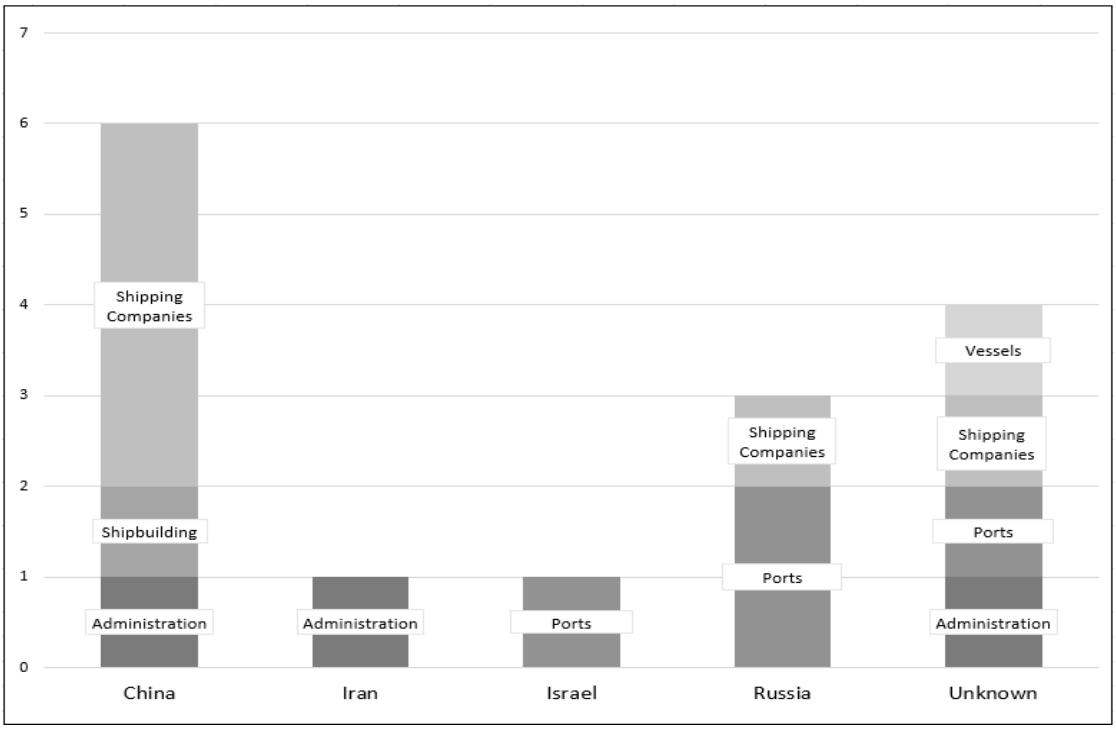

Figure 4: Adversary customer per MTS asset

Looking at the security fundamental compromised across the 15 cyber incidents, Figure 5 shows:

- Availability was compromised in eight of the incidents impacting every MTS asset except shipbuilding.
- Confidentiality was compromised in seven of the 15 cyber incidents impacting administration, shipbuilding, and shipping companies.
- Integrity was not compromised in any of the 15 cyber incidents studied.

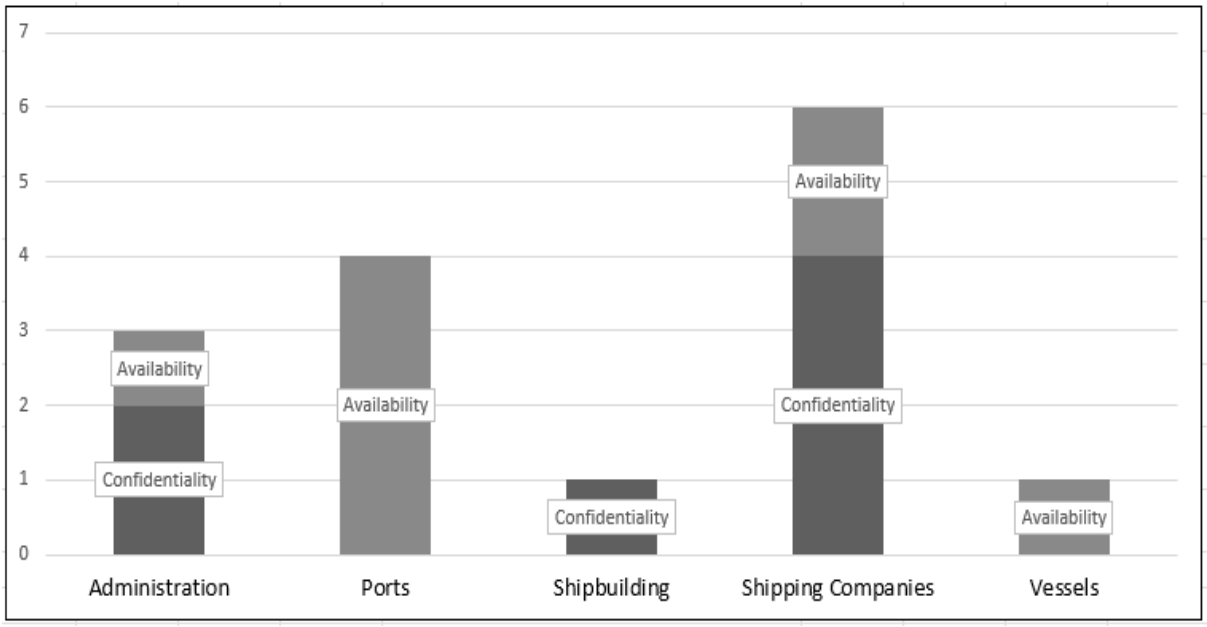

Figure 5: Security fundamental compromised per MTS asset

Last, the adversary's social-political needs per adversary customer, CIA triad aspect, and MTS asset are shown in Figure 6:

- Data exfiltration accounted for six of the cyber incidents in administration (one incident), shipbuilding (one incident), and shipping companies (four incidents).
    - China was the adversary customer for all six data exfiltration incidents.
    - Confidentiality was compromised in all six data exfiltration incidents.
- The second highest social-political need was ransomware at four incidents impacting ports (two incidents) and shipping companies (two incidents).
    - Russia was adversary customer for three ransomware incidents.
    - The adversary customer was unknown for one ransomware incident.
    - Availability was compromised in all four ransomware incidents.
- Political agenda had two incidents with one cyberattack each in administration and ports.
    - Iran was the adversary customer for one political agenda incident.
    - Israel was the adversary customer for one political agenda incident.
    - Confidentiality was compromised in both political agenda incidents.
- Last, three cyberattacks were categorized as unknown needs involving an unknown adversary customer with one incident each in administration, ports, and vessels.

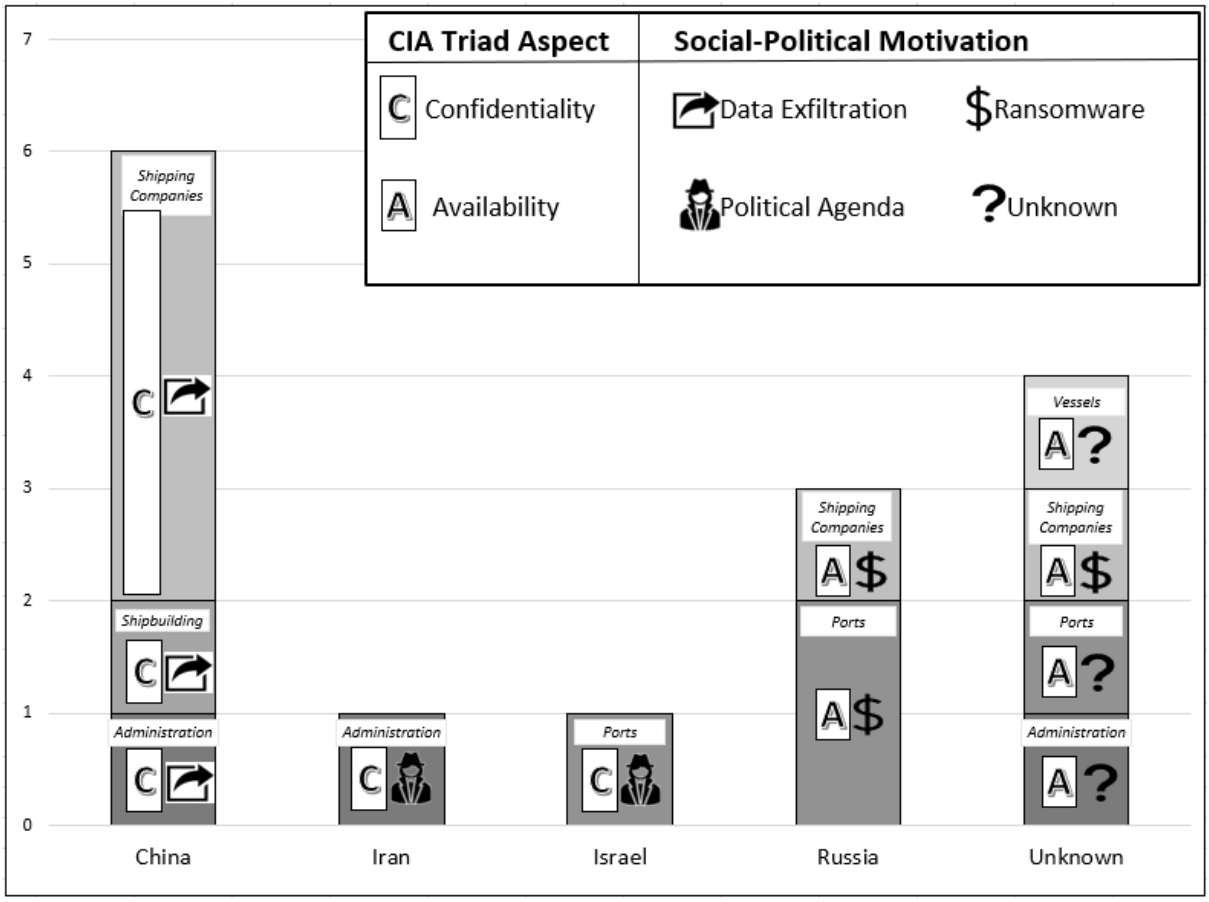

Figure 6: Adversary social-political needs per adversary customer, CIA triad aspect, and MTS asset

5. Conclusion and Future Work

Despite the lack of cyberattacks in publicly available data, this limited exploratory document analysis revealed that commonalities exist for adversaries conducting cyberattacks against the MTS. Data exfiltration and ransomware are concerns for administration, ports, shipbuilding, and shipping companies. Over half of the cyberattacks studied involved adversaries disrupting Availability, with the remaining cyberattacks impacting Confidentiality. China and Russia account for most of the adversary customers in MTS cyberattacks, but some adversary customers were unknown for a few cyberattacks.

Limitations identified during this exploratory document analysis of adversaries conducting cyberattacks against the MTS include:

- An overall lack of knowledge and research about adversaries conducting cyberattacks against the MTS;
- A lack of publicly available datasets for cyberattacks impacting the MTS;
- Information found in the two databases used, CSIS and CFR, provided some data about adversaries but additional details were found in open-source reporting;
- Cyberattack information concerning the MTS is disjointed and found across a variety of sources.

This work can be extended by including additional information from publicly available sources, especially sources focused on or popular across the MTS. Identifying amplifying resources could provide further data on adversaries, including adversary operators, adversary capabilities, and adversary infrastructure. Future research could address identifying the unknown adversary customers, unknown social-political needs, and the lack of information on adversary operators. In addition, future research could identify trends in adversaries' techniques, tactics, and procedures (TTPs) when conducting cyberattacks against MTS assets. Developing a database providing comprehensive data on cyberattacks against the MTS would be beneficial for organizations to identify and implement the appropriate security measures to harden IT and OT against cyber adversaries.

Acknowledgements

The author thanks Dr. Donna Schaeffer for her efforts as their project advisor. Additionally, the author thanks M.D. for reviewing and providing feedback on this paper.

References

Caltagirone, S., Pendergast, A., and Betz, C. (2013) *The Diamond Model of Intrusion Analysis* (Technical Report ADA586960), [online], Center for Cyber Threat Intelligence and Research, https://apps.dtic.mil/sti/pdfs/ADA586960.pdf.

Center for Strategic & International Studies. (n.d.) *Significant Cyber Incidents Since 2006*, [online], https://csis-website-prod.s3.amazonaws.com/s3fs-public/210430_Significant_Cyber_Events_List.pdf?B21zjJhsoO3qkgQNyGMmZN5IhAE80S_I.

Council on Foreign Relations. (2022) *Tracking State-Sponsored Cyberattacks Around the World*, [online], https://www.cfr.org/cyber-operations.

Dickerson, S. (2021) *The MTS-ISAC and NORMA Cyber Strengthen Information Sharing Ties*, [online], EIN News, https://www.einnews.com/pr_news/545608768/the-mts-isac-and-norma-cyber-strengthen-information-sharing-ties.

Paté-Cornell, M.-E., Kuypers, M., Smith, M., and Keller, P. (2018) "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies," *Risk Analysis: An International Journal* [online], Vol. 38, No. 2, February, pp 226–241, https://doi.org/10.1111/risa.12844.

Statista Research Department. (2022) *Container Shipping – Statistics & Facts,* [online], https://www.statista.com/topics/1367/container-shipping/.

Tam, K., and Jones, K. D. (2019) "Situational Awareness: Examining Factors That Affect Cyber-Risks in the Maritime Sector," *International Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp 40–68.

Tam, K., Moara-Nkwe, K., and Jones, K. (2021) "A Conceptual Cyber-Risk Assessment of Port Infrastructure," *2021 World of Shipping Portugal: An International Research Conference on Maritime Affairs [online]*, 28-29 January, https://pearl.plymouth.ac.uk/handle/10026.1/16704.

Vanguard News. (2020). *Maritime cyber attacks increase by 900% in three years*, [online], https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years/.