WHY MARITIME CYBER-SECURITY IS AN OCEAN SCIENCE POLICY PRIORITY, AND HOW IT CAN BE ADDRESSED

Dr. Phil McGillivary, US Coast Guard Pacific Area & Icebreaker Science Liaison
email: philip.a.mcgillivary@uscg.mil

USCG Icebreaker POLAR STAR, Ross Sea, Antarctica, Jan. 29, 2018
(Mt. Erebus in background)

Outline of talk on Maritime Cyber-security

- Background & Scope of the Problem
- Approaches to Cyber-security from Industry, Federal & International Agencies
- Cyber-Attack Reporting Requirements & Response Resources
- The Question of Methods (of Ensuring Cyber-security)
- Autonomous Vessels, Unmanned Shipping & Cyber-security issues
- The Role of Education & Outreach in Maritime Cyber-security
- Quantum Components of Future Cyber-security
- Summary & Conclusions: Role of the MTS Cyber-security & Infrastructure Committee

Background & Scope

- Port of LA = largest US port, $140B in 2014.; @$0.4B/day.
  This is old data; shutdown costs for most ports, e.g. LA, SF are now on the order of @$1B/day.
- @300+ unclassified hacks to date: including false fuel levels; ECDIS/GPS/AIS position info spoofing; faked shipping manifests; bridge or engine take-overs
- Maersk hack, June 2017 = 13 global ports shut down, including in US.
  Cost Maersk $300M. This was a phoney ransom hack.
- Clarkson hack, 2017 = faked shipping manifestos, allowed for theft of containers, potentially introduction of illegal goods in containers;
  put Clarkson client data at risk as well, another potential cost to Clarkson.
- Naval Dome cyber penetration test: @200,000 ships didn't pass minimal requirements to withstand cyber-attacks.

Approaches to Addressing Maritime Cyber-security: Industry & International

- DNV-GL issued cyber-security recommendations in 2016: http://www.dnvgl.com.
- IMO issued Guidelines on Maritime Cyber-security Risk Management in 2017, which must be implemented by 2021:

  http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf.
- IMO starts 5 international Maritime Technology Cooperation Centers [of Excellence] (MTCCs) in 2017, which should help disseminate cyber-security best practices.
- Shipping/port conferences begin addressing the issue, e.g.:
  - GST Shipping 2030– https://maritime.knect365.com/gst-shipping2030/
  - Maritime Risk Symp–http://www.tiffin.edu/criminaljustice/maritime-risk-symposium-2017
  - Port Security Tech. – https://www.smi-online.co.uk/defence/uk/port-security-technology
- UK sets up National Cyber Security Centre & EU sets up cyber security “Code of Practices”

Approaches to Addressing Maritime Cyber-security: within US

- Navy: Navy Cyber Command established in 2017
- Nat. Res. Council/Nat. Acad. Scis.: series of reports on cyber-security (2007-2017)
- POTUS: Exec. Order 'Cyber-security for Federal Networks & Critical Infrastructure', May 2017
- NSF: Cyber-security Center of Excellence; and Center for Trusted Scientific Infrastructure
- DARPA, 2017:
  - High Assurance Military Systems (HACMS)
  - Configurational Security (ConSec) = automating systems configurations to minimize security risks
  - RFP for Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)
- DOT/Maritime Administration(MARAD): 2017 Guidance on Cyber-Security for Essential Transportation Systems (including for Commercial Vessels)
- Natl. Inst. Standards (NIST): National Initiative for Cyber-security

Cybersecurity approach from: The Guidelines on Cyber Security Onboard Ships, 2017. (https://www.bimco.org/products/publications/free/cyber-secuirty [sic]).

Approaches to Addressing Maritime Cyber-security: Coast Guard

- USCG Cyber Strategy released in 2015: http://www.overview.uscg.mil/Portals/6/Documents/pdf/cg_cyber_Strategy.pdf
- Coast Guard Proceedings 2015 special issue on maritime cyber:

  http://uscgproceedings.epubxp.com/i/436751-win-2015/47
- July 2017 CG releases a Navigation & Vessel Inspection Circular (NVIC) No. 05-2017, “Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Facilities” document requesting input from industry and the public on how to establish best practices and policies in mitigating cyber-security risks
- NVIC 05-2017 also requests comments on how the CG should accommodate changes in technology that will affect maritime cyber-security

Cyber-attack Reporting Requirements & Response Resources: Who ya gonna call?

- Coast Guard guidance: “Reporting Suspicious Activity & Breaches of Security” (info will remain non-public): National Response Center: PH 1-800-424-8802
- Report to Captain of Port
- Report to the 24/7 National Cyber-security & Communications Integration Center (NCCIC): PH 1-888-282-0870, which links to all federal Law Enforcement agencies
- CG Recommends contacting local Area Maritime Security Committees (AMSCs), contact info for which can be obtained from local Captain of Port
- EUROPOL also accepts cyber-security breach reports at:

  http://www.europol.Europa.eu/report-a-crime/report-cybercrime-online
- CERT request for help at: https://ics-sert.us-cert.gov
- Joint Industry/FBI “InfraGuard” activates triage response resources:
  - https://www.fbi.gov/resources/law-enforcement/iguardian
- National Suspicious Activity Reporting = Not for reporting, but to see reports from DHS, FBI & local LE: http://sni.ncirc.gov

The Question of Methods (of Ensuring Cyber-security)

- We use DTN (Delay & Disruption Tolerant) comms protocol, the free Internet Engineering Task Force secure comms protocol funded by NSA and intel agencies, c.f. http://www.dtnrg.org . While currently used for wireless comms, is also being developed for optical comms between satellites, and from satellites to 'earth' systems, as well as between earth-based systems
- Oil & Gas industry has focused on comms cyber-security to counter serious prior hacks (Goel, 2017): in 2018 the Oil Companies International Marine Forum (OCIMF) included a cyber requirement for tankers as part of their Ship Inspection Report Program (SIRE)
- Suggestion of modified hashing methods (Jackson, 2014), or use of Format Preserving Encryption (FPE) (Roy, 2017) vs current encryption methods that can potentially be more easily hacked
- Use of Continuous Diagnostics & Mitigation (CDM) methods to recognize intrusions and respond in near-real time
- Most current methods have one major problem: they require 'pushing' of software updates, which remains problematic (Nat. Acad. Sci. 2017a,b)

Autonomous systems, including underwater vessels (AUVs), surface vessels (ASVs) and unmanned aircraft (UAS), are coming into use for port and harbor security. Commercial shipping with unmanned vessels is already being developed and tested. Communications between all these systems require cyber-security assurance.

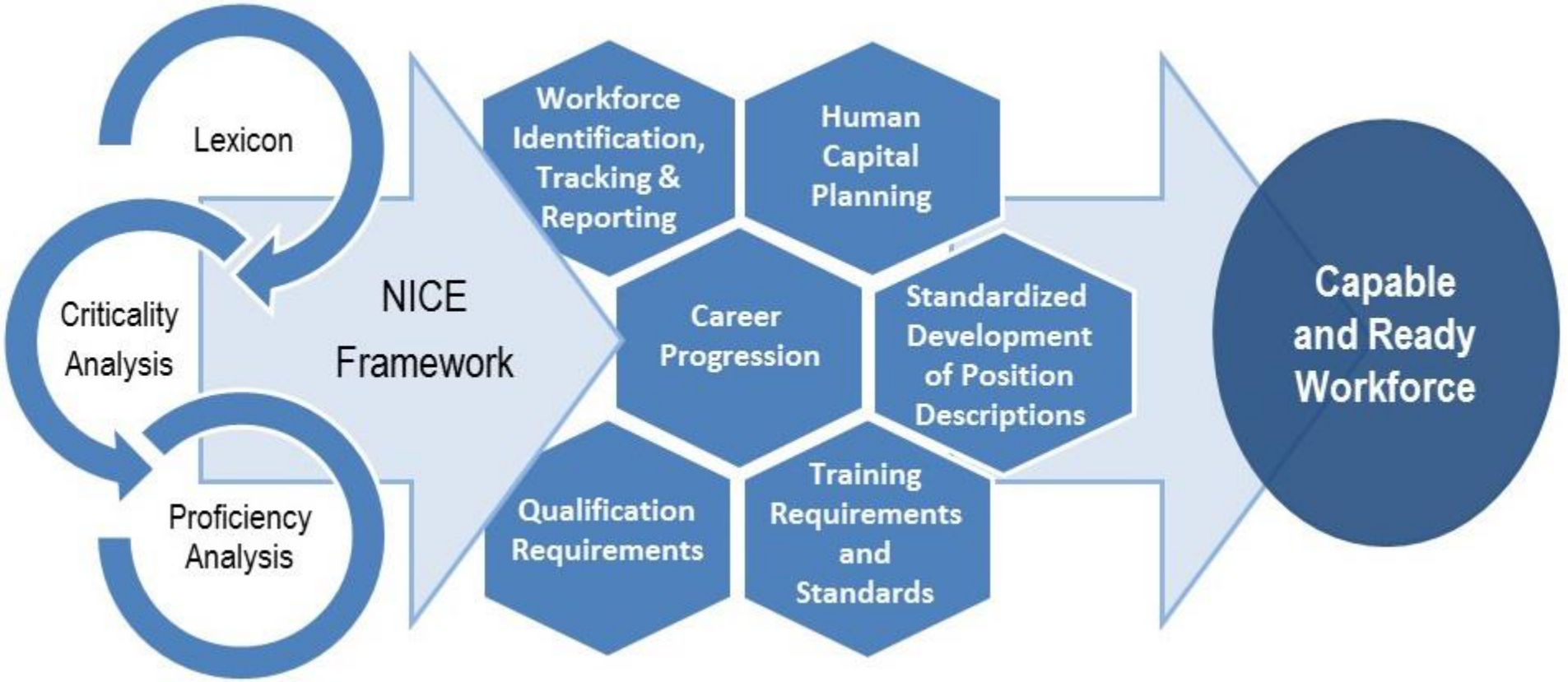
Autonomous Vessels, Unmanned Shipping & Cyber-security Issues

- AUVs, ASVs, UAS will all require cyber-security as an essential part of their operation, especially when used for port & harbor security
- Lloyd's Insurance released recommended cyber-security procedures in 2016
- Rotterdam started a testbeds for Autonomous shipping for Ports
- Trondheimfjord in Norway set up a testbed are for testing autonomous ship operation systems jointly with NTNU
- Security components have been essential to these operations, e.g.:

  The NTNU (Norwegian Science & Technology University) Center for Cyber and Information Security focuses on ASV and Unmanned Shipping Cyber-security
- EU SARUMS (Safety And Regulations for Unmanned Systems) addresses guidelines for AUVs, ASVs and UAS

The Role of Education & Outreach in Advancing Maritime Cyber-security

- Without trained Maritime Cyber-security personnel, maritime cyber-security technology cannot be developed, administered or advanced
- NIST has therefore established a plan for training maritime cyber-security personnel (shown in next slide)
- Several university program are focused on maritime cyber-security, including for example, Stevens Institute, which offers a focused summer program (funded in part by DHS); and Texas A&M University which offers a Cyber-security degree with a focus on maritime cyber.
- In 2017 Congress passed the Maritime Centers of Excellence program – a consortia of Community Colleges which can also include maritime cyber-training
- National Science Foundation Cyber-security Centers of Excellence could potentially also assist in this regard.



The NIST National Initiative for Cybersecurity Education (NICE) has established a Cybersecurity Workforce Framework to ensure a cyber-workforce is developed that can monitor and administer cyber-security standards correctly (NIST, 2018a,b).

Quantum Components of Future Cyber-security

- The National Security Telecommunications Advisory Committee (NSTAC, 2017) advised the President to: “consider the impact of quantum computing…and develop a plan for implementing quantum-resistant encryption schemes”
- Immediate efforts are underway to ensure current encryption technologies can withstand quantum computer attacks
- China already has quantum encryption on principal fiber optic networks between their major cities, and a satellite which does quantum encryption communication, proving quantum encryption methods work
- In 2017 free QUIL quantum computer language & instruction guide was released
- In 2017 a free 1 qbit quantum software testbed was released (Geils, 2017)
- In 2017 IBM made their 5 qbit quantum computer available online free
- In 2017 a new quantum computer chip was developed in NZ which uses manufacturing methods similar to silicon chips, and does not require super-cooling…this method should allow wide use of quantum computing in the near future

Summary & Conclusions

Among other concerns satellite cyber-security remains an issue, but MTS's new Cyber Committee is there to help...

marine technology SOCIETY

Opportunity runs deep™

Maritime Cyber Security and Infrastructure Committee
http://www.mtsociety.org/communities/procommittees/maritime-cyber-security-and-infra.aspx.

This new MTS Professional Committee will:

- Provide a forum for the development & exchange of maritime cyber-security ideas, information & experiences
- Advance awareness of cyber risk
- Promulgate best practices to drive organizational cyber-resiliency
- Coordinate and disseminate through the Committee webpage cyber-security standards, training documents, guidelines, and maritime cyber-security resources, including a list experts and organizations that can be accessed when needed in case of cyber-attacks