Author Code: AB0015

CYBER-RISKS IN UNMANNED VESSEL INDUSTRY AND ADAPTING CURRENT U.S. AND INTERNATIONAL LEGAL FRAMEWORK TO NEW CHALLENGES

INTRODUCTION

With unmanned or self-driving vehicles making headlines on a near-daily rate, it would be irresponsible to assume the shipping industry will remain a bystander in the technological evolution.[1] With seafaring jobs becoming more and more undesirable,[2] the unmanned cargo vessel may be an economic necessity by shipping companies to deal with the dwindling availability of skilled mariners.[3] Currently, there are several projects world-wide researching and testing commercial unmanned vessels:

1. From 2012 through 2015, the Maritime Unmanned Navigation through Intelligence in Networks project (MUNIN), funded by the European Commission, investigated the technical, economic and legal feasibility of unmanned merchant shipping operations.[4] MUNIN proposed a concept whereby the ship's operations are fully autonomous and an operator monitors its status remotely in a shore control center enabling operators to supervise remotely a fleet of autonomous ships, intervening only when the automated system is unable to handle an operation.[5]

2. Rolls-Royce led the Advanced Autonomous Waterborne Applications Initiative (AAWA) to explore the economic, technical, legal and social challenges related to transitioning to increase autonomy in shipping industry.[6] AAWA proposed a more autonomous model than MUNIN with the unmanned ship nearly fully autonomous during the voyage and the interaction between the ship and operator minimal.[7] The ship would execute regular operations with the operator controlling the ship remotely in cases of high risk and complexity as well as while in port.[8]

---

[1] Unmanned vessels have been used for research and military purposes for years. NOAA already utilizes unmanned vessels to expand its knowledge of the environment while minimizing the potentially harmful human footprint. National Oceanic and Atmospheric Administration, 'How NOAA is transforming science with unmanned systems' (14 Jul 2016) <http://www.noaa.gov/news/how-noaa-is-transforming-science-with-unmanned-systems> accessed 15 Nov 2017. U.S. Navy sees unmanned warships as the future of its fleet. Megan Eckstein, 'Navy Betting Big on Unmanned Warships Defining Future of the Fleet' (USNI News, 8 Apr 2019) <https://news.usni.org/2019/04/08/navy-betting-big-on-unmanned-warships-defining-future-of-the-fleet?utm_source=USNI+News&utm_campaign=f55aabdfe9-USNI_NEWS_DAILY&utm_medium=email&utm_term=0_0dd4a1450b-f55aabdfe9-230456729&mc_cid=f55aabdfe9&mc_eid=d2215d145b> accessed 10 Apr 2019.

[2] Livingstone Divine Caesar et al, 'Exploring the range of retention issues for seafarers in global shipping: opportunities for further research*'* [2015] WMU J MAR AFF, v 14, 141 - 157.

[3] *See* Leslea Petersen, 'BIMCO/ICS Manpower Report Predicts Potential Shortage of Almost 150,000 Officers By 2025' (2016) <https://www.bimco.org/news/press-releases/20160517_bimco_manpower_report> accessed 9 Jan 2018; John Grady, 'U.S. Facing Looming Shortage of Merchant Mariners' (USNI News, 2016) <https://news.usni.org/2016/03/22/u-s-facing-looming-shortage-of-merchant-mariners> accessed 9 Jan 2018.

[4] MUNIN, 'Maritime Unmanned Navigation through Intelligence in Networks' (2016) <http://www.unmanned-ship.org/munin/> accessed 14 Nov 2017.

[5] MUNIN, '*Research in Maritime Autonomous Systems Project Results and Technology Potentials*' (2016) <http://www.unmanned-ship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf> accessed 14 Nov 2017.

[6] Rolls-Royce, "Remote and Autonomous Ships: The next steps" (2016) <https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf> accessed 1 April 2019.

[7] ibid 8, 10.

[8] ibid 10-12.

3. In 2017, maritime technology company, Kongsberg, entered an agreement with the Norwegian fertilizer manufacturer, Yara International ASA, to build an electrically-powered autonomous cargo ship that could carry about 100 Twenty-Foot Equivalent Units.[9]

4. Kongsberg is also helping develop Hrönn, a fully-autonomous, light-duty offshore utility ship servicing the offshore farm-fishing industries and energy, hydrographic and scientific industries.[10]

5. In 2017, Mitsui O.S.K. Lines and Mitsui Engineering & Shipbuilding Co. announced a joint development effort of an autonomous ocean transport system via a grant through the Japanese government.[11]

The maritime industry is evolving rapidly and technological advancement introduces new challenges, such as increased cyber-risks. On vessels, increased autonomy decreases the attack-surface area targeted by cyber-attackers by reducing the number of on-board navigation systems, traditionally used for human-based operations.[12] Yet, future remote-controlled or remote-monitored operations of unmanned vessels requires additional communication channels, which introduce new system vulnerabilities, increasing the severity and likelihood of successful exploits.[13] Also, unmanned vessels would completely rely on advanced sensors and automated systems increasing their susceptibility to false sensor data.[14] Cyber-attackers come in multiple forms and with varying motivations and objectives.[15] The unmanned ship may remove a major vulnerability, i.e., crew, for pirates seeking to kidnap crew and passengers for ransom.[16] Such vessels may instead become more appealing to normally non-aggressive "hacktivists" seeking to disrupt activities to alter behavior, for competitors seeking to extract data or disrupt business operations with little risk of human casualty or to criminals focused on stealing goods, ship components or the ship itself.[17] Unmanned vessels with a more vulnerable attack-surface area may also appeal to cyber-attackers not previously attracted to the maritime industry or international shipping.

---

[9] Kongsberg, "Wilhelmsen and Kongsberg Establish World's First Autonomous Shipping Company," <https://www.kongsberg.com/news-and-media/news-archive/2018/wilhelmsen-and-kongsberg-establish-worlds-first-autonomous-shipping-company> accessed 1 April 2019.

[10] Kongsberg, 'BOURGON joins Automated Ships Ltd and KONGSBERG to delivery groundbreaking autonomous offshore support vessel prototype' (2017) <https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/2364B2CBDFE718BDC12581400038D0EF?OpenDocument> accessed 14 Nov 2017.

[11] Mitsui O.S.K. Lines, 'MOL Launches R&D on Autonomous Ocean Transport System: Selected for Japanese Government Transportation Research Program' (26 May 2017) <http://www.mol.co.jp/en/pr/2017/17031.html> accessed 9 Jan 2018; Mitsui O.S.K. Lines, 'MOL-MES Joint Development "Next-generation Vessel Monitoring and Support System": Forging ahead to become "The World Leader in Safe Operation" and provide an "environmental-friendly" service through Open Innovation' (23 Jun 2017) <http://www.mol.co.jp/en/pr/2017/17042.html> accessed 9 Jan 2018.

[12] Kimberly Tam et al, 'Cyber-Risk Assessment for Autonomous Ships' (2018 International Conference on Cyber Security and Protection of Digital Services, 2018) 3.

[13] ibid 3-5.

[14] Petteri Vistiaho, 'Maritime Cyber Security Incident Data Reporting for Autonomous Ships: Master of Science Thesis (2018) <https://pdfs.semanticscholar.org/92eb/793555d584e7613d52d703c5d0b7cffb13d2.pdf> 18.

[15] Tam (n 12) 4.

[16] While the unmanned vessel may embolden a pirate due to the prospect of unopposed hijacking, attacks with goals such as hostage-taking are ineffective against a vessel with no crew. Paul Pritchett, 'Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology' (2015) 40 Tul Mar L J 197, 211.

[17] Tam (n 12) 4. There are four main types of cyber-attackers: hacktivists, competitors, criminals, and terrorists.

This essay provides a two-part analysis of the legal framework for handling cyber-attacks from a proactive then a reactive perspective. Section I evaluates the regulations for avoiding cyber-risk in the maritime industry by identifying the vulnerabilities the unmanned vessel industry introduces and providing suggestions for addressing these vulnerabilities. Section II considers the aftermath of a cyber-attack and identifies those legal frameworks available to victims. Focusing on international treaties and cooperation, this section assesses the effectiveness of investigating and prosecuting cyber-crime in the maritime sector.

DISCUSSION

SECTION I

PROACTIVE REGULATIONS: THE BEST DEFENSE IS A GOOD OFFENSE

Cyber-attacks are not new to the maritime industry. Between 2011 and 2013, drug smugglers hacked into the Port of Antwerp's systems to access shipping container locations and security details. [18] Drug traffickers used this data to place heroin and cocaine inside seemingly legitimate containers. In 2017, a computer virus affected the ICT systems of the world's largest container shipping line and port operator, Maersk, causing many systems to shut down completely, crippling operations for several days.[19] As a result, Maersk incurred financial losses of up to USD$300 million. Also in 2017, a suspected GPS spoofing attack affected at least 20 ships in the Black Sea.[20] Fortunately, the false GPS signal did not cause any collisions or damages. Additionally, an organized cyber-threat group identified as GOLD GALLEON targets maritime shipping organizations and its customers by compromising and spoofing business emails.[21]

1. Regulatory Framework

Cyber-security is necessary in the maritime industry and approaches to mitigating cyber-risk are already under development. In February 2013, President Obama signed Executive Order 13636 which recognized that "[t]he cyber threat to critical infrastructure…represents one of the most serious national security challenges we must confront[,]" defining critical infrastructure broadly so as to include the maritime transportation sector.[22] This order included a directive to the National Institute of Standards and Technology (NIST) "to lead the development of a framework to reduce cyber-risks to critical infrastructure."[23] The resulting Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), collaboratively developed by governmental and private sector entities and promulgated February 12, 2014, identifies "a set of industry standards

[18] Tom Bateman, 'Police Warning After Drug Traffickers' Cyber-Attack' (BBC News, 16 Oct 2013) <http://www.bbc.com/news/world-europe-24539417> accessed 1 Apr 2019.
[19] Safety4Sea, 'Maersk Line: Surviving from a cyber-attack' (31 May 2018) <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/> accessed 1 Apr 2019.
[20] Michael Jones, 'Spoofing in the Black Sea: What really happened' (GPS World, 11 Oct 2017) <https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/> accessed 1 Apr 2019.
[21] Secureworks, 'GOLD GALLEON: how a Nigerian Cyber Crew Plunders the Shipping Industry' (18 Apr 2018) <https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry> accessed 1 Apr 2019.
[22] Exec Order No 13,636, 78 Fed Reg 11,739 (2013). Critical infrastructure are "systems and assets, whether physical or virtual, so vital to the U.S. 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."
[23] ibid § 7(a).

and best practices[.]"[24] Rather than developing new cyber-security standards and risk-management processes, the NIST Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the NIST Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements."[25]

The international maritime industry recognized the importance of the NIST Framework; recently promulgated industry guidance cites and encourages implementation of the NIST Framework. Notably, the Baltic and International Maritime Council issued its Guidelines on Cyber Security Onboard Ships (BIMCO Guidelines) which provides maritime-specific cyber-risk assessment and management procedures based on the NIST Framework.[26] Recognizing the industry's need for cyber-security, the Maritime Safety Committee of the International Maritime Organization (IMO) published a short document entitled "Interim Guidelines on Maritime Cyber Risk Management" (IMO Interim Guidelines) encouraging shipowners/operators to include cyber-risk in their security plans and provides a broad overview of risks for consideration.[27]

2. Concerns

a. Insufficient maritime-focused guidance

A major concern is the maturity of the existing guidelines. The IMO Interim Guidelines is four pages long and provides no guidance, procedural or technical, on cyber-security measures. It instead strongly suggests that ships take necessary safeguards to protect against cyber-risks and directs shipowners/operators to the BIMCO Guidelines and NIST Framework for further reference.

The BIMCO Guidelines are more comprehensive and provide some direction for maritime-specific cyber-risks, including risks associated with unmanned vessels (e.g. risk assessment of ship-to-shore interface in Section 3.1, uncontrolled networks in Annex C).[28] However, the BIMCO Guidelines are procedural rather than technical and provide generic recommendations rather than detailed guidance for cyber-risk assessment, management, countermeasures or products. For example, to address vulnerabilities in ship-to-shore operations, the BIMCO Guidelines recommend that companies understand the ship's operational and informational technology systems and their integration with shore-side operations, but fails to explain how to reach this objective.

Conversely, the NIST Framework, while not industry-specific, does cross-reference numerous technical policies and protocols. Shipowners/operators must then shift through thousands of documents to find relevant and effective protocols. That alone may sufficiently deter shipowners/operators from attempting to create a successful cyber-risk management (CRM) plan. The difficulty is also identifying those protocols relevant to maritime transportation systems and,

---

[24] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity' (2014), *amended as* 'Framework for Improving Critical Infrastructure Cybersecurity' (ver 1.1, 2018) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[25] ibid 2.

[26] Baltic and International Maritime Council, 'The Guidelines on Cyber Security Onboard Ships' (ed 3, 2018) <https://www.bimco.org/products/publications/free/cyber-security>.

[27] International Maritime Organization, 'Interim Guidelines on Maritime Cyber Risk Management' (2016) MSC.1/CIRC 1526, <http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf>.

[28] BIMCO (n 26) 14, 46-49.

with unmanned vessels, the cross-section of maritime transportation systems and automated systems generally.

The U.S. Coast Guard (USCG) formally recognized the nation's maritime interests in its "Cyber Strategy" policy[29] and attempted to provide cyber-security guidelines applicable to certain maritime-regulated facilities.[30] The draft guidelines recommend best practices derived from various standardized industry practices including the NIST Framework. These policies involve establishing roles and responsibilities for a CRM team, policies and program, as well as guidance for implementing these programs over various business models. The draft guidelines only apply to facilities regulated by the Maritime Transportation Security Act of 2002 (MTSA), i.e, shore-side facilities and facilities located on the Outer Continental Shelf. [31] Thus, they would not apply to vessels nor their on-shore operation centers unless those centers are located "in, on, under or adjacent to any water subject to [U.S. jurisdiction]."[32] Based on the promotional material from Rolls-Royce, MUNIN and Kongsberg, the anticipated shore-side facilities for unmanned vessels can be located anywhere and not limited to a water-adjacent location.[33] The USCG's efforts could leveraged by the unmanned vessel industry, expanding the guidance to apply to vessels and joint facilities/vessel with special attention to ship-to-shore communications.

The IMO and USCG need more detailed, cybersecurity-focused guidance before they can adequately provide the U.S. maritime industry with effective CRM policies. The advent of unmanned vessels strengthens the need for clear cyber-security practices both onboard and at ports. The needed vessel-specific guidance on cyber-security should encourage owners/operators to create effective CRM plans. Further, expanding the USCG's MTSA guidance to apply to maritime transportation facilities regardless of their vicinity to the water could encourage the new unmanned vessel industry and also reduce future regulatory changes to accommodate the changing industry.

b. Flexibility and Lack of Compulsion Leads to Inconsistency and Vulnerability

Even with detailed, maritime-specific guidance, owners/operators have no threshold from which to assess their risk tolerance or the appropriate cyber-security tiers applicable to their needs. The NIST Framework and BIMCO Guidelines both gloss over the risk tolerance assessment. The NIST Framework offers four tiers of CRM and offers guidance on how to achieve those tiers but defers to the company to determine the appropriate tier.[34] The tiers range from informal practices managed in an *ad hoc*, sometimes reactive, manner to a formal policy that adapts to previous and current cyber-security best practices. The BIMCO Guidelines similarly defer to owners/operators for assessing cyber-risk tolerance and determining the applicable tier but do note the advantage of employing third-party experts.[35]

The flexibility inherent to these guidelines allows organizations to tailor their CRM approach to meet their unique operating concept as the threats, vulnerability and risk tolerances vary between

---

[29] USCG, 'Cyber Strategy' (2015) <https://www.work.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf?ver=2016-10-13-122915-863> 32-33.

[30] 'Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, 82 Fed Reg 32189 (2017); *see generally* 33 CFR part 105.

[31] ibid.

[32] *See* 46 USC § 70101(3).

[33] *See* Rolls-Royce (n 6); MUNIN (n 4); Kongsberg (n 9).

[34] NIST (n 24) 2.

[35] NIST (n 24) s 4.2

shipowner/operators. Having the ability to assess individual risk and apply the practice that best applies to their circumstances is preferred. Yet, due to the wide-reaching impact of a cyber-attack on vessels, inconsistency in the industry's CRM results in compliant actors, both maritime and inter-modal, at risk due to another's inadequate/nonexistent CRM. One recommendation is that the NIST Framework and BIMCO Guidelines offer direction as to which tiers are "best practice" for specific industries and vessels. For example, barges with mostly analog systems and little-to-no computerization could reasonably implement NIST Framework's first CRM tier whereas Rolls-Royce's proposed container ship and remote operator system should probably be required to employ the fourth tier.

Also, compliance is voluntary. While shipowners/operators are currently required to consider "computer systems and networks" in their security plans, the requirement is imprecise and lacks direction.[36] The IMO only encourages States to address cyber-risks, [37] but should also provide standards for assessment and management techniques of those "computer systems and networks." Similarly, the USCG could expand their current efforts to apply to vessels and all maritime facilities and create a minimum standard applicable to all documented vessels.

The new guidance is available though and shipowners/operators cannot claim ignorance to the dangers posed. Negligence principles would require shipowners/operators to take appropriate steps to mitigate cyber-risk and avoid potential liability for any loss or damages resulting from cyber-attacks.[38] Fear of an unfavorable judgement alone may encourage shipowners/operators to increase their CRM efforts. Also, increased compliance may also be anticipated as classifications societies and insurance underwriters begin to take notice.[39] However, rather than wait for market forces to stimulate action, providing proactive policies would lower technical complexity and costs and encourage early adoption of best practices.

c. Information-Sharing Required for Effective Solutions

Cyber-risks are ever-evolving and cyber-attackers are constantly finding novel, creative ways to access the data they desire. Available cyber-preventive protocols, services and products are only as effective as the last major cyber-attack experienced by the operators and network operators often lack information about attacks experienced by others and the effectiveness of deployed solutions in responding to those attacks.[40] Yet, they are resistant to sharing information for fear of bad press or possibly exposing trade secrets. Coordinating cyber-defense or information sharing may also give rise to antitrust liability deterring further cooperation within the industry.[41]

---

[36] 33 CFR Pts 101-107; IMO, International Ship and Port Facility Security Code (London 2003) Pt B, para 8.3.5.

[37] International Maritime Commission, 'Maritime Cyber Risk Management in Safety Management Systems' (adopted 16 Jun 2017) Resolution MSC.248(98).

[38] The foreseeability of the cyber-risks and insufficient mitigation may be applied in Jones Act litigation by seamen injured due to a cyber-attack. 46 U.S.C. § 30104(a). *See also* 45 U.S.C. § 51 *et seq*.

[39]DNV-GL recently issued guidelines on classifying autonomous and remotely-operated ships requiring CRM utilizing a recognized framework, specifically the NIST Framework. DNV GL AS, 'Class Guideline: Autonomous and remotely operated ships' (Sept 2018) DNVGL-CG-0264, s 4.5. Lloyd's Register also created threat assessment and rick management products to encourage compliance with the BIMCO guidelines. Lloyd's Register, 'Assessing compliance to the BIMCO guidelines' <https://www.lr.org/en/bimco-guidelines/> accessed 7 Mar 2019.

[40] David Simpson, 'Cybersecurity Risk Reduction' (Public Safety and Homeland Security Bureau, Federal Communications Commission, 2017) 40-51.

[41] Nathan Alexander Sales, 'Regulating Cyber-Security' (2013) 107 Nw U L Rev 1503.

However, information sharing is a critical tool for network defenders by allowing them to avoid the missteps of their peers and deploy proven defensive measures.

Information sharing benefits the entire maritime industry and should be considered as part of the IMO and U.S.'s cyber-security policy. Shipowners/operators have mandatory reporting requirements for marine casualties which includes cyber-attacks. Current USCG regulations require certain vessels to keep records of and report security breaches and incidents to the Department of Homeland Security.[42] In 2016, the USCG issued policy guidance specifically placing certain cyber-security events within the scope of reportable incidents.[43] The policy expands the reporting requirements for vessels and USCG-regulated facilities to include all breaches of security, both physical and computer-related, that may result in a transportation security incident, a reportable incident under USCG regulations.[44] Such incidents may range from acts of piracy to intrusions into network systems and instances of viruses and Trojan Horses with a widespread impact.[45] The policy further requires reporting of suspicious activity, both physical and computer-related, which include unsuccessful attempts to access network systems.[46] Due to the countless malicious but low-level events within the cyber-domain, shipowners/operators are advised to report only those events out of the ordinary based on sophistication, volume or other factors which, from the operator's perspective, raise suspicions.[47]

The reach of the regulations extends only to vessels and operators within USCG jurisdiction.[48] As cyber-attacks on the shipping industry have a global effect, CRM in maritime cannot be a domestic concern. In the international realm, the IMO can similarly establish a special obligation for shipowners to report cybersecurity incidents to their flag-State. Subsequently, the flag-State could share knowledge about the type and number of cybersecurity incidents in anonymized form with other flag-States as well as shipowners and other relevant stakeholders, e.g. classification societies and insurance companies, with a view to acquiring a better knowledge base for countering and planning a preparedness against cybersecurity incidents.[49]

Changes are necessary and have been so for a while. These recommendations are not novel and can be useful to all cyber-attack victims, not just unmanned vessels. Perhaps the fast approaching unmanned vessel industry with its increased cyber-risk and unique vulnerabilities will be the catalyst for a much-needed update to the current CRM regulations.

---

[42] 33 CFR §§ 104.235(b), 101.305.

[43] P P.F. Thomas, 'Reporting Suspicious Activity and Breaches of Security' (USCG, U.S. Department of Homeland Security, 2016) CG-5P Policy Letter No 08-16 <https://homeport.uscg.mil/Lists/Content/Attachments/2676/CG-5P%20Policy%20Letter%2008-16_3.pdf>.

[44] ibid 2-3.

[45] ibid 3.

[46] ibid 3-4.

[47] ibid 4.

[48] Jeanne Suchodolski, 'Cybersecurity of Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms' (2018) 20 N.C. J. L. & Tech 121, 161.

[49] Danish Maritime Authority, 'Analysis of Regulatory Barriers to the Use of Autonomous Ships: Final Report' (2017) <https://www.dma.dk/Documents/Publikationer/Analysis%20of%20Regulatory%20Barriers%20to%20the%20Use%20of%20Autonomous%20Ships.pdf > accessed 9 Jan 2018, 36.

SECTION II

REACTIVE LAWS: SEEKING JUSTICE

While proactive regulations/standards are necessary and will prevent or deter most cyber-attacks, they only mitigate rather than eliminate risk. At some point, a cyber-attack will be successful and justice will be demanded. A gut-reaction will be to rely on the existing criminal laws and procedure to investigate and prosecute cyber-crime.

1. Investigation Limitations

a. International Cooperation Needed

There are more than fifty federal laws relating to cyber-security, directly and indirectly, but no overarching framework legislation is in place.[50] Instead, established by Presidential Policy Directive 41 in 2016,[51] the National Cyber Incident Response Plan (NCIRP) creates a government-wide response plan to cyber-incidents, delineating responsibilities and outlining the coordination of federal agencies.[52] The NCIRP establishes a twofold response: (1) efforts directed at tracking down and punishing the aggressor, led by the Department of Justice's Federal Bureau of Investigation and National Cyber Investigative Joint Task Force; and (2) efforts providing support to victims to mitigate the effects of an attack, led by the Department of Homeland Security.[53] At the same time, the intelligence community is tapped to provide assistance to both lines of effort.[54] Rather than prescribing specific actions, the NCIRP outlines how the government is to activate a Cyber Unified Coordination Group to address the specific incidents. Thus, the NCIRP is not an operational plan and, as such, may not have the intended deterrent effect on aggressors.[55] Also, in the realm of unmanned vessels engaging in international trade, the reach of the NCIRP falls short, not only due to its lack of effective deterrence but also for jurisdictional issues. Generally, the most devastating cyber-attacks are often carried out using multiple computers simultaneously from around the globe, hampering the victim nation's ability to pursue justice unilaterally due to jurisdictional issues. This is especially so in the maritime industry due to its inherently global character and the global effects of a cyber-attack. The maritime industry is the backbone of international trade and the global economy – around eighty-percent of global trade by volume and over seventy-percent of global trade by value are carried by sea and handled by ports worldwide.[56] However, there is no comprehensive international framework addressing cyber-security[57] and the current "system" is fraught with complications, delays and diplomatic red-tape.

---

[50]Eric Fisher, 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation' (Congressional Research Services, 2014) R42114, 2-3.

[51] The White House, 'Presidential Policy Directive—United States Cyber Incident Coordination' (26 Jul 2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policydirective-united-states-cyber-incident>.

[52] Department of Homeland Security, 'National Cyber Incident Response Plan' (December 2016) <https://www.uscert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf>.

[53] ibid.

[54] ibid.

[55] Chris Jaikaran, 'Cybersecurity: Selected Issues for the 115th Congress' (Congressional Research Service, 9 Mar 2018) R45127, 20.

[56] United Nations Conference on Trade and Development, 'Review of Maritime Transport 2015' (17 Apr 2017) <http//unctad/org/en/PublicationsLibrary/rmt2015_en.pdf> 48.

[57] William Stahl, 'The Unchartered Waters of Cyberspace: Applying the Principles of International Maritime Law to the problem of Cybersecurity' (2011) 40 Ga J. Int'l & Comp. L 247, 260.

The Council of Europe's Convention on Cybercrime is the only multilateral, legally binding instrument that addresses criminal activity in cyberspace.[58] The Convention on Cybercrime is intended to harmonize substantive criminal law and procedure on cybercrime and facilitate mutual legal assistance. While the Convention identifies specific content-related offenses, e.g., child pornography, and categories of other offenses, it allows the signatory States to unilaterally determine the elements of prohibited conduct and the domestic procedure of enforcement.[59] The Convention does not purport to set out universal standards for prosecuting cyber-attacks or require a particular response or punishment for a given act.[60] Also, it does not compel signatories to enforce one another's domestic laws, relying instead on international cooperation.[61] The U.S. does have multilateral and bilateral treaties with other countries, including non-signatories to the Convention, to ensure mutual assistance in criminal matters, including cyber-crimes.[62] However, while international cooperation is ensured by these Mutual Legal Assistance Treaties (MLATs), the mechanisms available to facilitate investigations are often inefficient and lack oversight.

b. Formalities and Delays

Under an MLAT, prosecutors in one country may request assistance from their counterparts in a foreign country to perform tasks such as the investigation of suspects and the collection of evidence.[63] This is problematic for two reasons. First, access to evidence through an MLAT is restricted to prosecutors, government agencies that investigate criminal conduct, and government agencies that are responsible for matters ancillary to criminal conduct. This explicitly excludes non-government parties such as criminal defendants and civil litigants from accessing evidence through an MLAT.[64] Second, obtaining evidence through formal MLATs between nations can be time-consuming due to the level of formality and the availability of resources. Merely submitting a request from the U.S. requires coordination with the Department of Justice's Office of International Affairs in obtaining a model request, clearance on the content, translation and submission to the other nation.[65] Once a sufficient request is drafted and submitted, the prosecutors must rely on their foreign counterparts to execute the requested task, assuming the foreign state has sufficient resources to and experience in investigating cyber-attacks.[66] According

[58] Convention on Cybercrime (adopted 23 Nov 2007) TIAS 13,174, 2296 UNTS 167.
[59] ibid 4-10.
[60] Jon Jurich, 'Cyberwar and Customary International Law: The Potential of a "Bottom-Up" Approach to an International Law of Information Operations' (2008) 9 Chi. J. Int'l L. 275, 283-284.
[61] ibid 284.
[62] *See* 18 USC § 3181.
[63] T Markus Funk, 'Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges' (Federal Judicial Center, 2014) < https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf> accessed 1 Apr 2019, 5.
[64] Rather, non-governmental parties must use letters rogatory to security evidence located abroad, a process that is less efficient and less reliable. *United Kingdom v United* States, 238 F.3d 1312, 1314 (11th Cir. 2001), *cert. denied sub nom. Raji v. United States*, 534 US 891 (2001). Unlike MLATs, letters rogatory are available only after formal proceedings have commenced and would be useless in the investigation stage. *See In re Letter of Request from Crown Prosecution Serv. of United Kingdom*, 870 F.2d 686, 692 (DC Cir 1989); *see also* 28 U.S.C. § 1782(a).
[65] U.S. Department of Justice, "Treaty Requests," (Criminal Resource Manual) CRM 201-299, <https://www.justice.gov/jm/criminal-resource-manual-276-treaty-requests> accessed 12 Mar 2019.
[66] Jason Gonzalez et al, 'Cases Without Borders: The Challenge of International Cybercrime Investigations' (Criminal Justice, vol 30, no 4, Winter 2016) 17.

to a 2013 report, the MLAT process averages approximately ten months to fulfill, with many requests taking considerably longer.[67]

The MLAT process provides shipowners/operators with little confidence of resolution but alternatives are often lacking or impractical. The IMO may consider creating an informal/expedited process for flag-States and non-governmental victims to seek investigative assistance. Participation would likely be inconsistent and considered a burden by the requested States who may prioritize more formal MLAT requests or who lack sufficient resources. The IMO might provide technical assistance or encourage flag-States to engage in public-private partnerships to lessen the resource burden. The IMO's authority over flag-States requires a balancing act though and it is unlikely we will see any change to the current MLAT process.

2. Extradition Obstacles

Assuming the U.S. is successful in identifying the foreign cyber-attacker, prosecution may be further thwarted by extradition limitations. "Dual Criminality" is a principal of international criminal law under which an accused individual may be extradited "only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations."[68] Under the Convention on Cybercrime, Article 24, the offenses described in the Convention are deemed extraditable offenses in any extradition treaty existing between/among the signatories.[69] However, while the Convention identifies cyber-crime offenses in Articles 2 through 11, States are permitted to determine the elements of the offense. Even if an activity is deemed a cyber-crime under U.S. law, it might not meet the elements of the counterpart crime in the foreign jurisdiction and is, thus, not an extraditable offense.

An alternative to relying on the Convention on Cybercrime for extradition purposes is to apply existing maritime laws. Under the United Nations Convention on the Law of the Sea ("UNCLOS"), dubbed the "Constitution for the Oceans," piracy is specifically addressed by defining conduct that constitutes piracy and describing the duties of all nations with respect to combating piracy.[70] The UNCLOS requires that "[a]ll states…cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State."[71] The UNCLOS defines "piracy" as:

> (a) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed—
>
> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; and

---

[67] Richard Clark, 'Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies' (12 Dec 2013) <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 12 Mar 2019.

[68] *U.S. v Saccoccia*, 18 F3d 795, 800, n. 6 (9th Cir 1994).

[69] Convention on Cybercrime (n 58) 4-10.

[70] United Nations Convention on the Law of the Sea (opened for signature 10 Dec 1982, entered into force 16 Nov 1994) 1835 UNTS 3. Although the U.S. was not a signatory, the U.S. believes many sections of the UNCLOS reflect customary international law which the U.S. does, with some minor exceptions, abide by. The White House, 'United States Oceans Policy, Law of the Sea and Exclusive Economic Zone (10 Mar 1983) National Security Decision Directive Number 83; 'Stewardship of the Ocean, Our Coasts, and the Great Lakes' (19 Jul 2010) Exec Order No 13547, 75 Fed Reg 43021.

[71] UNCLOS (n 70) art 100.

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) Any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).[72]

Under federal law, the UNCLOS definition has been adopted as law and punishable by life imprisonment.[73]

What makes the concept of piracy on the high seas unique is that "it permit[s] nations to invoke universal jurisdiction, such that any country could arrest and prosecute pirates in its domestic courts, irrespective of the existence of a jurisdictional nexus."[74] While there is much debate as to its "universal jurisdiction," UNCLOS does grant concurrent jurisdiction which would allow any State to enforce the UNCLOS.[75] If the cyber-attacker is located in a signatory State, not only would piracy be a punishable crime, but the concurrent jurisdiction allows that State to prosecute on behalf of the victim's State. This avoids extradition concerns and dual criminality issues.[76] However, as the proceedings would then be subject to the local State's laws, the victim's reparations would be limited to those available by the local State.[77]

Though a cyber-attack on a vessel should logically be considered piracy, the definition of piracy under UNCLOS would have to be updated to include cyber-attacks. The definition is premised on the use of a ship or aircraft by the pirates. In a cyber-attack, the aggressor would need neither ship nor aircraft to commit an attack on a vessel. It is recommended that the definition remove the language "by the crew or the passengers of a private ship or a private aircraft" to encompass remote attacks.[78]

---

[72] ibid art 101.

[73] 18 U.S. Code § 1651. *See U.S. v. Dire*, 680 F3d 446, 459 (4th Cir. 2012); *Inst. of Cetacean Research v. Sea Shepherd Conservation Soc'y*, 725 F3d 940, 944 (9th Cir. 2013) (noting that the U.S. has refused to ratify UNCLOS but the courts found the piracy definition therein to be an accurate statement of customary international law).

[74] *U.S. v. Hasan,* 747 F.Supp.2d 599, 605 (EDVA 2010) (citing 4 William Blackstone, *Commentaries* (describing piracy, in the mid–1700s, as an "offence against the universal law of society," "so that every community hath a right, by the rule of self-defense," to punish pirates)).

[75] UNCLOS (n 70) art 105.

[76] Absent concurrent jurisdiction, jurisdiction to capture and prosecute pirates would still be present under traditional notions of standing. UNCLOS (n 70) 92.

[77] UNCLOS (n 70) art 105.

[78] It should be noted that the U.S. should also update its federal piracy law to clearly reference the UNCLOS and its successors to avoid inconsistent judicial interpretations. In 2010, the U.S. Navy thwarted two separate alleged acts of piracy and the U.S. charged the individuals in the same U.S. District Court on charges of piracy resulting in two inconsistent definitions of piracy. The first trial ended with the defendants found guilty on numerous charges, including piracy. *U.S. v. Hasan,* 747 F.Supp.2d 599 (EDVA 2010). The defendants argued that the charge of piracy should be dismissed because "general piracy requires a robbery on the high seas, and that, because robbery requires the 'taking' of property, the Government's failure to allege any actual taking precludes a conviction for general piracy." The court concluded "that both the language of 18 U.S.C. § 1651 and Supreme Court precedent indicate that the 'law of nations' connotes a changing body of law, and that the definition of piracy in 18 U.S.C. § 1651 must therefore be assessed according to the international consensus definition at the time of the alleged offense." The court adopted the UNCLOS art 101 definition of piracy and the defendants were found guilty on fourteen (14) counts each of piracy, attack to plunder a vessel, assault and related charges. In contrast, the other trial dismissed the charge of piracy as the 1820 Supreme Court case, *U.S. v Smith*, 18 US (5 Wheat.) 153, 162 (1820), was the "definitive authority

Arguments may be made then that piracy should not apply to the unmanned vessel. The perceived motivation for concurrent jurisdiction, or universal jurisdiction, was the heinousness of piracy.[79] With an unmanned vessel however, there can be no violence against the persons not onboard. While acts that involve "violence" do not have to be directed at a person, [80] it is doubtful that taking control of an unmanned vessel by exploiting weaknesses in its electronic information systems would be considered violent. However, as the effects of a cyber-attack on a shipping vessel, regardless of manning, can have far reaching and devastating results, piracy should include cyber-attacks and apply to all vessels, both manned and unmanned.

CONCLUSION

Cyber-crime is a serious and growing problem with global effects in the maritime sector. The emergence of unmanned vessels with their unique vulnerabilities should spur increased activity in preventing and addressing cyber-risk and crime. As sophisticated cyber-attacks are difficult to uncover and attribute and cyber-attackers are often outside the reach of U.S. courts or judgment proof, few if any cyber-attacks will end up in criminal and civil litigation. While the reactive laws on cyber-crime investigation and prosecution should be updated, greater deterrence and more effective cyber-risk mitigation will result from more proactive measures and planning. The NIST Framework and BIMCO Guidelines are a good starting point, but are not comprehensive and offer too much flexibility to shipowners/operators. It would behoove the USCG and IMO to promote best practices and facilitate information sharing. They should offer more maritime-specific technical guidance and risk management direction as well as make CRM mandatory. There will be no one-size-fits-all approach but, at a minimum, we should require shipowners/operators in one of the most vital transportation sectors to implement basic cyber-security preparedness.

on the meaning of piracy" and defined piracy as "robbery upon the sea." *U.S. v. Said*, 3 F. Supp. 3d 515 (EDVA 2014), *reversed in part, vacated in part, remanded U.S. v Said*, 798 F3d 182 (4th Cir 2015). This ruling was later overturned on appeal and upheld the UNCLOS definition of piracy.

[79] Eugene Kontorovich, 'The Piracy Analogy: Modem Universal Jurisdiction's Hollow Foundation' (2004) 45(1) Harvard International Law Journal 183, 205.

[80] *Inst of Cetacean Research v Sea Sheperd Conservation Soc'y*, 725 F2d 940, 944 (9th Cir 2013) ("[M]alicious acts against inanimate objects also comports with the commonsense understanding of the term.").