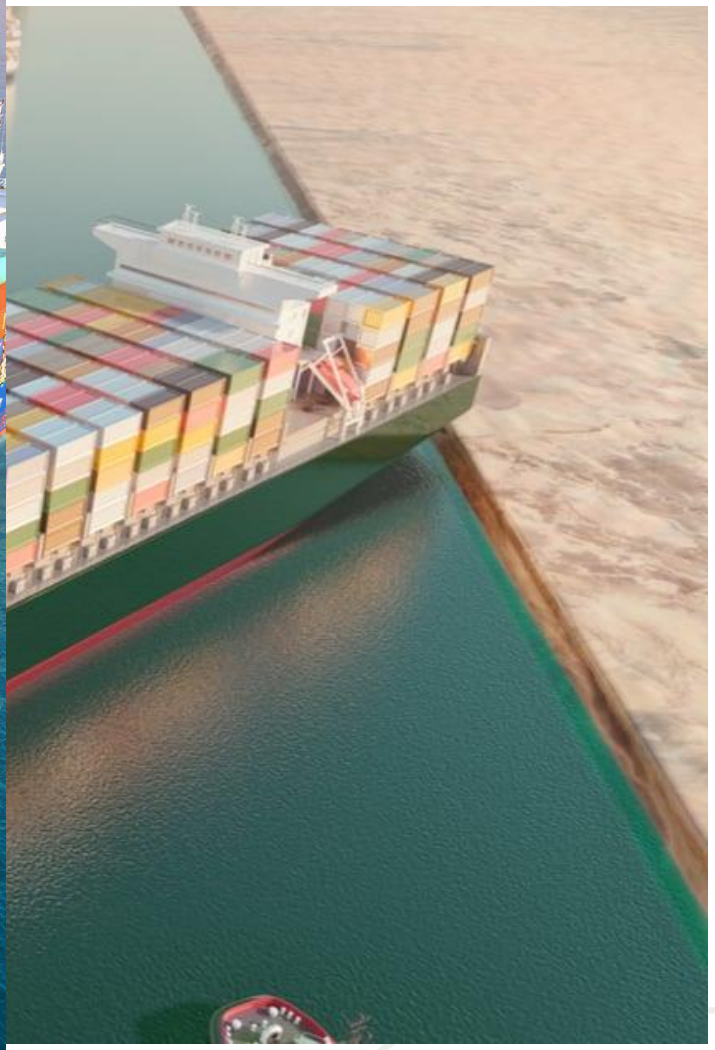
Maritime Cybersecurity in the CPSec Lab

Raheem Beyah, Animesh Chhotaray, Frank Li, Ryan Pickren, Anna Raymaker, Ryan Von Brock, Saman Zonouz

Georgia Tech

Motivation 1: Impact of Shipping on the Globe



Georgia Tech

Motivation 2: Increasing 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.

software

Summary of Work (1.5 years)

Progress

- Fully outfitted maritime cybersecurity testbed *(live demo today)*
- User study published at CCS
- Mutiny malware research under submission

Invited talks and presentations

- TED Talk (Last Spring)
- Level Zero Conference (Last Spring)
- User study presentation - Taiwan (October)
- ICS security talk - (October)
- Government of Singapore - testbed demo (November)

Ongoing Projects

- Military mariner user study
- GPS spoofing measurement study

First Published Work: A Sea of Cyber Threats

21 officer-level mariners interviewed

- 10 reported **direct cyberattacks** (GPS/AIS spoofing)
- 21 reported **generic training** with no OT connection
- 14 said **no cyber response plan** on their ship
- 11 mentioned **unsafe cyber practices**
  - Contractor USBs, passwords on keyboards, unmanaged Starlink
- 11 viewed **regulations** as **burdensome and impractical**

Georgia Tech

Voices from the Mariners

“I’ve been cyber-attacked by Iran… viciously spoofed into Iranian waters.” (P2)

“Our cybersecurity training was just a PowerPoint about flash drives.” (P9)

“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)

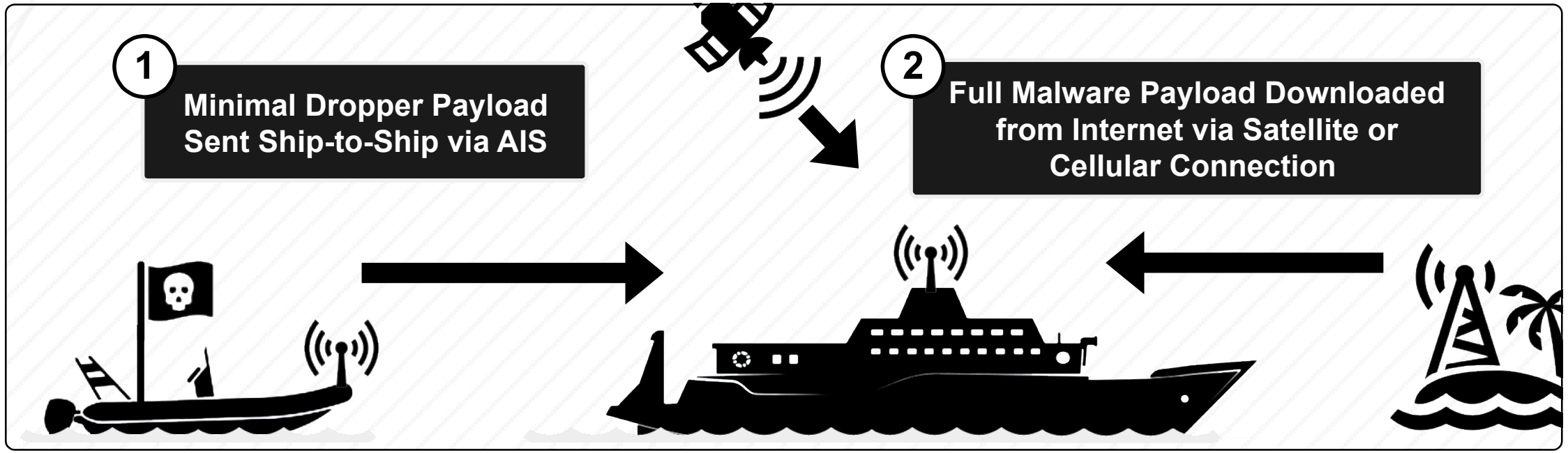
“I can operate my vessel remotely… if I can do that from a thousand miles away, so can somebody else.” (P4)

“If somebody was smart enough… they could bring the maritime world to a crawl. It’s probably a matter of time.” (P9)

Georgia Tech

Mutiny Worm: A Self-Spreading Maritime Malware

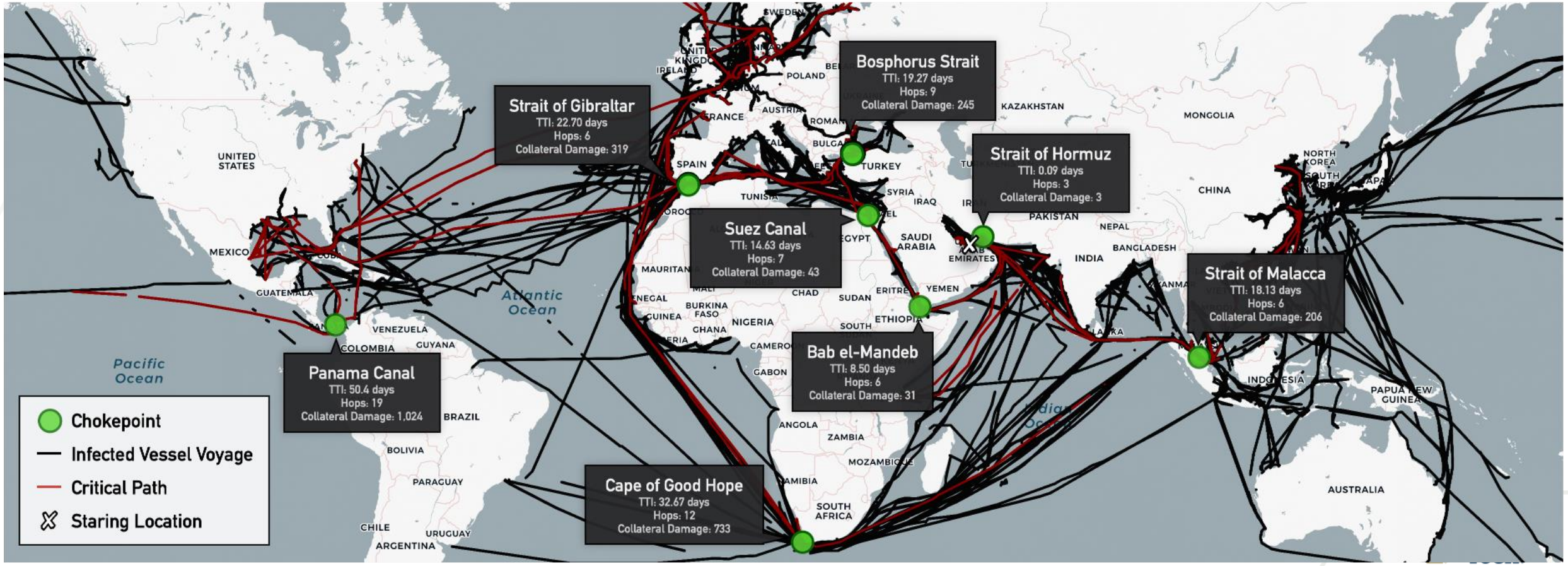
- Ship-to-ship malware that spreads via **AIS broadcasts**, requiring no internet.
- Can **manipulate navigation, steering, and onboard systems** remotely.
- Exposes critical risks in **unsecured maritime communication protocols**.



Georgia Tech

Mutiny Enables Global Takeover

- Regardless of where Mutiny is deployed, it can reach a major global chokepoint in an average of 29.5 days with only a 1% infection rate of ships.



Talks on Maritime Cybersecurity

- TED Talk (Last Spring)
- CCS presentation - Taiwan (October)
- ICS security talk - (October)
- Government of Singapore - testbed demo (November)

In Progress: Military Mariner User Study

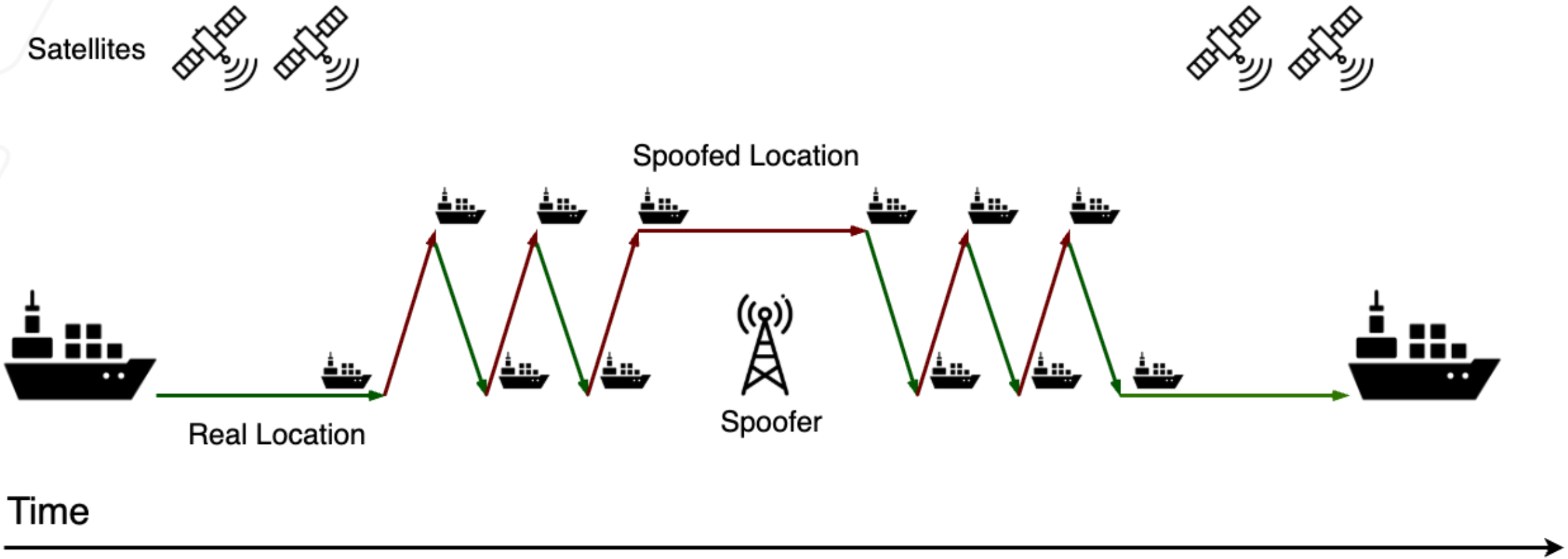
- 5 interviews with Coast Guard deck watch officers

Early Insights:

- Military systems introduce new vulnerabilities and **high** consequences.
- Robust non-cyber training mitigates some vulnerabilities.
- Rank may override technical expertise.
- Cybersecurity is an individual responsibility—though abstractly understood.

“You could cripple a vessel or you could cause World War III if you wanted to.” *–B4*

In Progress: GPS Spoofing Measurement



Georgia Tech

Recent publications leveraging the testbeds

- **CCS'25:** 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
- **CCS'25:** One Video to Steal Them All: 3D-Printing IP Theft through Optical Side-Channels, Twisha Chattopadhyay, Fabricio Ceschin, Marco Garza, Dymytriy Zyunkin, Animesh Chhotaray, Aaron Stebner, Saman Zonouz, Raheem Beyah
- **CCS'25:** The Challenges and Opportunities with Cybersecurity Regulations: A Case Study of the US Electric Power Sector, Sena Sahin, Burak Sahin, Robin Berthier, Kate Davis, Saman Zonouz, Frank Li
- **CCS'24:** Release the Hounds! Automated Inference and Empirical Security Evaluation of Field-Deployed PLCs using Active Network Data, Ryan Pickren, Animesh Chhotaray, Frank Li, Saman Zonouz, Raheem Beyah
- **CCS'24:** ERACAN: Defending Against a Game-Changing CAN Threat Model, Zhaozhou Tang, Khaled Serag, Berkay Celik, Saman Zonouz, Raheem Beyah, Dongyan Xu **(Distinguished Paper Award)**
- **NDSS'24:** Compromising Industrial Processes using Web-Based Programmable Logic Controller Malware, Ryan Pickren, Tohid Shekari, Saman Zonouz, Raheem Beyah

Georgia Tech

Currently ongoing funded projects…

- NSF CHORUS $7M — Automotive
- Hyundai $280K — Automotive
- GDoT $100K — Automotive
- Brusa HiPower (CH) — Automotive

- DOD BA-BOM $3M — Controller security
- GTRI/SEI IRAD $160K — Controller security
- GTRI IRAD $270K — Controller security
- DHS $500K (terminated) — Resilience

- DOE DerGuard $4.2M — Power grid
- DOE Phrensics $4.6M — Power grid
- DOE SCORE $250K — Power grid
- DOE INL/CIE $300K — Power grid
- DOE Sandia Labs $70K — Power grid

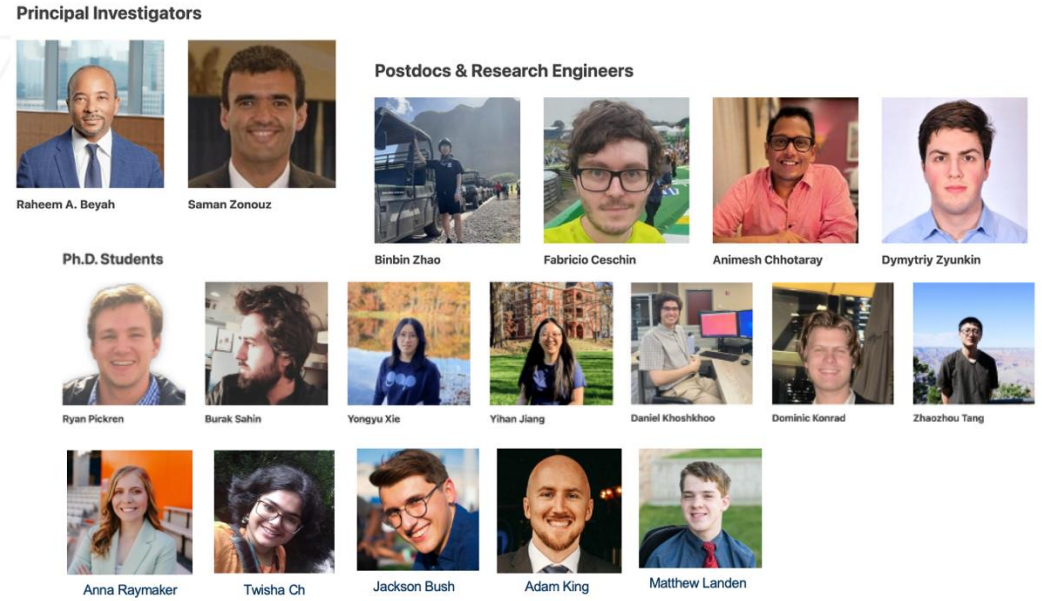
- AI-Manufacturing $65M — Manufacturing
- NSF SaTC $600K — CPS Deception
- Accenture $200K — AI-based CPS

Georgia Tech

CPSec Lab @ Georgia Tech

Cyber-Physical Systems Security Research Lab

CPSec: Cyber-Physical Systems Security Lab



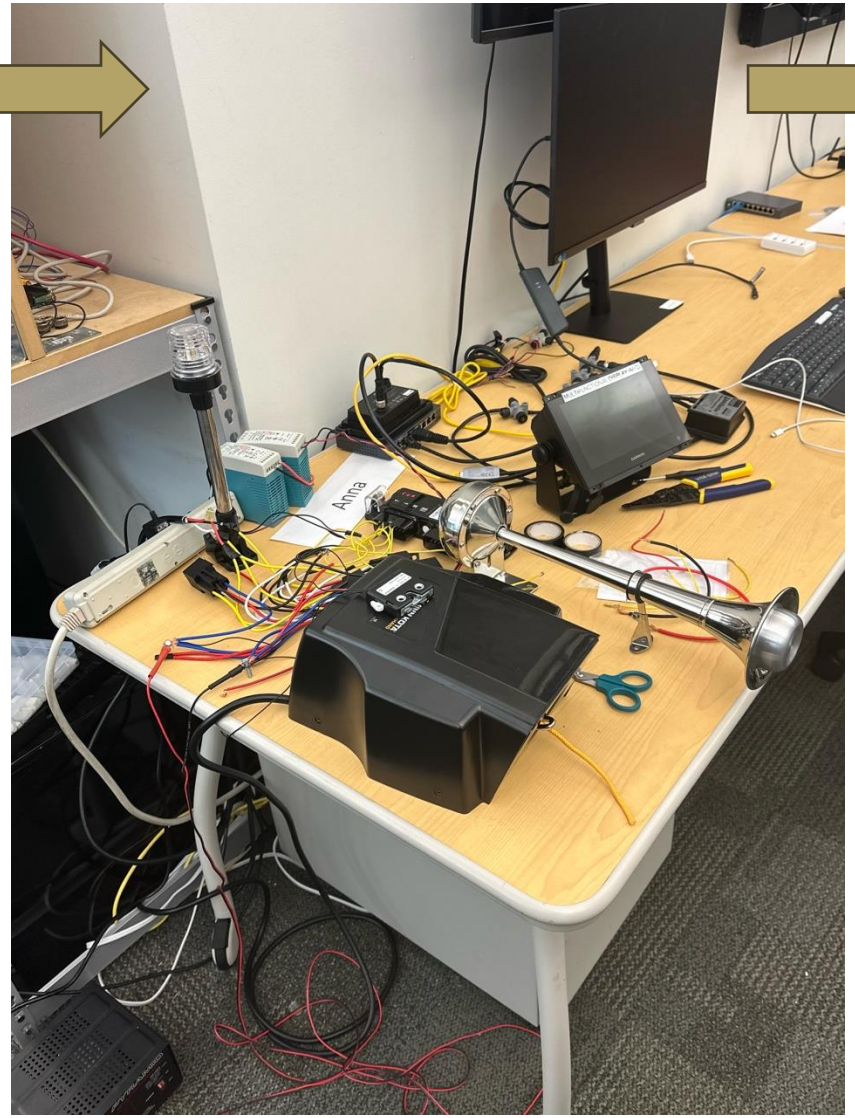
Georgia Tech

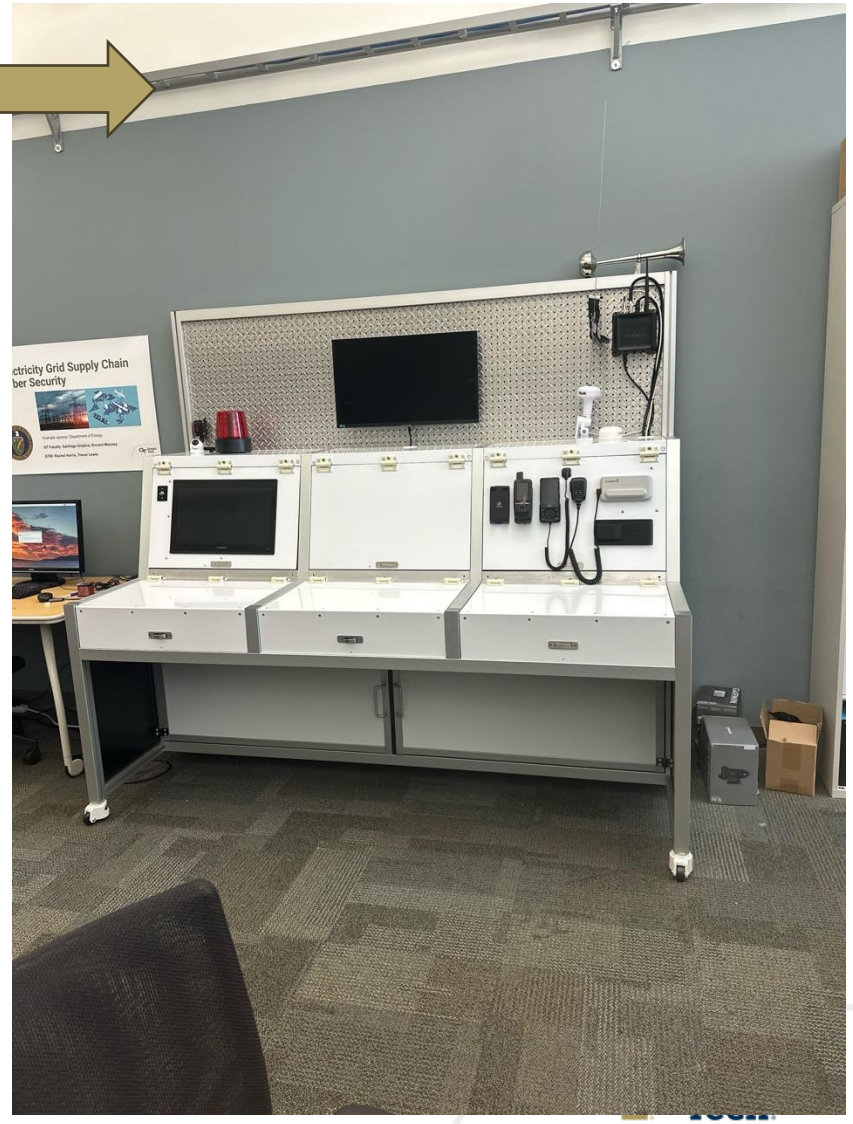
U.S. Congressional Visit

CPSec: Cyber-Physical Systems Security Lab

Georgia Tech

Maritime Cybersecurity Testbed Progress





Maritime Cybersecurity Testbed Demo!

Georgia Tech