CYBER-PHYSICAL SYSTEMS SECURITY: THREAT AND RISK INTELLIGENCE FOR THE MARITIME SECTOR

PROF. SIRAJ AHMED SHAIKH

Systems Security Group
Future Transport and Cities (FTC) RI
Coventry University, United Kingdom
Email: s.shaikh@coventry.ac.uk

Co-Founder and Chief Scientist
CyberOwl
London, United Kingdom
Email: siraj.shaikh@cyberowl.io

5th ShipIT Conference @ Athens, Greece, 26th September 2019

Research Institute
Future Transport and Cities

Coventry University

Coventry University

Systems Security Group Mission

Research and technological excellence across disciplinary themes that converge on the engineering of secure cyber-physical systems, such as maritime vessels and ports.

- Scientific and technological underpinning for CyberOwl technology, providing protective monitoring system for vessels;

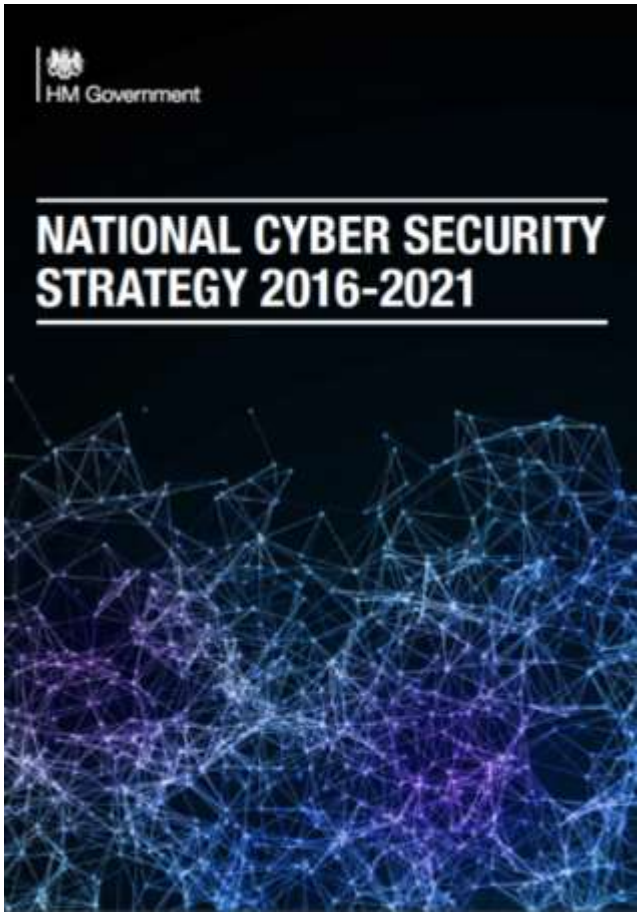
- Authored the maritime cyber threat evidence review “Future of the Sea: Cyber Security” for the Government Office of Science (UK);

- Part of the ‘Cyber Readiness for Boards’ initiative to work with maritime boards on cyber risk governance, funded by the UK’s National Cyber Security Centre and Lloyds Register Foundation.

Research Institute
Future Transport and Cities

Coventry University

Systems Security is a National Priority



"Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference."

- National Cyber Security Strategy (November 2016)
- It acknowledges UK's critical national infrastructure and industrial control systems are threatened;
- A commitment to develop an innovative, growing cyber security industry, underpinned by world-leading scientific research and development.

Systems Security is a Global Priority

Global Economic Risk: "Failure to adequately invest in, upgrade and/or secure infrastructure networks (e.g. energy, transportation and communications), leading to pressure or a breakdown with system-wide implications."

- World Economic Forum's Global Risks (January 2019)
- Resilient transport infrastructure is identified as a key underpinning to addressing risks arising from environment disasters, rural-urban divide, and food security issues.

“The necessity of procuring good intelligence is apparent and need not be further urged.”

General George Washington
Letter to Colonel Elias Dayton
26th July 1777

Some challenges for maritime cybersecurity..

- **How do we bridge across IT and OT systems?**

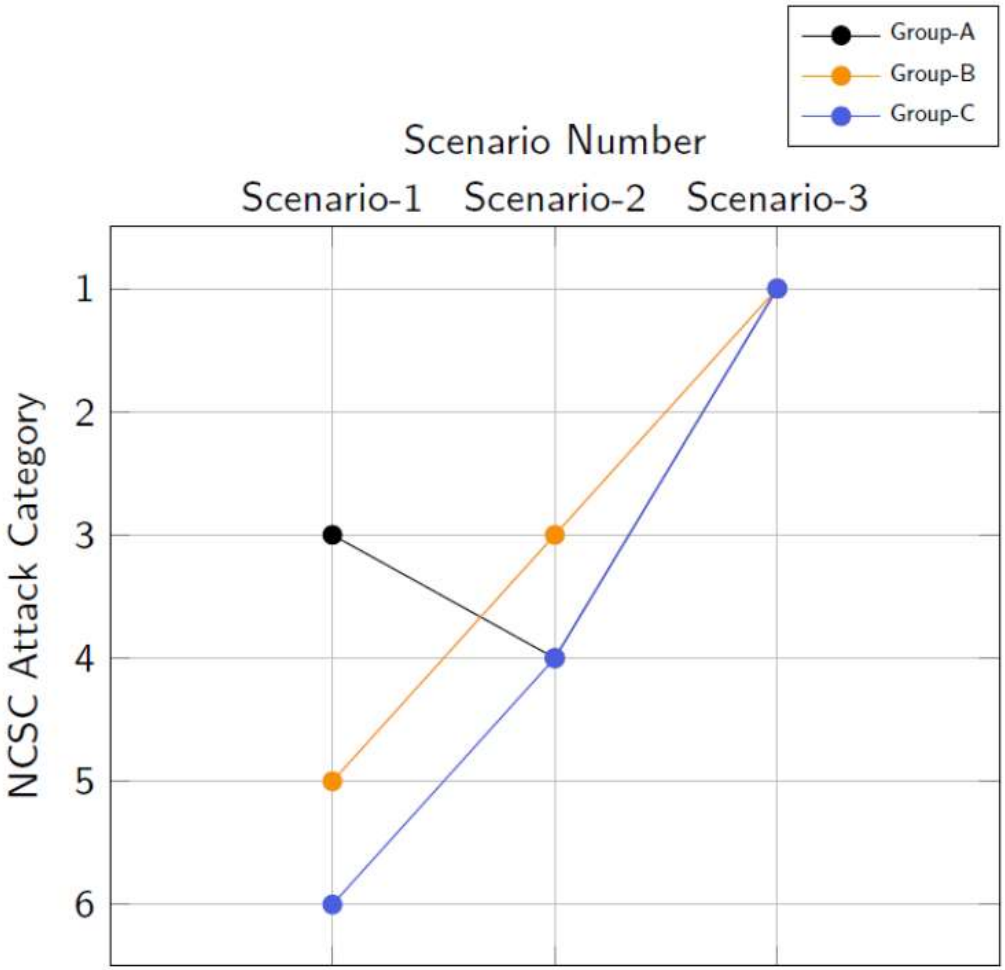
  Example: For planned maintenance systems (PMS) – increasingly integrated with sensors and telemetry across the vessel or an intelligent remote asset management system (iRAMS) – which are often run on on-board workstations, how do we ensure we detect for malicious attempts across our IT/OT systems?

- **How do we detect cyber incidents?**

  How effective is our current situational awareness and actionable intelligence capability? Typical malware dwells in the target system for well over five months (FireEye). Supply chain infiltration means that vulnerabilities remain hidden and threats remain stealthy.

Lessons from other sectors (automotive industry)

- We have run a policy game with cyber analysts to understand threat assessment and risk perception
- Three escalating scenarios, from keyless theft, to remote telematics hacking, to autonomous vehicle ramming attacks
- NCSC attack categorisation goes from local incidents (6) to tier-1 threats to the nation (1)



Monitoring challenges for cyber-physical systems

- As opposed to layered enterprise systems, such systems…
  - are assembled in a component-driven bespoke fashion, where attack signatures are not obvious;
  - where design is asset and process centric, with critical functionality earmarked.

- Learning on behaviours on data/io and traffic/interface is not straightforward because…
  - diverse data domains, where malicious behaviours are predicated across multiple domains of learning;
  - baselining across multiple domains for threat anomalies is a challenge for current generation of ML/AI.

Where do we go from here?

- A different monitoring approach is needed where…
  - Asset-sensitive health indicators, both at local and system level, need to be identified
    - Indicators, atomic in nature, falling under early phases of kill chain, are the core;
  - Risk-sensitive approach to monitoring to detect for threshold violations.
  - Aim is not to signature-detect or rule-match but to detect
    - Potential physical safety violations (physical assessments are key therefore);
    - Potential cyber safety violations (in terms of data-flow or control-flow violations).
- Domain-agnostic early-stage threat estimation for risk profiling
  - Low-tier sensor alert processing (reducing cognitive load) to direct human-in-the-loop decision making;
  - Automation of risk-sensitive low-level orchestration (in case of an ‘active’ early warning system).

We need a shift to..

Shift 1

- From attribution to early warnings: towards protective monitoring of assets

Shift 2

- From signatures to indicators and symptoms: looking for ‘unknown unknowns’
  - Needs to be achieved through horizontal integration across purpose-built sensors needs to aggregate on multi-domain visibility.

Shift 3

- From isolated predictions to system judgements: alerts and indicators to aggregated threat estimation
  - Human-in-the-Loop decision cycles, underpinned with risk-sensitive active defence.

Thank you