SECURITY WITH PLYMOUTH UNIVERSITY

Cyber-Risk Assessment for Autonomous Ships

Prof. Kevin D Jones & Dr. Kimberly Tam

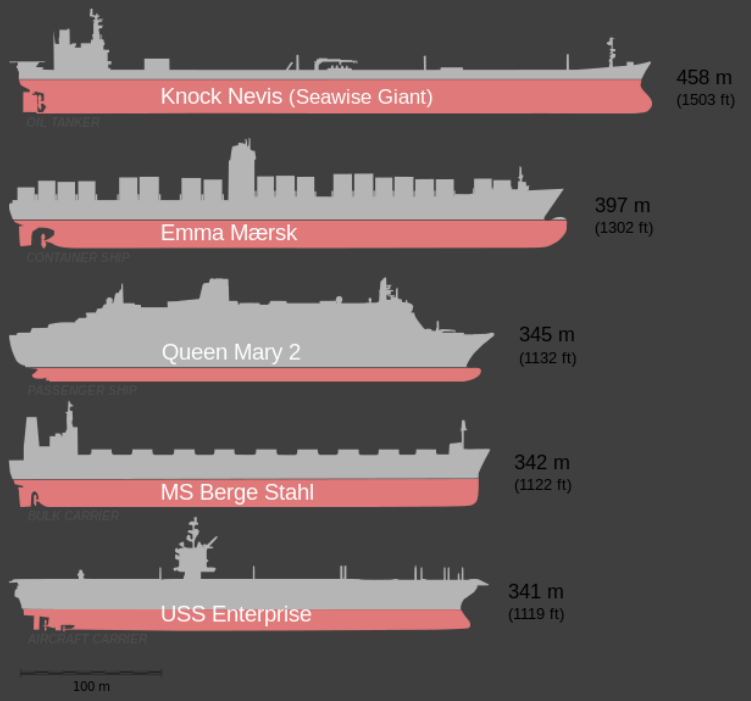
Glasgow, Cyber Security, June 12th 2018

Maritime Threats: Then & Now

Traditional Maritime Threats + Modern Maritime Threats

Different Risk Profiles

- Ships have different functionalities
- Ships are equipped with different systems
- Ships travel through different locations
- Attackers have different interests
- Attackers have different resources levels



https://commons.wikimedia.org/wiki/File:Bateaux_comparaison2.svg

Each ship has a dynamic risk profile that changes depending on circumstances

Autonomous Ships (by 2020)

YARA Birkeland

- Zero emission
- Short ranged
- Fully autonomous
- Close to shore
- Cargo

Mayflower500 (MAS)

- Science vessel
- Fully autonomous
- Trans-Atlantic
- Deploy drones
- Collect samples

AAWA Rolls Royce

- Multi-purpose
- Reduced crew
- Ocean travelling

To compensate for no human crew, more sensors needed
For remote access and remote downloads, all must be satellite connected

Model Based Risk Assessment

- A way to characterize and quantify risks
- Model ship (target) and attacker

System Vulnerability

- AIS
- ECDIS
- IBS Internet
- GNSS
- GMDSS
- …

Ease of Exploit

- Attacker members
- Attacker resources
- Target defences
- Target location
- …

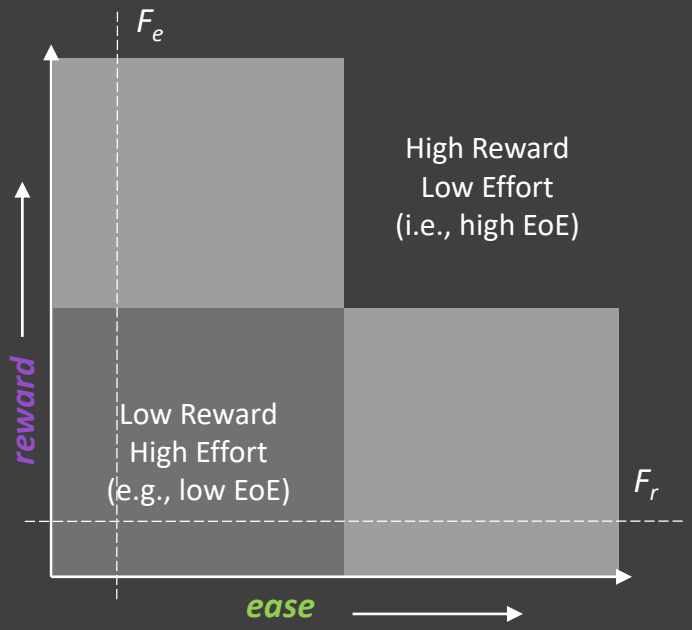
Attacker Reward

- Profit
- Collision/Damage
- Denial of Service
- Misdirection
- Obfuscation
- …

The Macra Framework

MaCRA: Maritime Cyber-Risk Assessment Models the three axis:

1. Maritime system **vulnerabilities** and effects
2. "**Ease of Exploit**" based on target defences and attacker resources
3. Exploit **reward**, based on attacker profiles and target



Sample Target Ship Systems

Cyber Vulnerabilities	System	Physical/Cyber Effect(s)
USB/CD/DVD, SCADA, **satellite**	Deck Machinery	damage, theft
VHF, **satellite**, radar, IBS	AIS	DoS, damage, misdirect, theft, obfuscation
satellite	GNSS	damage, misdirect
Radar	Radar	DoS, obfuscation
USB/CD/DVD, **satellite**, Internet	IBS/Main PC	DoS, damage, misdirect, theft, obfuscation
USB/CD/DVD, **Internet**, NBDP, IBS	NAVTEX	DoS, damage
radio, **satellite**, ECDIS, NAVTEX, IBS	Sailing Directions	DoS, damage, misdirect
USB/CD/DVD, IBS (**satellite**)	VDR	DoS, obfuscation
radio, NAVTEX, **satellite**, radar	GMDSS	DoS, damage
satellite, USB/CD/DVD, IBS	Internet	DoS, damage, misdirect, theft, obfuscation
Networks, **satellite**, USB	Sensors	DoS, damage, misdirect, theft, obfuscation

- Without (or with less) crew, autonomous ships will rely more heavily on sensors for information
- Systems will be more connected to satellite or internet providing systems (IBS) to send data and potentially receive commands

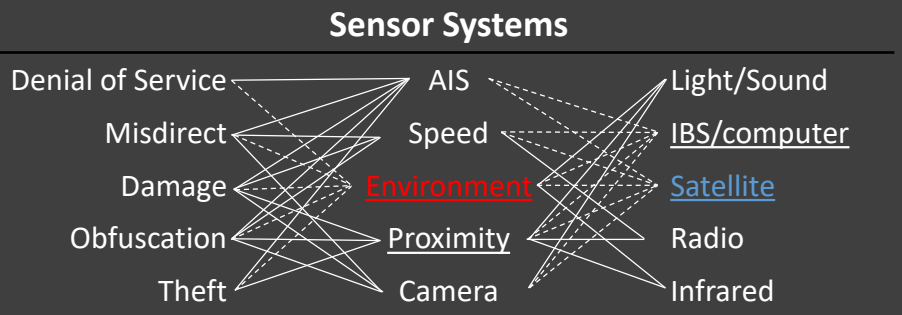
Main Attacker Profiles

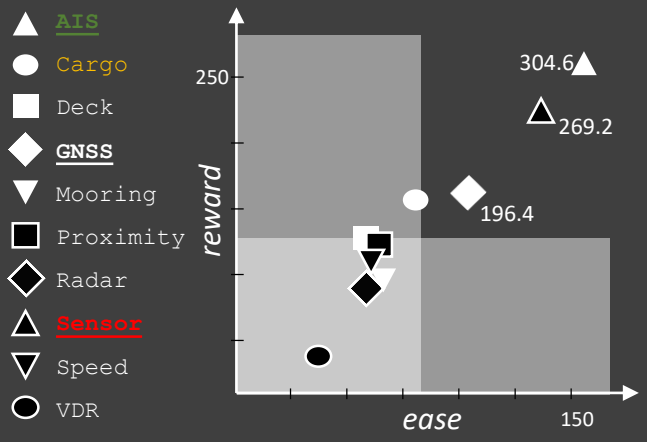
Attacker	Profile
Activists	The desired outcome is often to achieve ideological goals • Attacks designed to disrupt activities • Attacks designed gain, and publicize, data to alter target behaviour
Competitors	Mainly seek to increase their own market influence in the global economy • Acquire information (e.g., opponent's current bids and customers) • Disrupt operations to damage financial status or reputation
Criminals	Profit-driven individual to groups of different sizes and sophistication • Physical/intellectual theft, fraud, smuggling, blackmail, and extortion • Indirectly selling cyber-attack tools or stolen data etc.
Terrorists	Actively seek destructive and disruptive outcomes • Cause death, damage, and fear • Increase their member count (e.g., propaganda) and resources

- Security and monitoring must be even stronger against attackers
- May attract more cyber-compentent attackers

Autonomous Ships: Sensors

An analysis of the three autonomous ships showed us the likely risk profile for autonomous ships.





From the risk views, ways to lower risks are:

- Secure satellite (because highly connected)
- Secure environment sensors (can cause many effects)
- Secure AIS (sitting in high risk quadrant)

Events that may push low-risks into high-risk zones

- Vulnerability in cargo loading …

Summary

- Maritime cyber-security a rapidly changing area
  - Autonomous ships in the near future (beginning 2020)
- Moving from awareness to analysis, detection, and risk assessments
  - Still generally at the “cyber hygiene” stage
  - Use risk profiles to raise awareness and identify vulnerable systems and possible outcomes
- Active area of research
  - Technical
  - Socio-technical
  - Physical/Cyber-Physical
  - Law and Policy
- The problem will continue to grow
  - Autonomous ships/ports
  - Internet of things

Overview

As a Tier1 National UK threat, cyber-attacks can cost companies millions in a maritime cyber-attack. As the world heavily depends on maritime operations, we at the University of Plymouth have been researching maritime cyber-threats as few organisations have the capability, connections, and facilities to do so. This group is uniquely placed to make significant contributions in maritime cyber-security and brings together leading-edge multidisciplinary research and practical expertise from across UoP and beyond.

Current projects

- Compiling a **body of knowledge** for maritime cyber-threats.
- **Vulnerability and risk analysis** for existing ship-based systems.
- **Threat assessment** for ship operations and

Recent publications and presentations

- Tam K, Jones K. Cyber-Risk Assessment for Autonomous Ships, Cyber Security, 2018
- Tam K, Jones K. MaCRA: A Model-Based

Thank You

Professor Kevin D Jones
kevin.jones@plymouth.ac.uk

Dr. Kimberly Tam
kimberly.tam@plymouth.ac.uk

Website:
https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group

Assessment Tiers

	SAE-Based Ship Autonomy	Attacker Reward	Ease-of-Exploit
Tier 1	Minimal crew required and for most, if not all, ship operations.	Little to no value for the attacker. Minimal impact.	Nation State: Advanced Persistent threats, requires nation-level resources.
Tier 2	Partial automation with local crew for simple tasks, e.g. advanced auto pilot.	Small value to attacker.	Corporate: Advanced level attacks requiring considerable resources.
Tier 3	Conditional autonomy, potential interventions by crew.	Average to moderate value for the attacker.	Professional: Moderate level of attack with significant resource investments.
Tier 4	High autonomy, mostly self-running. Local/off-shore crew rarely required.	Valuable to attacker and third parties.	Basic Attack: Minimal skills or resources used.
Tier 5	Complete autonomous ship operations in all potential settings.	Extremely valuable to most players, large-scale or significant impacts.	Little to no skill needed, often uses pre-made exploits (i.e., script kiddies).