ENGINEERING
TEXAS A&M UNIVERSITY

Legal and Policy Issues with Maritime Cybersecurity

Paula S. deWitte, J.D., Ph.D., P.E.
Paula.dewitte@tamu.edu

Associate Professor of Practice
Computer Science & Engineering

Agenda

ENGINEERING
TEXAS A&M UNIVERSITY

- Maritime assets as targets for cybersecurity attacks on critical infrastructure
- Differentiators between maritime systems and other systems
  - OT (operational technology) and IT (information technology)
- Status of cybersecurity legal and ethical framework
- Going forward—what to expect?

What is Critical Infrastructure?

ENGINEERING
TEXAS A&M UNIVERSITY

- Defined by the Patriot Act as:
  - "*…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*."
    [42 USC § 5195c(e)]

What are the Critical Infrastructure Sectors?

ENGINEERING
TEXAS A&M UNIVERSITY

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
- Water & Wastewater Systems

Unique Maritime Environment

ENGINEERING
TEXAS A&M UNIVERSITY

- Underlies myriad industries
- Criticality
- Integration of maritime- and land-based logistics chain
  - Integration of OT and IT in the supplier chain
- Both IT and OT target-rich environments:
  - Cruise ship: How many passengers/credit card numbers/nationalities?
  - OT/ICS/Highly automated systems
- Subject to multiple jurisdictions

Critical Infrastructure Attacks

ENGINEERING
TEXAS A&M UNIVERSITY

- Who?
  - Nation-state
  - Hacktivists
  - Criminals
- How?
  - Advanced Persistent Threats (APTs)
  - Synchronized attacks

IT Cybersecurity Issues

ENGINEERING
TEXAS A&M UNIVERSITY

- Ransomware
  - June 2017: Maersk by the WannaCry NotPetya variant sabotage/ransomware incident, which the company believes cost it as much as $300 million.
- Phishing attack
  - November 2016: Europe's largest manufacturer or wires and electrical cables, Leoni AG, lost £34 million in a whale attack, when cyber criminals tricked finance staff into transferring money to the wrong bank account.
  - https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats
- General Data Protection Regulation (GDPR)
  - Extra- extraterritorial jurisdiction
  - Privacy Impact Assessments (PIA)

OT Cybersecurity Issues

ENGINEERING
TEXAS A&M UNIVERSITY

- Autonomous ships
- GPS Spoofing
- Compromise operational controls
- …

Why is this so Difficult?

ENGINEERING
TEXAS A&M UNIVERSITY

- Law always lags technology
  - Precedence
- Most laws relate to physical (and not electronic) assets
- Cybersecurity is risk based
- Legal concepts:
  - Jurisdiction and extraterritorial jurisdiction
  - Standing
  - Statute of Limitations
  - “Foreseeability”
  - Proving causality
  - Proving damages
  - Common law vs statutes
  - … <etc>
- Federal vs states’ laws vs international law
- Uncertainly of cyber insurance

GDPR

ENGINEERING
TEXAS A&M UNIVERSITY

- EU response to privacy issues.
- Several key changes:
  - Explicit consent
  - Right to be forgotten
  - Privacy by design
  - 72-Hour breach notification
  - Differentiate “controller” and “processor”
  - Requirement for a qualified Data Protection Officer (DPO)
  - …

Applicable Laws, EOs, and PPDs…

ENGINEERING
TEXAS A&M UNIVERSITY

- Federal Laws
  - FISMA (Federal Information Security Management Act) under the 2002 Homeland Security Act; Enhanced in 2014
  - CISA (Computer Information Sharing Act) or the Cybersecurity Act; 2015
  - CFAA (Computer Fraud and Abuse Act) under Comprehensive Crime Control Act 1984
  - GLB (Gramm-Leach-Bliley); HIPAA (Health Information Portability and Protection Act)
- Who governs?
  - OMB, NIST, …
  - Regulatory/guidance agencies vs investigative agencies
- Who regulates?
  - SEC, FTC, …

Applicable Laws, EOs, and PPDs…

ENGINEERING
TEXAS A&M UNIVERSITY

- Presidential Executive Orders
  - President Obama:
    - Executive Order 13636: Improving Critical Infrastructure Cybersecurity (February 12, 2013)
    - Paired with PPD-21: Critical Infrastructure Security and Resilience
    - Executive Order 13691 Creation of Information Sharing Analysis Organizations (ISAOs) (February 13, 2015)
      - Started with UT-SA for non-governmental entities
    - Information Sharing Analysis Centers (ISACs) created EO 12472/PPD-63 (May 22, 1998)
      - Risk mitigation, incident response, alert and information sharing
    - Executive Order 13694 (April 1, 2015) "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"
  - President Trump:
    - 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Executive Order 13636/Presidential Directive 21 (February 12, 2013)

ENGINEERING
TEXAS A&M UNIVERSITY

- Develop a **technology-neutral voluntary cybersecurity framework**
  - NIST Cybersecurity Framework V1 released (February 12, 2014) and revised (April 14, 2018)
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- **Explore the use of existing regulation** to promote cyber security

→ Lacking other standards, U.S. Courts are looking at the NIST Standards as "reasonable" practices and the de facto legal standard

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

ENGINEERING
TEXAS A&M UNIVERSITY

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan (NIPP)
- Develop comprehensive research and development plan

The NIST Cybersecurity Framework

ENGINEERING
TEXAS A&M UNIVERSITY

- Included industry experts who have battled cyber attacks
- Conducted working groups in conjunction with other standards organizations
- Appeals to the best interests of companies & their shareholders
- Considers total supplier chain -- enterprises, suppliers, partners, & customers

How Implemented: NIST Cybersecurity Framework

ENGINEERING
TEXAS A&M UNIVERSITY

- United States Coast Guard Draft Navigation and Vessel Inspection Circular No 5-17
  - Define cyber risk management policy
  - Protection of computer systems
  - Detection
  - Response
  - Recovery
- Maps to other laws (e.g., MTSA – Maritime Transportation Security Act)
- *"It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements."*
  - http://www.iadc.org/wp-content/uploads/2017/10/DRAFT-Cyber-NVIC-05-17.pdf

What Laws May Apply?

ENGINEERING
TEXAS A&M UNIVERSITY

- International maritime law?
- GDPR with “extra-territorial jurisdiction” for protecting privacy?
- U.S. laws on critical infrastructure?
- And now we have …

Why the uncertainty?

ENGINEERING
TEXAS A&M UNIVERSITY

- Last year – introduction of CFAA ACDC (Active Cyber Defense Certainty) Act
  - Legalize “hacking back”
- National Cyber Strategy (Sept 20, 2018) released by the White House
- “Defense forward”
  - Outside of US networks
  - Target critical infrastructure
  - *"We will respond offensively as well as defensively."*
- Actually two strategies released:
  - DoD National Cyber Strategy
    - DoD readiness to support offensive operations
    - Push on the defense supplier chain
      - Cost + Schedule + Performance →
        Security + Cost + Schedule + Performance
    - PPD-20

What's Ahead?

ENGINEERING
TEXAS A&M UNIVERSITY

- More regulation.
- Uncertainty in the U.S. federal courts:
  - U.S. federal circuit courts split on important cybersecurity legal issues:
    - What constitutes "standing?" 3rd vs 7th
    - 11th Circuit invalidated an FTC order two years after issued
- GDPR court cases
- ???

ENGINEERING

TEXAS A&M UNIVERSITY