Maritime UK

Cyber-security of evolving maritime technology

Dr Kimberly Tam

Lecturer in Cyber-Security

Cyber-SHIP Lab Academic Lead

7th Maritime Autonomous Systems Regulatory Working Group Conference

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Evolving Technology

- Semi-autonomous
- Full autonomy
- Clean maritime growth
- Efficiency
- Monitoring
- Safety/Security

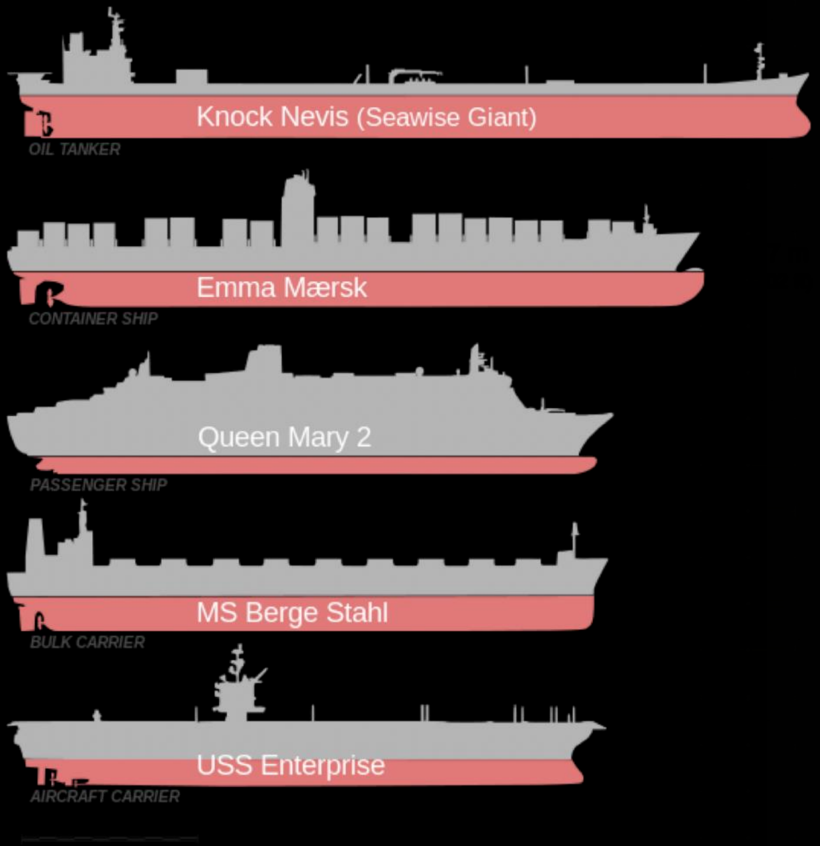
UNIVERSITY OF PLYMOUTH
MARINE BUSINESS TECHNOLOGY CENTRE
SMART SOUND
European Union
European Regional Development Fund

MARINE BUSINESS TECHNOLOGY CENTRE PLYMOUTH
Where enterprise meets the ocean

European Union
European Regional Development Fund

HM Government

Technology, cyber-risk, and people



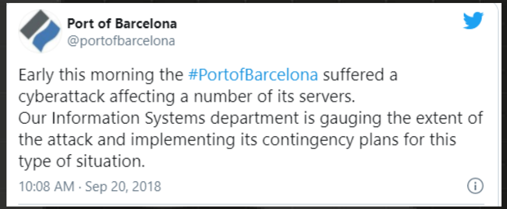
- Ships have different functionalities
- Ships are equipped with different systems
- Ships travel through different locations
- Attackers have different interests
- Attackers have different resources levels

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

Maritime cyber attacks

UNIVERSITY OF PLYMOUTH

- **Growing exponentially**, with ports and ships experiencing costly attacks now on a monthly basis
- Port of Barcelona in 2017, Maersk Not Petya in 2018, and CMA Ransomware in 2020 being recent high-profile examples
- Latest attack on CMA CGM means that all the Big-Four shipping lines, including MSC and COSCO, have suffered recent disruptive cyber events
- **90% of world-trade is moved by ship** and recent events have highlighted a potential fragility in (just-in-time) supply chains
- Ships' complex and myriad system-of-systems that could present **many thousands of attack surfaces**



Port of Barcelona
@portofbarcelona

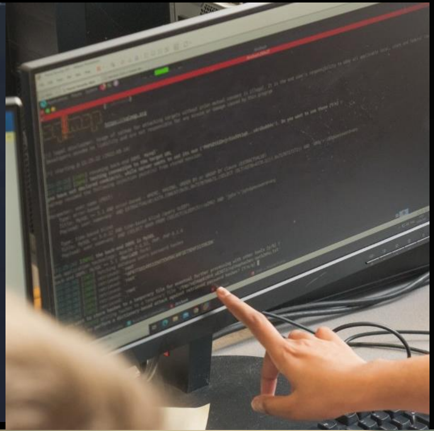
Early this morning the #PortofBarcelona suffered a cyberattack affecting a number of its servers.
Our Information Systems department is gauging the extent of the attack and implementing its contingency plans for this type of situation.

10:08 AM · Sep 20, 2018

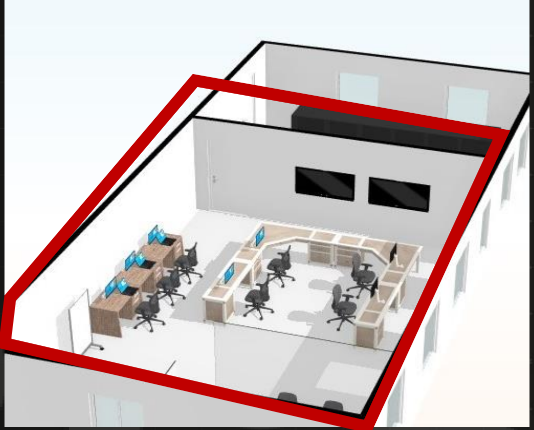
Cyber-SHIP Lab

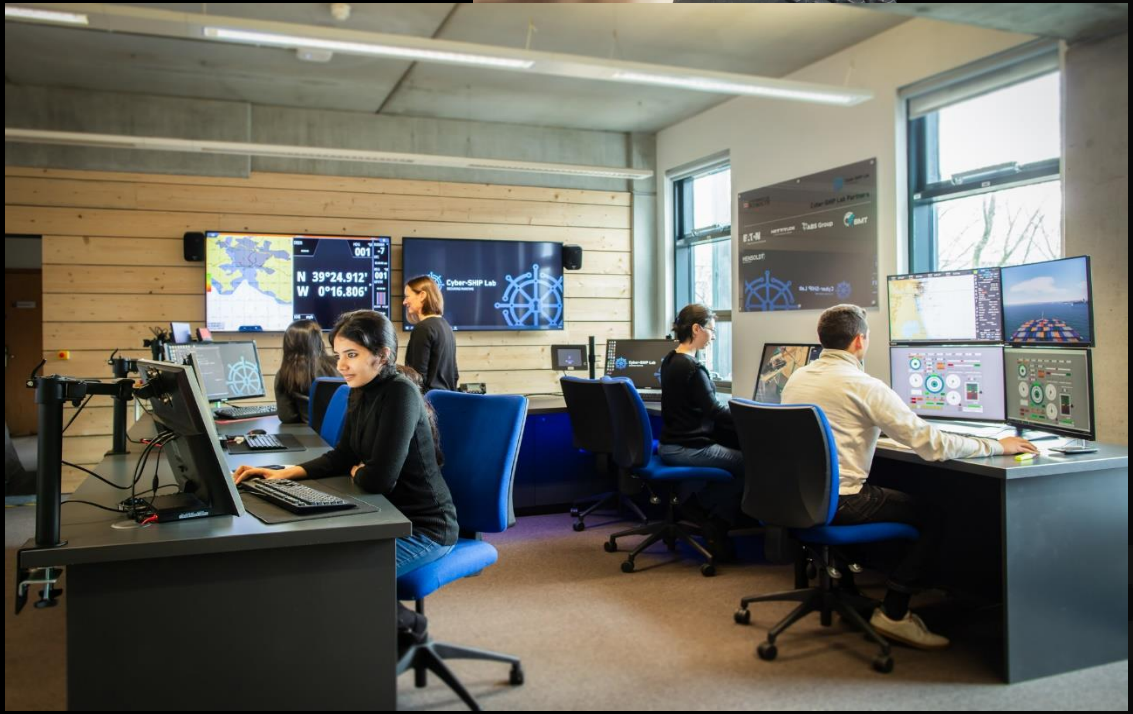
The Console Room

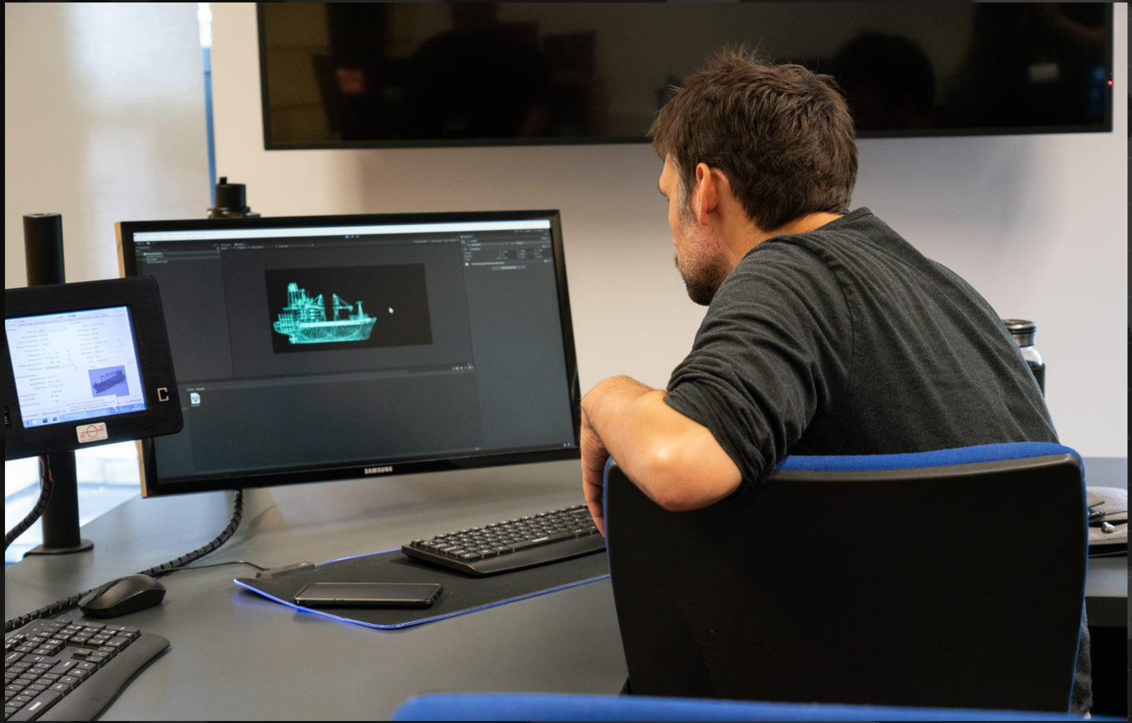
```
File  Actions  Edit  View  Help
2021-10-06 11:05:[illegible]
[illegible]
broken from time loop about to attack
start
setting ip forwarding
net.ipv4.ip_forward = 1
compiling

etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team

 14 protocol tables loaded:
        DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr [illegible]

 13 constants loaded:
        VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

 Parsing source file '/home/kali/attacks/injectionfilter.ecf'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to '/home/kali/attacks/injectionfilter.ef'  done.

 -> Script encoded into [illegible] instructions.

starting attack

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Content filters loaded from /home/kali/attacks/injectionfilter.ef...
Listening on:
  eth0 -> [illegible]
          [illegible]
          [illegible]

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %
```



- Visualisation of data
- Physical hardware visualisation of attacks
- Pen-testing
- Research Project development
- Development of custom electronics and software
- Teaching/training





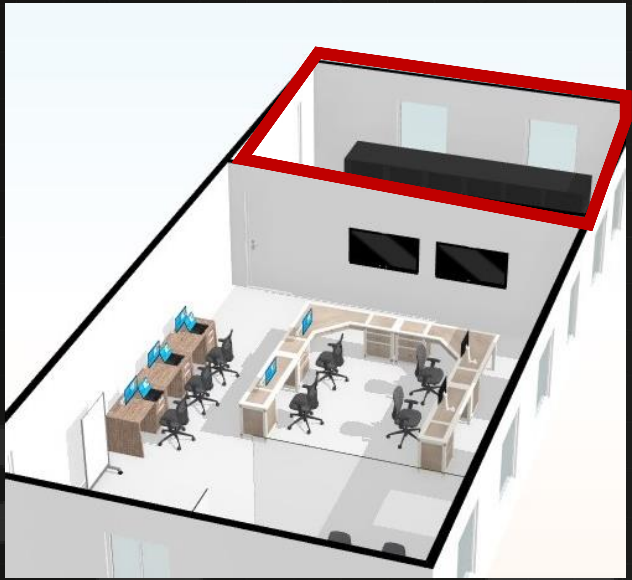


The Vault

Drones and USVs

Radar equipment

Custom Power Distribution



VDRs and NAVTEX

AIS receivers

Custom Cyber-SHIP 24V Logic Interface and monitor

MFDs

Cyber-SHIP Lab

UNIVERSITY OF PLYMOUTH

Current status – Oct 2022

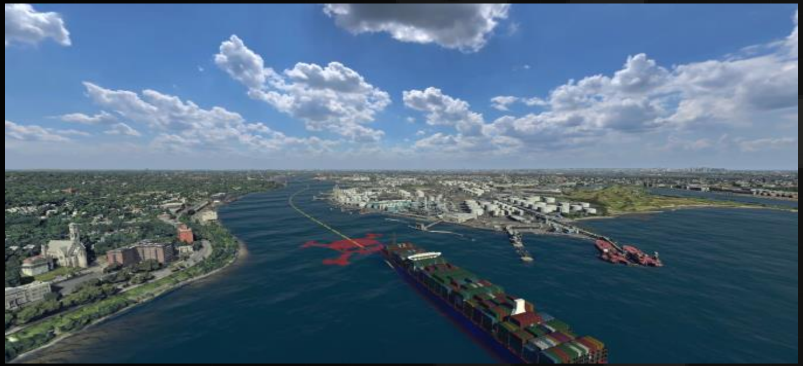
UNIVERSITY OF PLYMOUTH

Physical twin

- **Fully functioning lab** with a growing number of bridge and control system configurations
- In-house custom built scale **physical test rigs** for steering and propulsion systems
- *Still a **work in progress**, but progressing steadily…*

Visualisation

- Visualisation expert
- Developing mariner-checked **realistic scenarios**
- Visually pleasing and comprehendible **animations of attack flow** and consequences



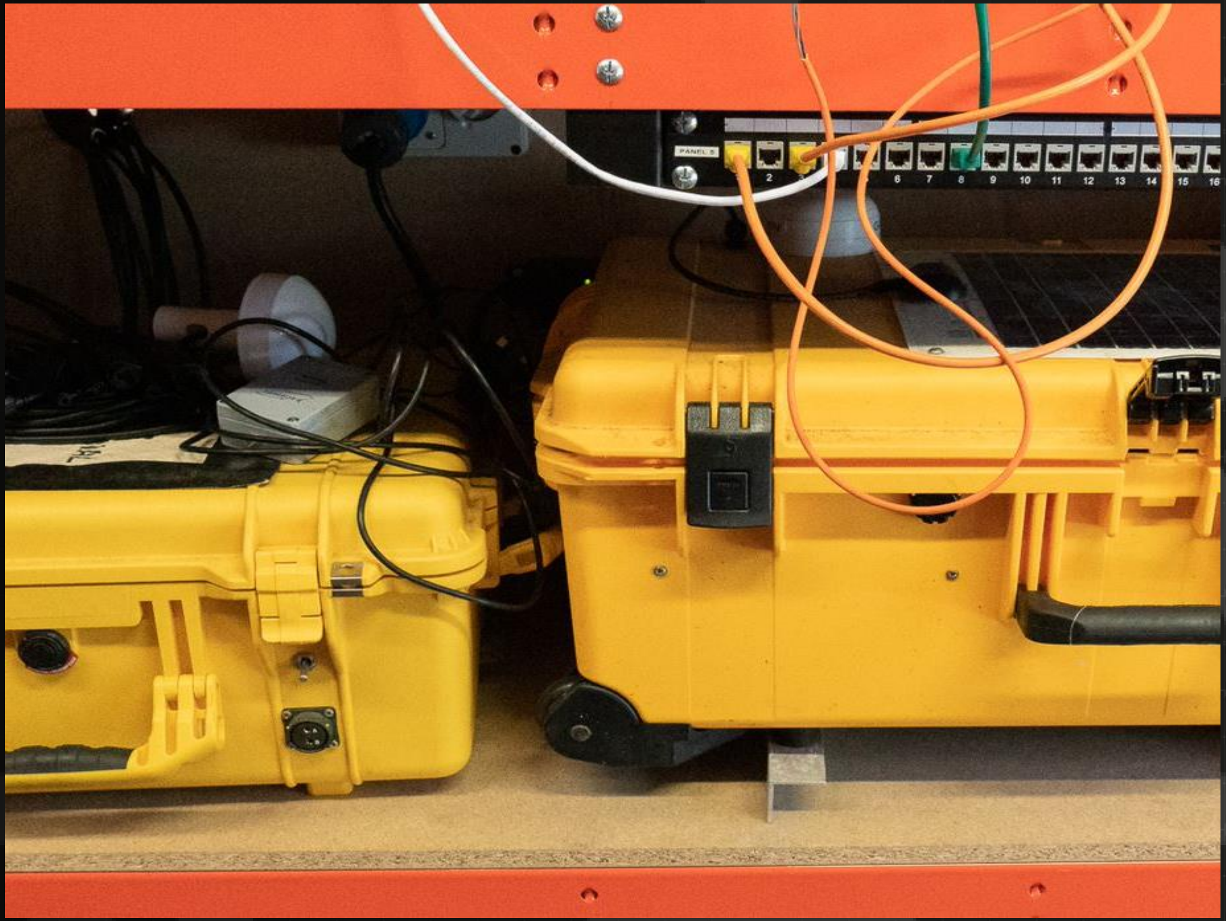
Testing

- Standard approach to device testing
- Testing at **system level and entire configuration level**
- Commercial consultancy to provide standard **vulnerability reports**
- Variety of **attacks and vectors**: MiTM, Ransomware, CommsChannel ,Supply Chain, NMEA 2000 injection, Custom malware

Cyber-SHIP Lab

Dry USV

- Physical twin of a USV
- Torquedo thrusters, battery bank, Sat Comms System, Industrial PC, Power generators, other peripherals e.g., switches GPS units, radio modems, solar panels, cameras and AIS equipment
- Building a command-and-control unit



Other Activities/Projects

- Maritime Autonomous Systems (MAS) AI & maritime cybersecurity (AIMSec) workshop on September 13th 2022. Workshop funded by the Turing Network Development Project and hosted by the University of Plymouth (UoP) and members of the Maritime Cyber-Threats Research Group
- EC H2020 Cyber-MAR: Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.
- MaCRA uniquely provides dynamic, multi-dimensional risk assessment tooling, uniquely addressing both IT and OT elements of a specific vessels systems, including threat factors associated with specific cargo and route.

Cyber-SHIP Lab MaCRA Cyber MAR UNIVERSITY OF PLYMOUTH

UNIVERSITY OF PLYMOUTH

Cyber-SHIP Lab
SECURING MARITIME

Cyber MAR

MaCRA

Dr Kimberly Tam
Lecturer in Cybersecurity
Academic lead of the Cyber-SHIP Lab

Kimberly.tam@plymouth.ac.uk
https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group

Thank you