

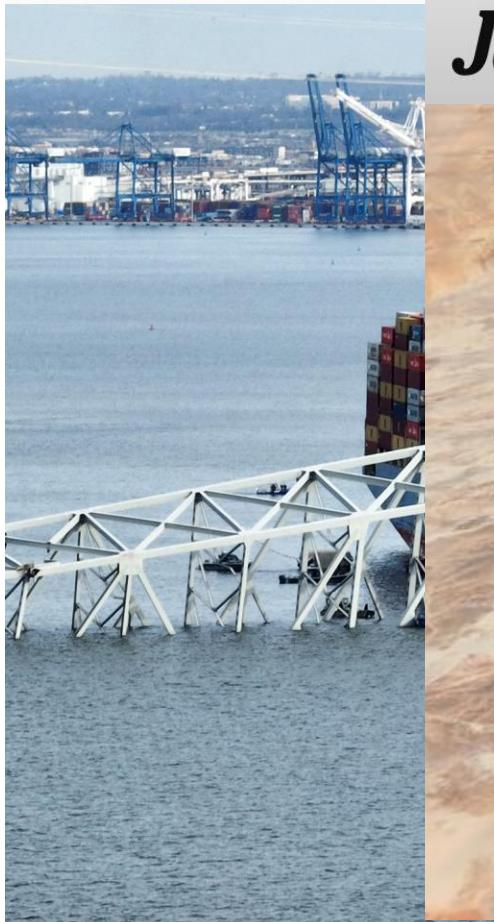
A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners

Anna Raymaker, Akshaya Kumar, Miuyin Yong Wong, Ryan Pickren,
Animesh Chhotaray, Frank Li, Saman Zonouz, Raheem Beyah



Motivation: Impact of Shipping on the Globe

Francis Scott Key E
Ship "DALI."



SHIPPING 101

Approximately 90% of the world's trade is transported by sea through shipping containers.

A large blue and white container ship is shown from an aerial perspective, heavily loaded with shipping containers. It is being towed by two small tugboats, one on each side, creating a wake in the dark blue ocean. The ship's superstructure is visible, featuring a yellow mast and various equipment. The text "rollingcargo.co.ke" is printed on the side of the ship. The overall scene illustrates the scale and complexity of global shipping operations.

ROLLING CARGO
Your Shipping Partner

CERTIFIED BY ISO ACCREDITED BY AEO KENYA CUSTOMS

Motivation: Growing Cybersecurity Threats

FACT SHEET: DHS Moves to Improve Supply Chain Resilience and Cybersecurity Within Our Maritime Critical Infrastructure

Release Date: February 21, 2024

Today, the Department of Homeland Security (DHS) and the Biden-Harris Administration are taking [new actions](#) to protect American maritime critical infrastructure, bolster port cybersecurity, and improve supply chain resilience.

As a maritime nation, America's prosperity remains inextricably linked to the integrated and extensive network of ports, terminals, vessels, waterways, and land-side connections constituting the U.S. Marine Transportation System (MTS). This extensive system supports \$5.4 trillion worth of economic activity each year and contributes to the employment of more than 31 million Americans.

DHS has a strong and demonstrated track record in securing and safeguarding the maritime transportation system. Through existing security and safety regulations, DHS and its partners have forged a robust public-private partnership through contingency planning, exercises, grant funding, and response and recovery efforts. These relationships are all the more important as the industry and the country faces evolving cyber and technology challenges.

We have a national imperative to protect this critical infrastructure in a complex threat environment. MTS operators increasingly rely on an ecosystem of automated and cyber-dependent systems to enable critical operating functions, including ship navigation, engineering, safety and security monitoring. These systems have revolutionized the maritime shipping industry by centralizing operational control and improving efficiency. However, they also introduce vulnerabilities that, if exploited, could have significant cascading impacts to the MTS, the economy, and the American people.

Cybercrime

MarineTraffic / Ash Martin

software

Limited Prior Work in Maritime Cybersecurity

2020 IEEE Symposium on Security and Privacy

A Tale of Sea and Sky On the Security of Maritime VSAT Communications

James Pavur*, Daniel Moser†, Martin Strohmeier†, Vincent Lenders† and Ivan Martinovic*

*Oxford University

Email: first.last@cs.ox.ac.uk

†armasuisse

Email: first.last@armasuisse.ch

Marine Network Protocols and Security Risks

by Ky Tran  , Sid Keene  , Erik Fretheim   and Michail Tsikerdekis *  

Computer Science Department, Western Washington University, Bellingham, WA 98226, USA

* Author to whom correspondence should be addressed.

J. Cybersecur. Priv. **2021**, 1(2), 239-251; <https://doi.org/10.3390/jcp1020013>

Cyber Physical Systems Security for Maritime Assets

by Iosif Progoulakis ^{1,*}  , Paul Rohmeyer ²  and Nikitas Nikitakos ¹ 

¹ Department of Shipping Trade and Transport, University of the Aegean, Korais St. 2A, GR 82132 Chios, Greece

² School of Business, Stevens Institute of Technology, 1 Castle Point on the Hudson, Hoboken, NJ 07030, USA

* Author to whom correspondence should be addressed.

J. Mar. Sci. Eng. **2021**, 9(12), 1384; <https://doi.org/10.3390/jmse9121384>

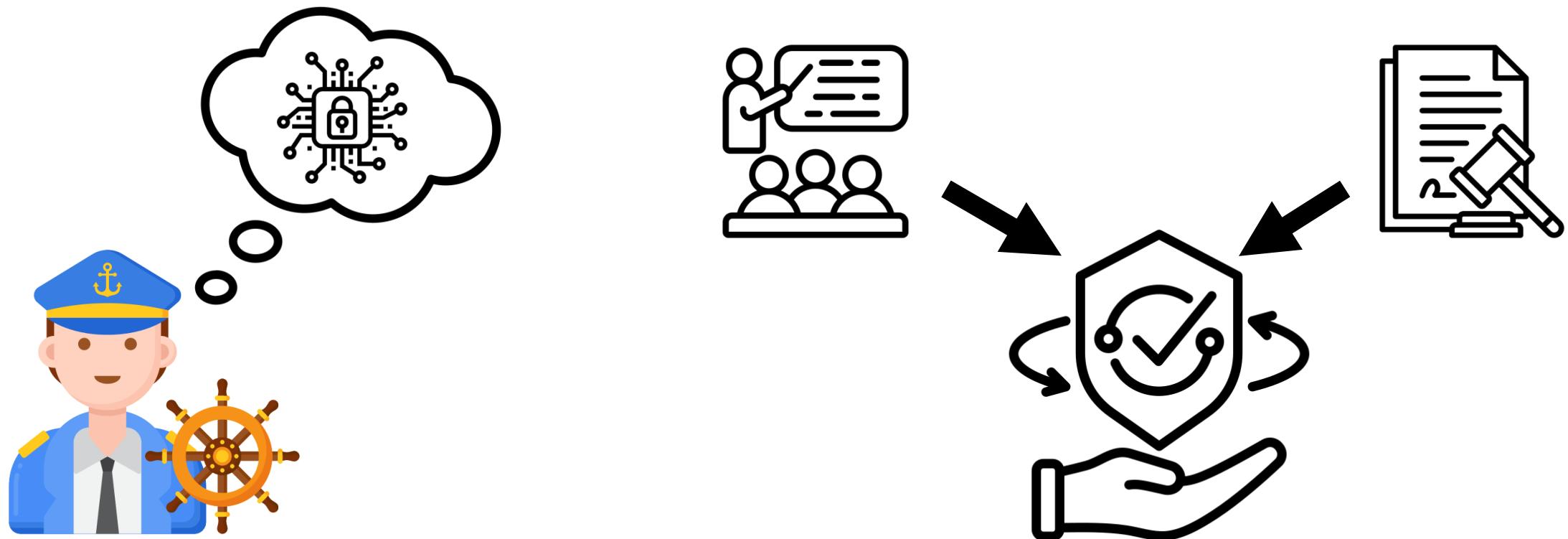
Closing the Research Gap

- Focus on the **human perspective**
- Goal: Expose what problems mariners face in practice



Questions to Investigate

- **RQ1:** What are mariners' perceptions of cybersecurity?
- **RQ2:** What are mariners' cybersecurity practices, and what role do training and regulation play in shaping these practices?



Perceptions

RQ1



Threats

RQ1



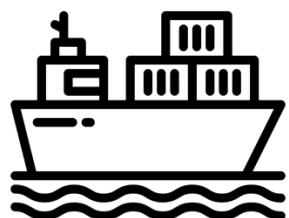
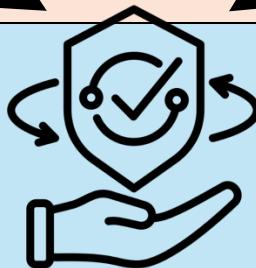
Training

RQ2



Regulation

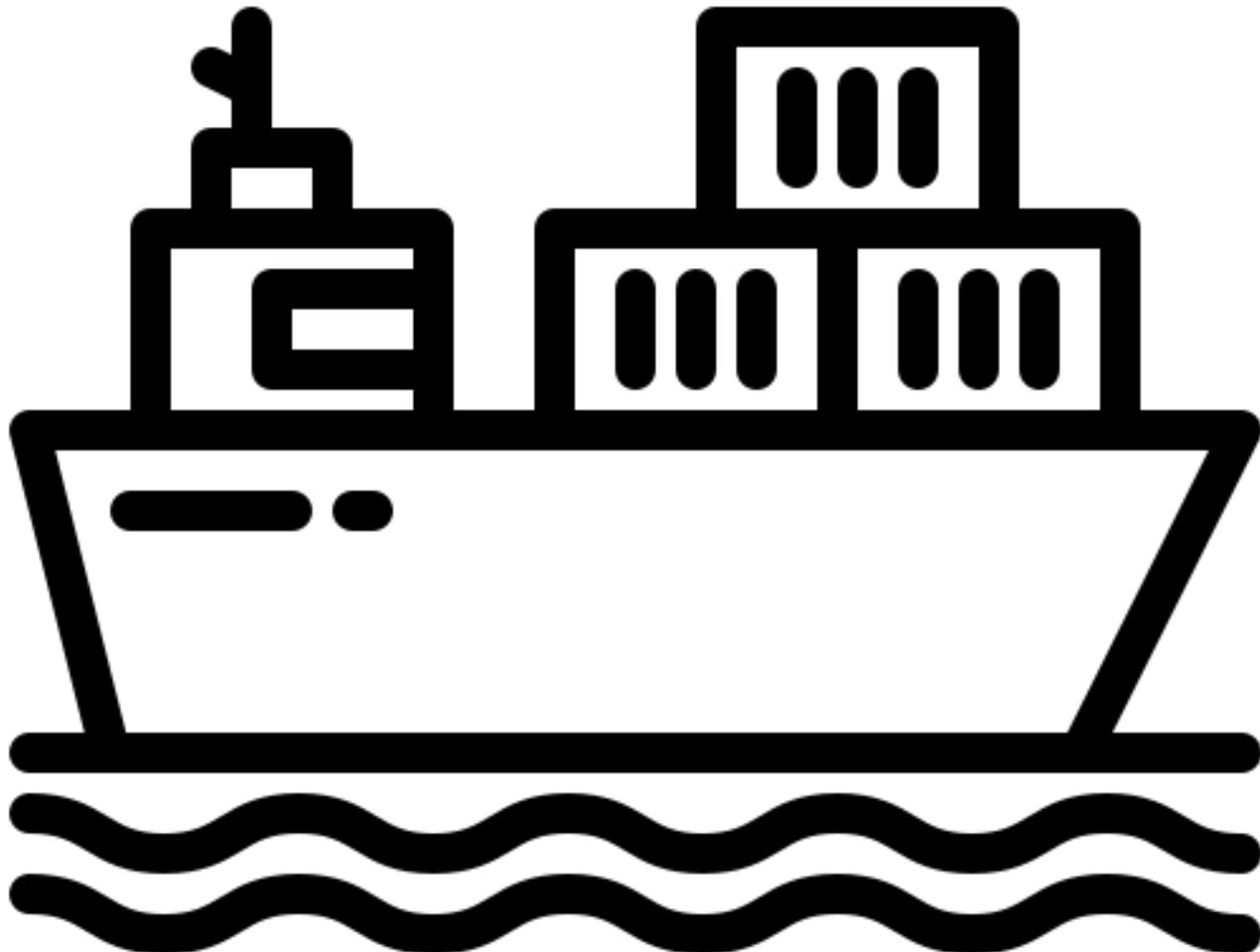
RQ2



Recommendations

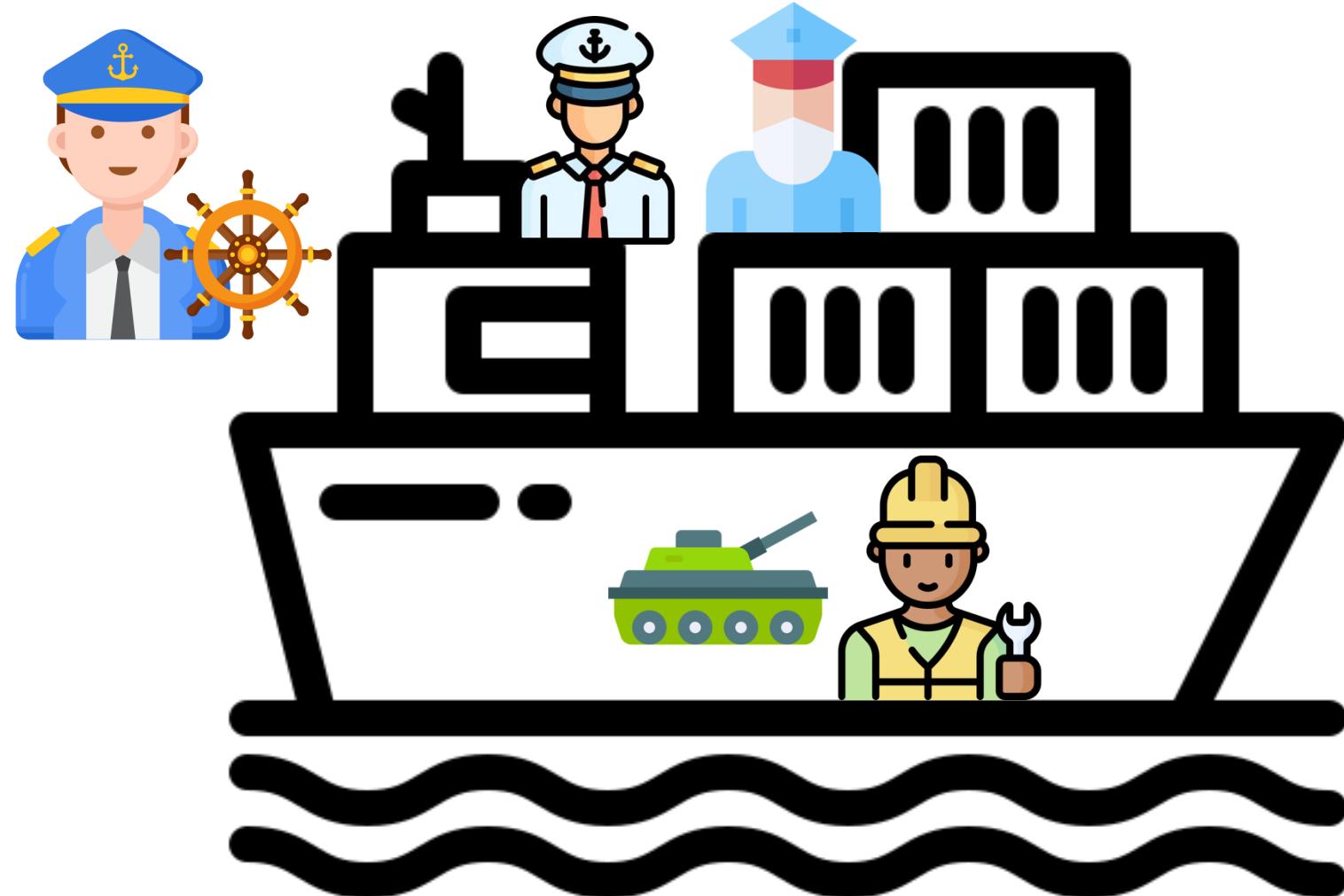
Method

- Semi-structured interviews
- **Recruitment:** gCaptain, Reddit, LinkedIn, and snowballing
- **Analysis:** qualitative coding with two coders, iterative refinement, saturation reached



Participant Demographics

- Interviewed 21 **officer-level** mariners
- Civilian + Military backgrounds
- Broad ages (20s to 70s!)
- Diverse ship types (cargo, passenger, cable, etc.)



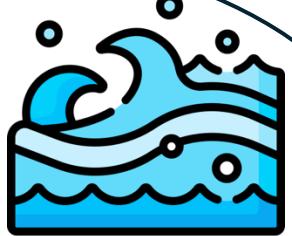
What did we find?

First, we found that mariners are up against steep challenges and difficult working conditions....

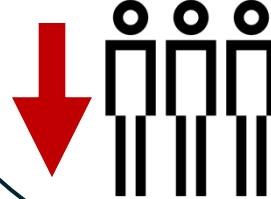


No Time Left for Cybersecurity

Months away at sea



Exhausting hours, little rest

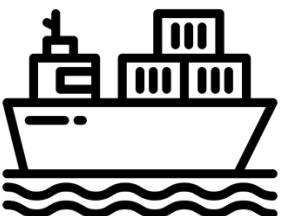


Smaller crews, heavier burden



Constant physical and safety risks

"If you're working 12 hours a day for 90 days... after 40 days you're not as alert and you just don't care." (P6)

Perceptions	Cybersecurity is seen as secondary to physical security	Recommendations
RQ1		
Threats	RQ1	
Training	RQ2	
Regulation	RQ2	
		

Mariner-Identified Threat Categorization

Threat Types

Threat Vectors

Vulnerable Times

Vulnerable Systems
and Devices

Impacted Assets

Consequences

Our framework bridges mariner experiences with industry standards

Unprompted, Emerging Threats

Generational gap: old vs. new practices

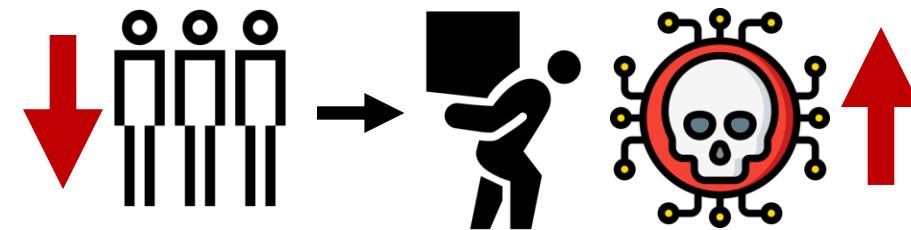


"If you don't have charts and you're being spoofed, you're a little screwed" (P18)

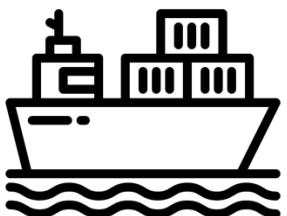
Starlink: faster, but
unmanaged connectivity



Automation: fewer crew,
heavier burden, more threats



Perceptions	Cybersecurity is seen as secondary to physical security	Recommendations
RQ1		
Threats	From GPS to Starlink, mariners see growing, unmanaged cyber risks	
RQ1		
Training	RQ2	
Regulation	RQ2	

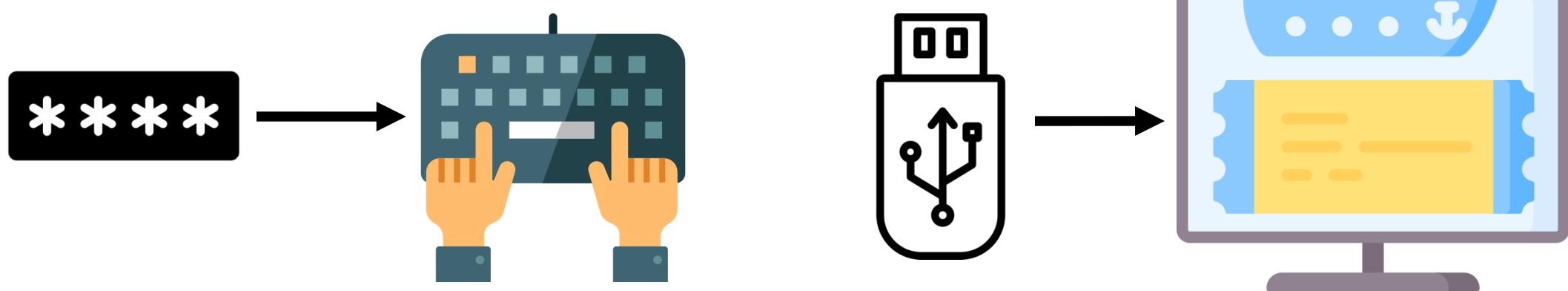


Training Fails to Prepare Mariners for Threats

- All 21 mariners had generic, non-ship-specific training
- 14 reported no cyber response plan at all

“[The training] didn’t even really say how to identify a cyber-attack; it talks a lot about flash drives.” (P9)

- 8 admitted to unsafe practices



Perceptions	Cybersecurity is seen as secondary to physical security	Recommendations
RQ1		
Threats	From GPS to Starlink, mariners see growing, unmanaged cyber risks	
Training	Training is generic, not role-specific, and often ignored	
RQ2		
Regulation		
RQ2		



Regulations Matter, But Don't Fit the Crew

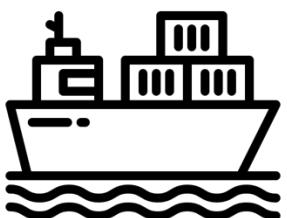
- 15/21 Mariners found regulations to be essential

"Most of the standards, regulations that we have in the maritime industry... are written in blood and oil. Mariners pay for it with their blood, sweat, and tears" (P7)

- 11/21 see regulations as burdensome
- 7/21 one-size-fits-all, not adequate for small crews
- Only 10/21 aware of IMO cyber regulations

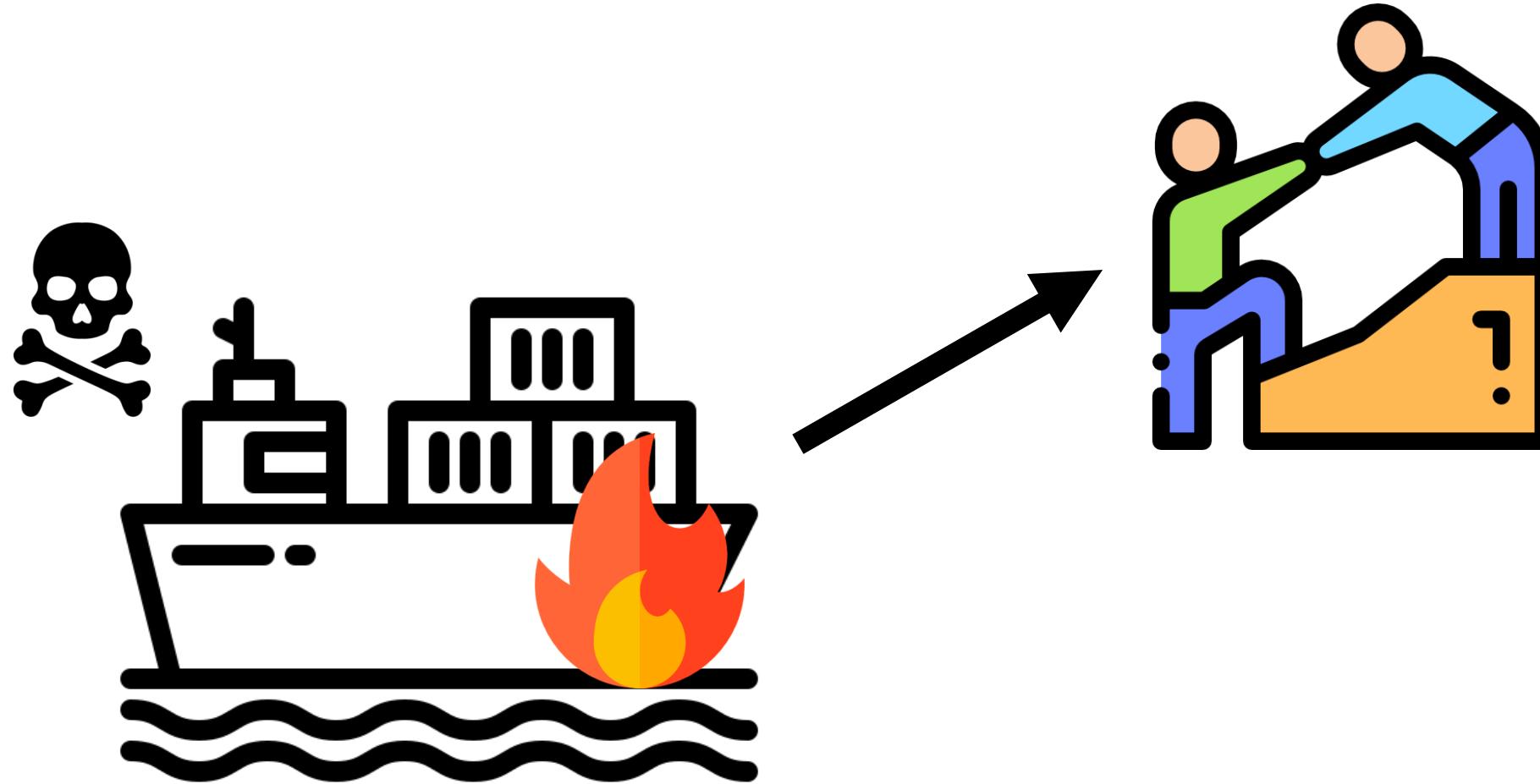
"A lot of retired Navy guys. . . they're writing the regulation. But they're writing it based off the Navy way of doing stuff with a 5,000 person crew on [an] aircraft carrier versus a 20 or 12 person crew" (P6)

Perceptions	Cybersecurity is seen as secondary to physical security	Recommendations
RQ1		
Threats	From GPS to Starlink, mariners see growing, unmanaged cyber risks	
Training	Training is generic, not role-specific, and often ignored	
RQ2		
Regulation	Standards are reactive, burdensome, and not tailored to ships	
RQ2		



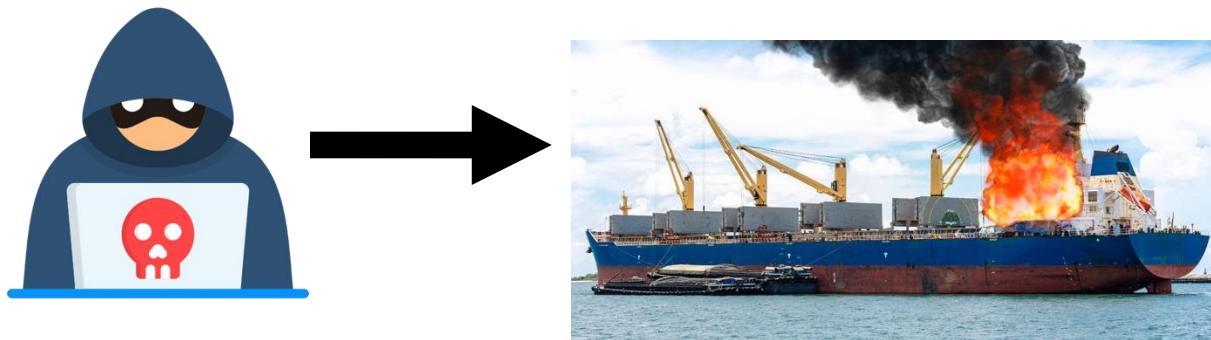
A lot to improve... but there's hope!

There's also clear ways we can help mariners....



Recommendations

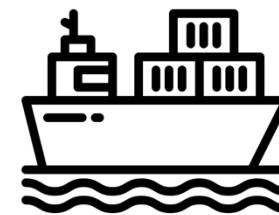
1. Connect cyber threats to real-world safety impacts



2. Deliver practical, role-specific training



3. Align regulations with operational realities



See paper for more details!

A Brighter Future at Sea

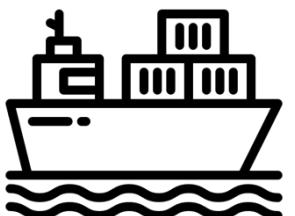
Safer ships, empowered mariners, resilient seas



Our Maritime Testbed

Turning
stories into
systems....



Perceptions	Cybersecurity is seen as secondary to physical security	Recommendations
RQ1		
Threats	From GPS to Starlink, mariners see growing, unmanaged cyber risks	
Training	Training is generic, not role-specific, and often ignored	<ol style="list-style-type: none"> 1. Connect cyber to physical consequences 2. Deliver practical, role-specific training 3. Align regulations with real-world conditions
Regulation	Standards are reactive, burdensome, and not tailored to mariners	
	<p>Contact me!!</p> <p>Email: araymaker3@gatech.edu</p>	