UNDERWAY TO IDENTIFYING COMMONALITIES OF CYBERSECURITY INCIDENTS IN THE MARITIME TRANPSORTATION SYSTEM

Rebecca J. Rohan
August 10, 2024

Agenda

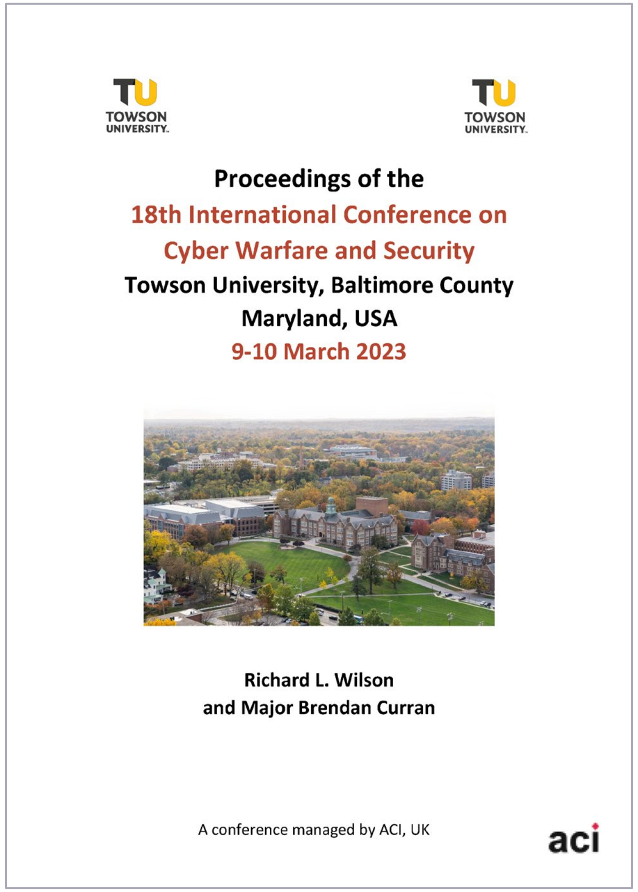
- Introduction
- Related Work
- Methodology and Research Design
- Results and Discussion
- Conclusion, Limitations, and Future Work
- Questions

Introduction

Image Credit: Michael A. McCoy for The Washington Post via Getty Images / Getty Images

Related Work

- Previously published initial work in *Identifying Commonalities of Cyberattacks Against the Maritime Transportation System (MTS)* in March 2023.
- Lack of research informing the MTS about trends in cybersecurity incidents:
  - What are the commonalities?
  - How are MTS systems affected?
  - Where should MTS resources be focused?
  - What tactics, techniques, and procedures (TTPs) are used?



TU TOWSON UNIVERSITY

TU TOWSON UNIVERSITY

Proceedings of the
18th International Conference on
Cyber Warfare and Security
Towson University, Baltimore County
Maryland, USA
9-10 March 2023

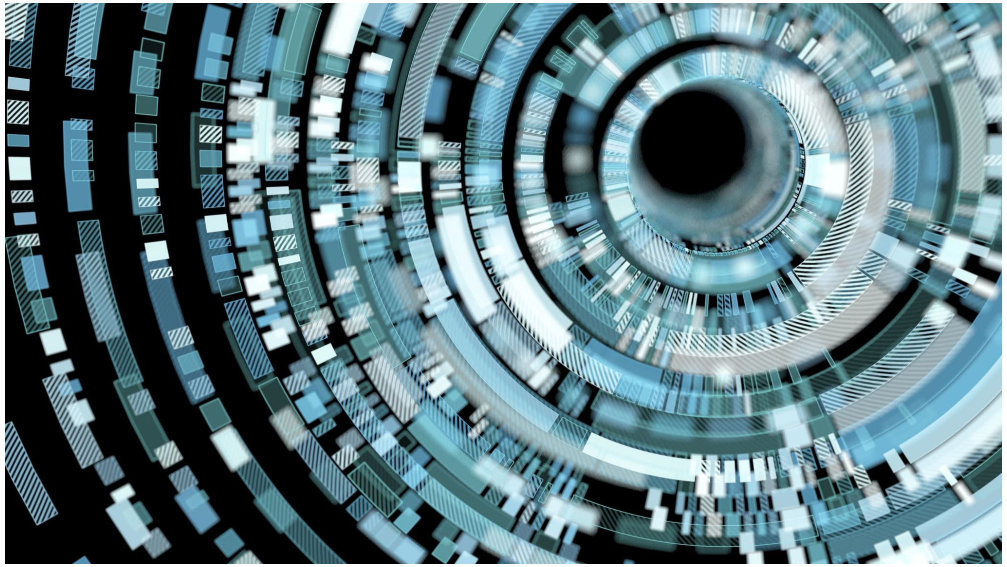
Richard L. Wilson
and Major Brendan Curran

A conference managed by ACI, UK

aci

Methodology and Research Design - 1

- Combine models and concepts to develop a more comprehensive threat picture
  - Diamond Model of Intrusion Analysis:
    - Adversary
    - Victim
    - Social-Political Needs
  - Parkerian Hexad:
    - Confidentiality-Integrity-Availability (CIA) Triad plus:
      - Possession
      - Authenticity
      - Utility
  - MITRE ATT&CK Framework:
    - Tactics
    - Techniques

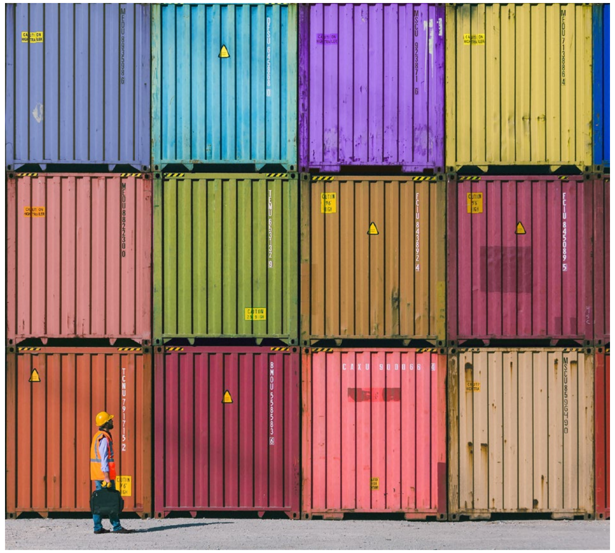


Methodology and Research Design - 2

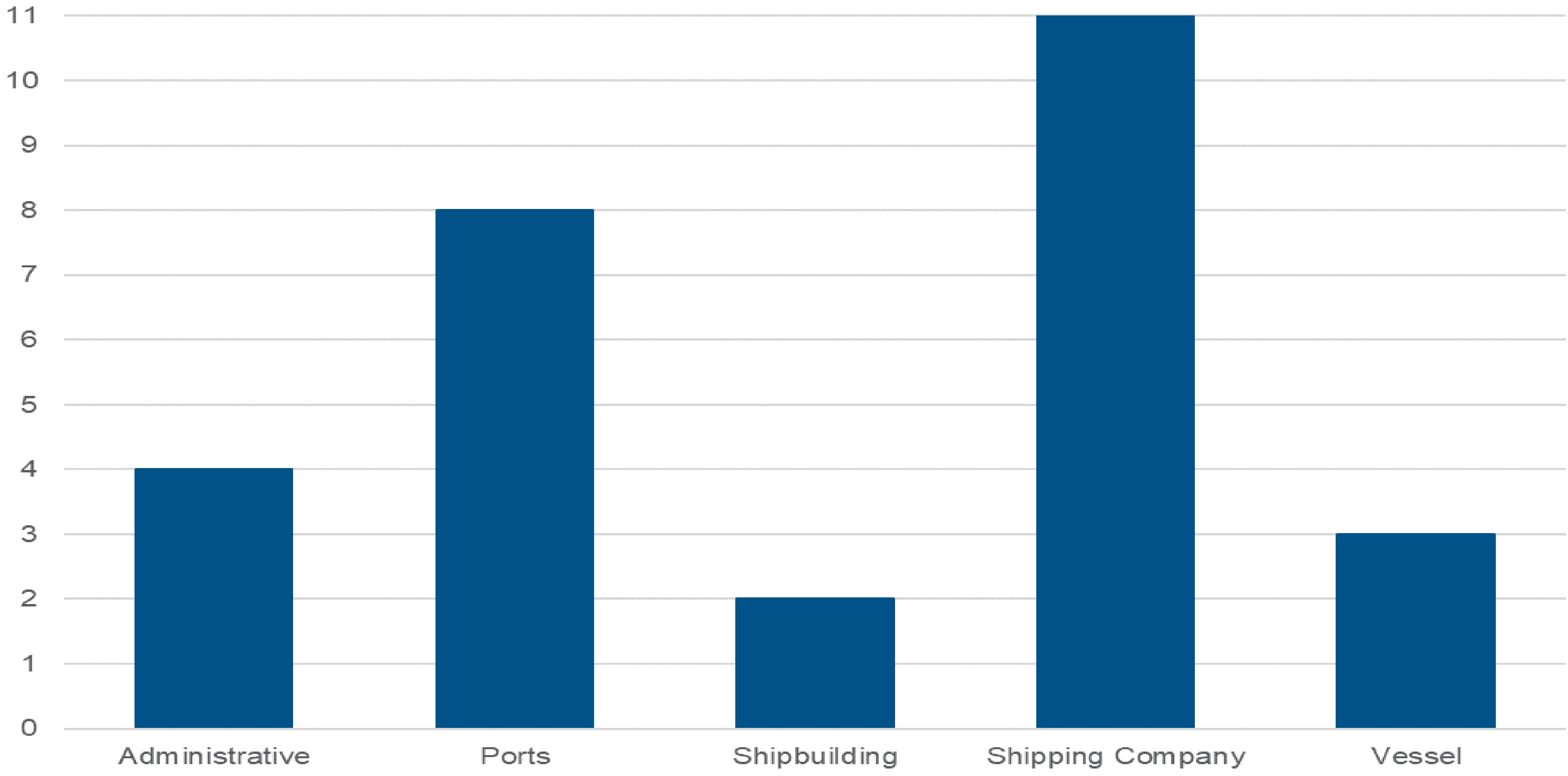
- Limited, exploratory document analysis expanding upon prior research using:
  - Center for Strategic and International Studies' (CSIS') *Significant Cyber Incidents*
    - 2006-Present: Cyberattacks against defense sector, government agencies, technology companies, and economic crimes ($1M+)
  - Council on Foreign Relations' (CFR') Cyber Operations Tracker
    - 2005-Present: Publicly known, state-sponsored cyber incidents
- Combined entries from CFR and CSIS
- Removed duplicates or entries lacking specific keywords—*maritime, port(s), logistics, ship, shipping, shipbuilder, terminal, vessel*
- Discarded entries related to military operations--*submarines, navy,*

Results and Discussion

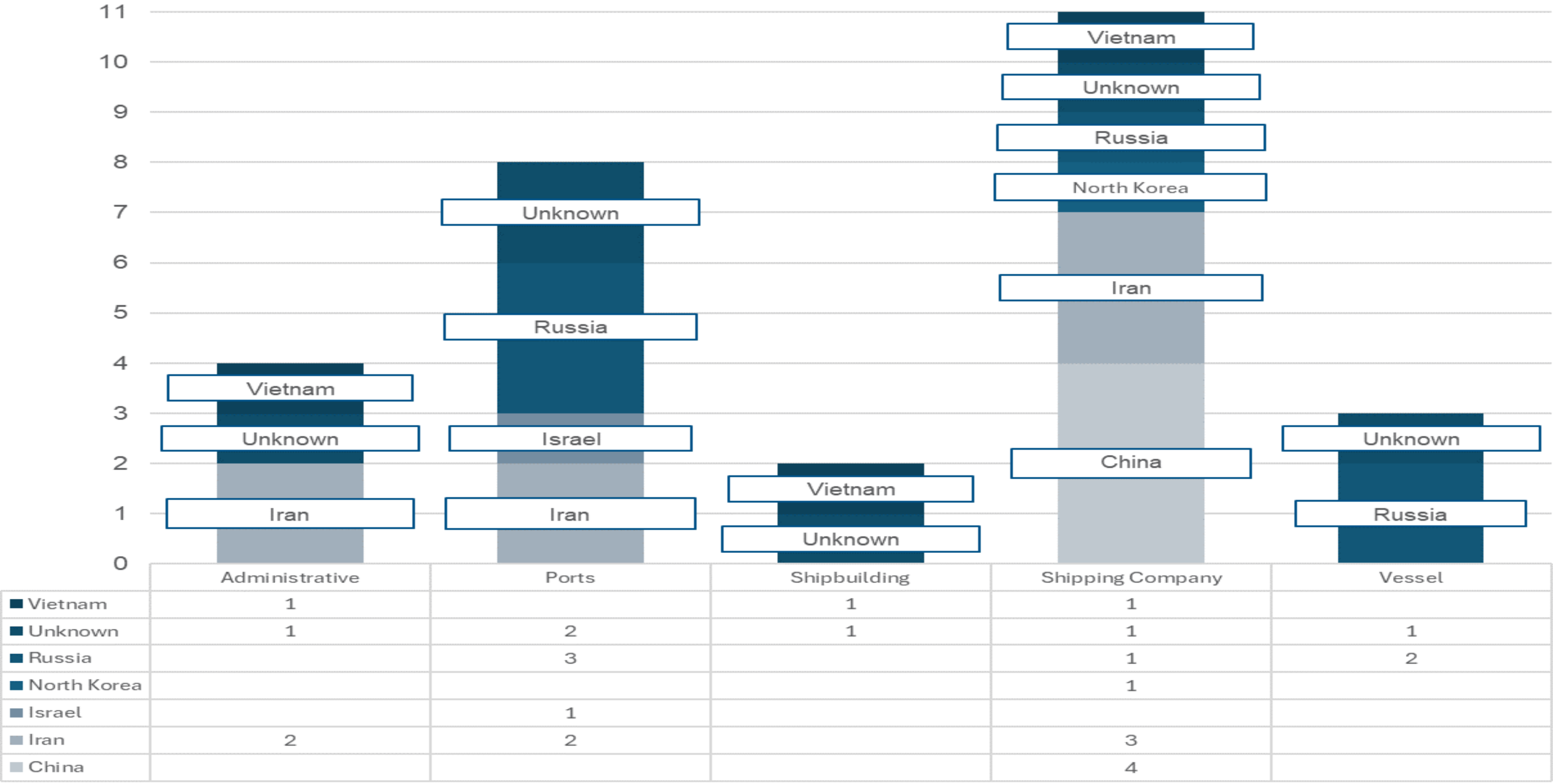
- MTS Aspect:
  - Administrative: maritime entity providing software or other support
  - Ports: ports/terminals where cargo is loaded/unloaded
  - Shipbuilding: companies building ships or equipment used by MTS
  - Shipping Company: company handling business or physical aspects of moving cargo
  - Vessel: a ship or merchant vessel transporting cargo
- Adversary:
  - Country
  - Social-Political Need
- Parkerian Hexad Element
- MITRE ATT&CK Tactic/Technique



Cyber Incidents per MTS Aspect

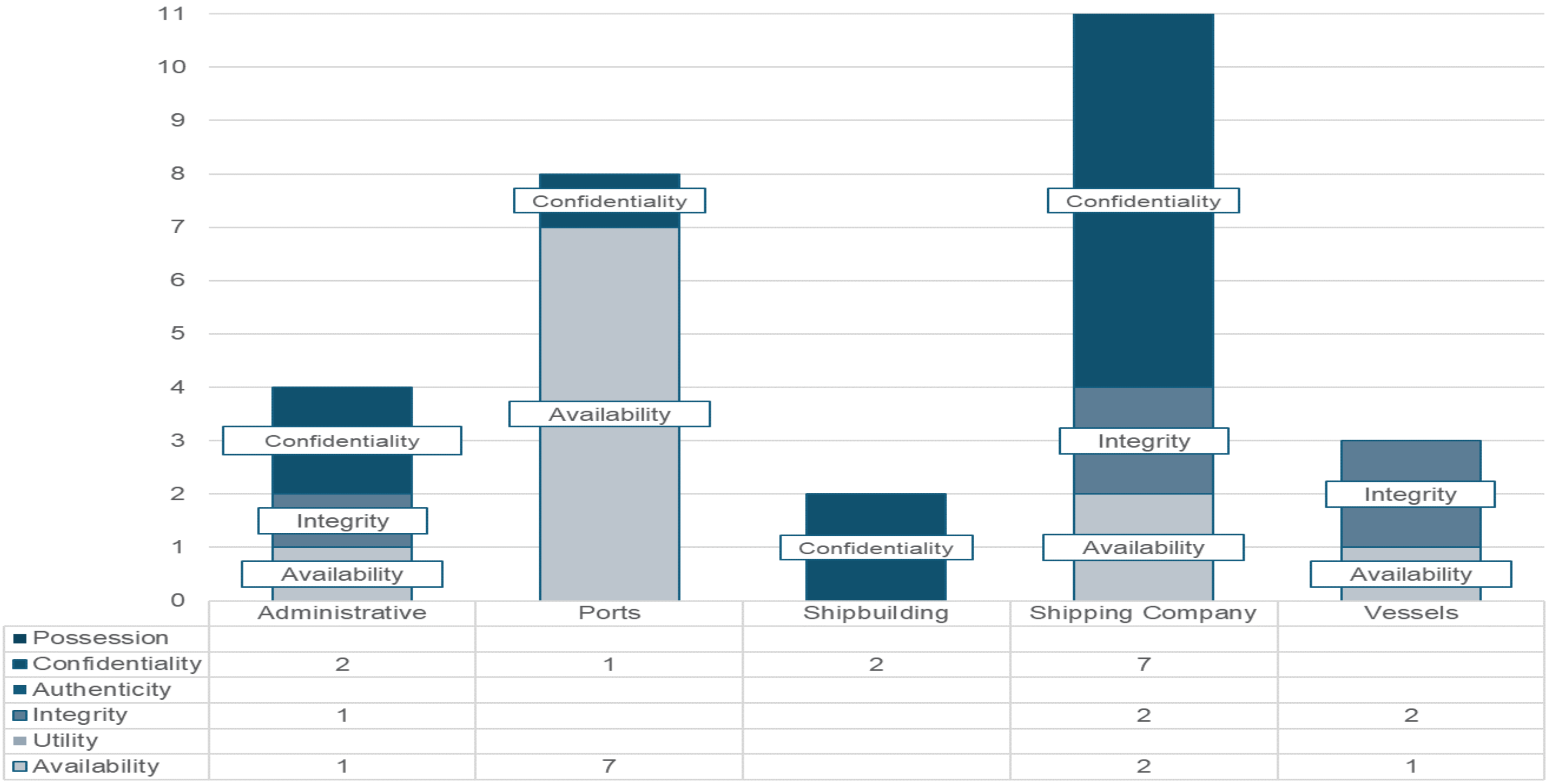


Adversary Customer per MTS Aspect



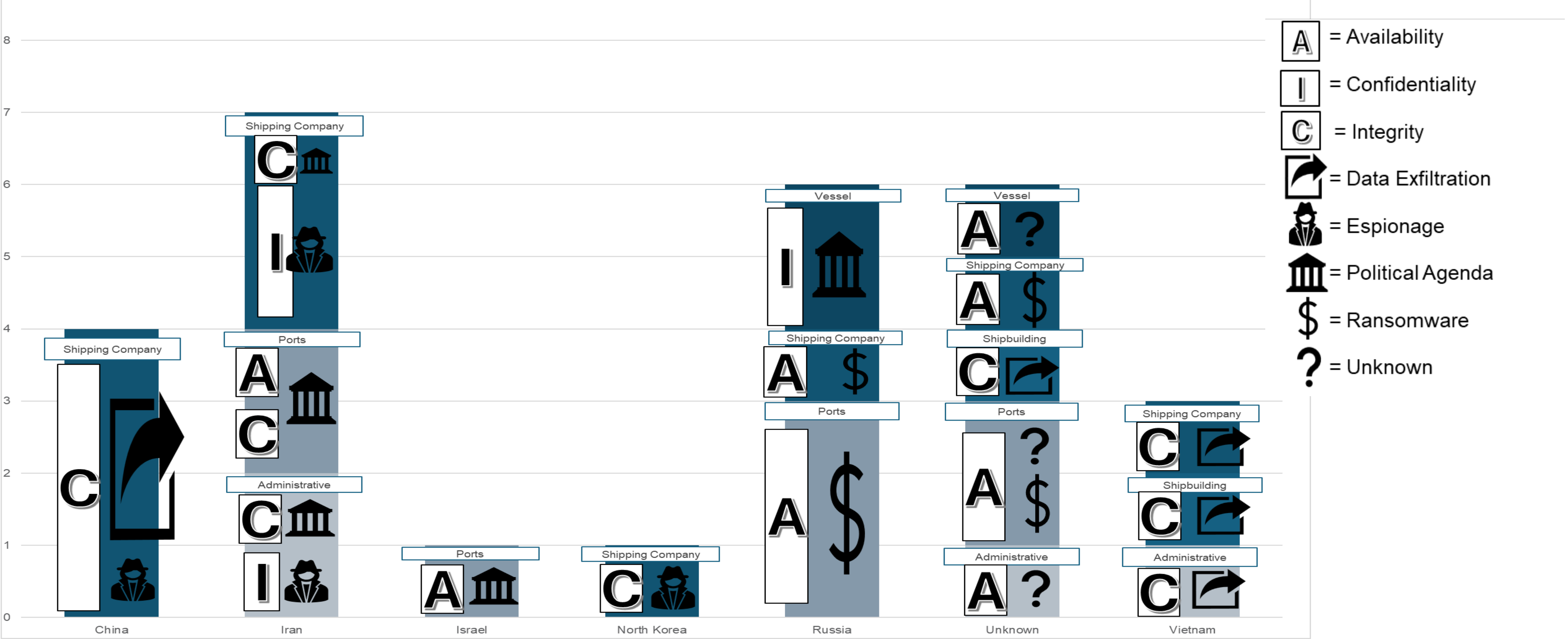
	Administrative	Ports	Shipbuilding	Shipping Company	Vessel
■ Vietnam	1		1	1	
■ Unknown	1	2	1	1	1
■ Russia		3		1	2
■ North Korea				1	
■ Israel		1			
■ Iran	2	2		3	
■ China				4	

Parkerian Hexad Element per MTS Aspect

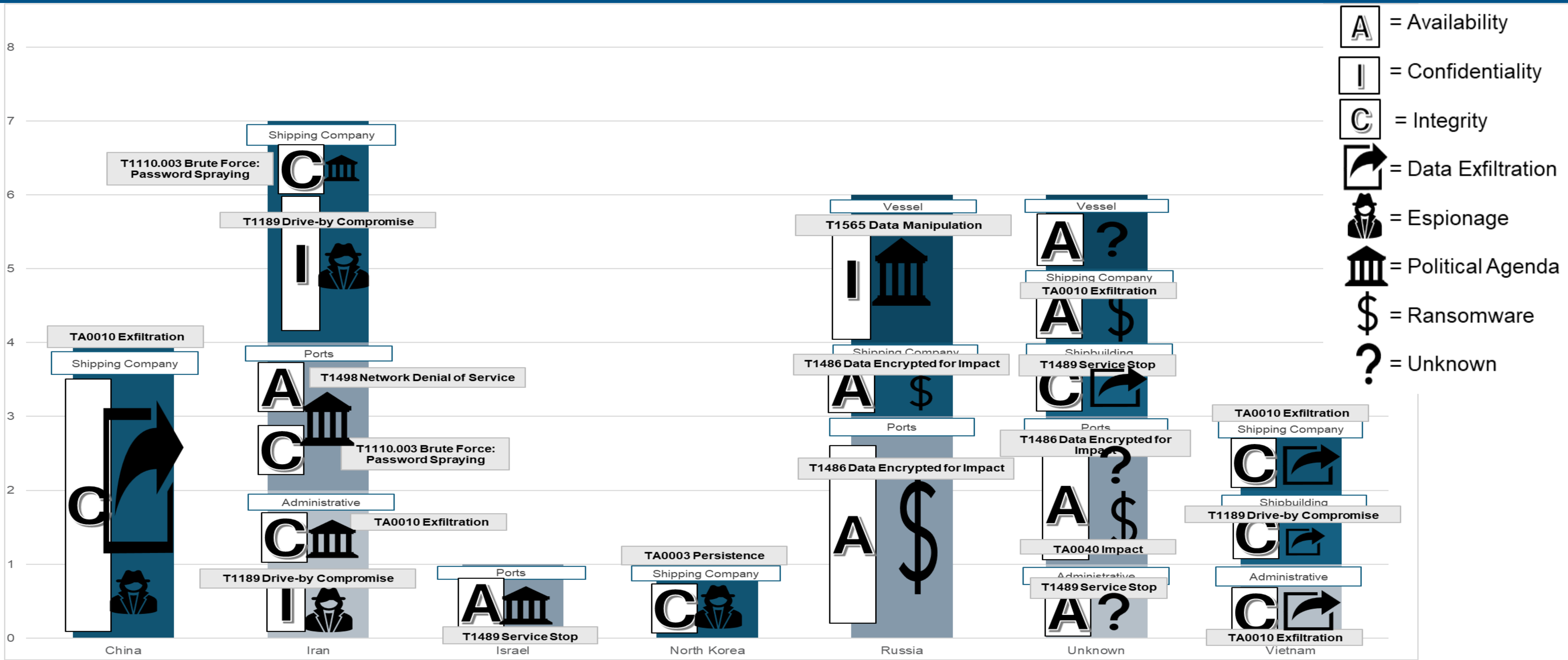


	Administrative	Ports	Shipbuilding	Shipping Company	Vessels
■ Possession					
■ Confidentiality	2	1	2	7	
■ Authenticity					
■ Integrity	1			2	2
■ Utility					
□ Availability	1	7		2	1

+ Social-Political



MITRE ATT&CK Tactics & Techniques



Conclusion, Limitations, and Future Work

- Conclusion: Commonalities do exist in cyberattacks against the MTS
- Limitations:
  - Lack of publicly available data
  - Available MTS cybersecurity incident information is disjointed across a myriad of sources
  - Did not include military operations
- Future Work:
  - Establish guidelines for categorizing MTS Aspect, Parkerian Hexad, Social-Political Need, and MITRE ATT&CK Tactics/Techniques
  - Expand work to include military
  - Incorporate additionally publicly available data, such as the Maritime Cyber Attack Database maintained by NHL Stenden University of Applied Sciences

For more information:
www.cisa.gov

Questions?
Email: rebecca.rohan@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA