A TALE OF TWO TREATIES: A MARITIME MODEL TO STOP THE SCOURGE OF CYBERCRIME

Brendan Sullivan*

ABSTRACT

Most of the goods purchased in the developing world are transported between countries aboard a ship operated by one of five companies. At least four of those companies have fallen victim to a cyber-attack. Their vulnerabilities can lead to devastating impacts on economies that rely on maritime transportation for development and prosperity. By shoring up cyber-vulnerabilities in the maritime industry, governments can set an example that will benefit all markets.

This article proposes a protocol to a maritime treaty, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention), as the first step to implementing the cyberthreat reporting and coordination mandates needed to combat cybercrime. Using two examples of attacks on technology in the maritime sector, the article discusses cyber-vulnerabilities that threaten the industry. One of these attacks impacted navigation systems aboard a ship while the other impacted cargo tracking systems, but both threaten the economic security of cargo interests that extend from transcontinental manufacturers to the store shelf. With these threats in mind, this article analyzes existing legal structures that prosecute cyber crimes.

Two treaties, one targeting threats to the maritime industry, and one targeting cyber-threats, should be leveraged to enact laws that will hold

* Commander Brendan Sullivan, Judge Advocate, United States Coast Guard, is presently assigned as Staff Judge Advocate, U.S. Coast Guard Cyber Command, Washington, D.C. He holds a Masters license for limited tonnage vessels and a license to serve as Second Mate aboard unlimited tonnage vessels. The views expressed are those of the author and do not reflect the official policy or position of the United States Coast Guard or Department of Homeland Security. He would like to thank the editors for their perseverance through challenging times and Mr. Brian Wilson, Professor David Stewart, and Lauren Sullivan for their support, noting that the views taken in this paper are not necessarily theirs.

cyber criminals liable. Even though these treaties are widely accepted, there is little evidence that nation states are using them to effectively combat cybercrime. Accordingly, this article proposes a protocol that will prompt cyberattack reporting and prosecutorial coordination in the maritime industry. Once proven effective, this protocol could be replicated in cybercrime treaties to promote broader reporting and coordination needed to stop the scourge of cybercrime.

CONTENTS

INTRODUCTION

> The jobs and livelihoods of billions of people in the developing world, and standards of living in the industrialized and developed world, depend on ships and shipping. The shipping industry has played an important part in the dramatic improvements in global living standards that have taken millions of people out of acute poverty in recent years. It will be just as critical for the achievement of the 2030 Agenda for Sustainable Development . . . . [1]

Everything from food to medicine is transported transnationally by ship to support jobs and standards of living for the world's growing population.[2] Even landlocked countries depend on goods shipped overseas and intermodally transported to their businesses.[3] Consequently, cyberattacks interfering with a ship's navigational equipment or programs designed to keep track of a ship's cargo and where it is going, can severely impact the price and availability of goods relied on by manufacturers, retailers, and consumers.[4] As exemplified by recent interruptions to market supply chains caused by the Covid-19 virus, a relatively moderate disruption to just-in-time distribution has cascading effects that directly impact consumers in the United States (U.S.) and across the world.[5] Exacerbating the problem, the top

---

[1] Press Release, U.N. Secretary-General, Maritime Transport Is 'Backbone of Global Trade and the Global Economy,' Says Secretary-General in Message for International Day, U.N. Press Release SG/SM/18129-OBV/166-SAG/486 (Sept. 22, 2016).

[2] *See id.*

[3] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, REVIEW OF MARITIME TRANSPORT 2013, ch. 6, U.N. Doc UNCTAD/RMT/2013, U.N. Sales No. E. 13.II.D.9 (2013).

[4] *See* Nishan Degnarain, *Could Oil Ship Wakashio Been Hacked Before Mauritius Spill?*, FORBES (Oct. 26, 2020), https://www.forbes.com/sites/nishandegnarain/2020/10/26/could-mol-chartered-mauritius-oil-spill-ship-wakashio-have-been-hacked/?sh=ac178e37fbbc; Jonathan Saul, *Global Shipping Feels Fallout from Maersk Cyber Attack*, REUTERS (June 29, 2017), https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE/. *See also* Victoria Coates and Robert Greenway, *The Next Suez Threat? A Big Hack*, BLOOMBERG (Mar. 30, 2021), https://www.bloomberg.com/opinion/articles/2021-03-30/a-cyber-attack-could-be-the-next-big-suez-canal-threat.

[5] See *The New Coronavirus Could Have a Lasting Impact on Global Supply Chains*, THE ECONOMIST, (Feb. 15, 2020), https://www.economist.com/international/2020/02/15/the-new-coronavirus-could-have-a-lasting-impact-on-global-supply-chains, for an explanation about how modern U.S. product distribution increasingly depends on goods being transported for production and distribution chains only when needed for sales. Unanticipated worker shortages, or any other interference with those goods arriving precisely when needed, results in a product deficit which in turn raises prices for that good. When other products depend on that good being produced (such as may be the case for a vehicle manufacturer that relies on tires being produced in order to finish building a car) the deficit has a cascading effect.

five cargo carriers control sixty-three percent of the containership market, which means that a company-wide network problem for one of these top corporations results in massive logistics problems that are felt around the world.[6]

Two events in June 2017 vividly demonstrate cyber-threat vulnerabilities in the maritime sector and the disastrous impacts they may have on supply chains supporting world markets. The first was an attack on shipboard navigation systems that caused navigators in the Black Sea to think their vessels were located miles away from their actual location.[7] The second was a malware attack that seized the world's largest containership company for days, leaving ports congested and goods aboard ships without a destination.[8]

This paper compares two legal frameworks in place that may be applied to prosecute perpetrators like those who caused havoc on the maritime industry in June 2017. Finding that legal frameworks currently in place adequately allow for cybercrime prosecutions in the maritime industry, the paper then considers what more can be done to stop the scourge of cybercrime. As will be discussed, a layered approach, that first establishes reporting and coordinating requirements for the maritime industry, will combat cybercrime in a sector that is the foundation for a large portion of the world's economy while also serving as a template for broader initiatives to fight cybercrime.

The Suppression of Unlawful Acts Against the Safety of Maritime Navigation Convention (SUA Convention)[9] and the Council of Europe Convention on Cybercrime (Budapest Convention)[10] take parallel approaches to addressing transnational criminal acts. With these multilateral agreements in place and little progress stunting cyberattacks, more must be done to prosecute these crimes. This paper recommends a protocol to the SUA Convention that will ratchet up governmental responses to transnational cybercrime by working with private sector shipping corporations to coalesce, analyze, and address indicators of cyberattacks that affect their interests. If successful, the protocol could be modified for broader application and

---

[6] Andrea van der Biest, *Top 10 Ocean Carriers Around the World*, CARGOFIVE.COM (Mar. 6, 2019), https://cargofive.com/top-10-ocean-carriers-around-the-world/.

[7] *See* Dana Goward, *Mass GPS Spoofing Attack in Black Sea?*, MAR. EXEC. (Jul. 11, 2017), https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

[8] *See* Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED.COM (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[9] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 27 I.L.M. 688, 1678 U.N.T.S. 221 [hereinafter SUA Convention].

[10] Convention on Cybercrime art. 5*, opened for signature* Nov. 23, 2001, Europ. T.S. No. 185 (entered into force Jan. 7, 2004) [hereinafter Budapest Convention].

considered as a protocol to the Budapest Convention, setting a trend for cybercrime prosecutions that will secure economic vulnerabilities in sectors beyond the maritime industry.

Both the SUA Convention and the Budapest Convention go a long way to require information sharing between parties and prosecution of those responsible for interference with critical equipment.[11] However, cyberthreats continue to be a major concern for businesses and the economy. Therefore, protocols need to supplement prosecutorial options by insisting upon a robust scheme for corporate reporting, investigations, and cybercrime prosecutions. In addition, mechanisms should be put in place for parties to engage in a coordinated response against cyber-threats.

Section I below describes two cases of disruption to marine transportation technology that exemplify the potential for disastrous impacts on the maritime industry and devastating impacts on global economies. Though the two events reflect distinct approaches to attacking maritime interests, either approach could be executed on a larger scale, wreaking havoc for businesses worldwide. Collectively, these examples can be used to show why cybercrime in the maritime industry is a particular vulnerability for economic security.

Section II discusses two multilateral agreements in place that may be leveraged to stop the perpetrators of cyberattacks impacting maritime interests. This section reviews common aspects of criminal treaties, how they apply to cybercrime, and how they address rapidly changing global interactions. Both agreements are incorporated into U.S. law and establish common frameworks for international criminal law that could be implemented effectively throughout the world.[12] The discussion finds that legal instruments are generally in place to prosecute an attributed cybercrime that interferes with a ship's navigation system. Similarly, international agreement and legislation is in place to address attacks that interfere with computer systems affecting a ship's cargo. Thus, the solution to cybercrime problems rests in mechanisms that will generate resources and evidence to prosecute the perpetrators of these attacks.

Given the utility of these legal frameworks, Section III undertakes a proposal to address the reason why existing structures fail to stop evolving cyberthreats. The proposal leverages reporting requirements and

---

[11] *See* SUA Convention, *supra* note 9, arts. 3, 6-7, 10, 13-15; Budapest Convention, *supra* note 10, preamble, arts. 24-26.

[12] *See* 18 U.S.C. § 1030 (codification of Budapest Convention); 18 U.S.C. § 2280 (codification of SUA Convention); Alexandra Van Dine, *When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures Under the Budapest Convention*, 20 CHI. J. INT'L L. 530, 535 (2020); THOMAS J. SCHOENBAUM, ADMIRALTY AND MARITIME LAW §2:32 (Nov. 2020).

coordination, two components of U.S. law that apply to the maritime industry domestically. The draft protocol appended to this article creates an international specialized agency charged with receiving reports of suspected cybercrime and assisting with the investigation and prosecution of those crimes. By applying these measures, this paper proposes that the maritime sector can be far more effective in its ability to prosecute cybercrimes.

In Section IV, this paper addresses domestic implementation and cybercrime prosecutions under the protocol proposed. It considers how courts in the U.S. would use a global system that coordinates cybercrime reporting, analysis, and prosecution. Perhaps just as importantly, it also assesses whether foreign courts will be able to effectively use a global coordination system. Recognizing how difficult coordination, transnational investigations, and information sharing can be even outside the cyber context, global efforts to gather evidence and use it in criminal prosecutions presents profound challenges. If those challenges are not addressed now, they will be exacerbated as networks and systems increase the amount of data they use and exchange.

In Section V, this paper concludes by emphasizing the importance of additional measures to combat cybercrime. Though companies may initially resist the additional burdens that result from reporting and investigatory efforts, the proposal put forth in this paper may open corporate eyes to the utility of such efforts. Section V explains why taking steps to shore up cyber vulnerabilities in the maritime industry will set an example that other international trade sectors will want to follow by imposing reporting and coordination measures to combat cybercrime.

I. BACKGROUND

Modern streams of commerce are so dependent on stable merchant shipping that a single maritime disaster, even one occurring far from U.S. shores, can significantly disrupt domestic markets. On June 24, 2017, the six hundred foot long *Tank Vessel Atria*, a twenty three thousand ton ship that carries oil and other dangerous cargoes, was making its approach past the rocky Black Sea coast of Novorossiysk, Russia when a series of alarms sounded.[13] The alarms alerted the navigation team that equipment used to track the ship's location could not accurately account for the vessel's position.[14] The ship's master, Captain Gurvan Le Meur, plotted a position indicating that the ship was hard aground at an airport almost thirty miles

[13] Matt Burgess, *When a Tanker Vanishes, All the Evidence Points to Russia*, WIRED.COM (Sept. 21, 2017), https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

[14] *Id*.

away from where it was actually located.[15] Nineteen other ships reported a similar anomaly affecting their ability to safely navigate.[16] In total, since 2016, over thirteen hundred ships have been affected by such acts which are known as GPS spoofing attacks.[17] As recently as September 2020, federal agencies warned of worldwide GPS interference affecting shipping.[18]

Following the 2017 spoofing incidents in the Black Sea, researchers from the University of Texas demonstrated that they could mirror the spoofing that occurred with commercially available equipment costing less than one thousand dollars.[19] The ramifications are that the modern-day pirate does not need to get underway to capture a ship for ransom, shipping competitors can create havoc for their rivals, and terrorists can disrupt the supply chain of commerce that supports the U.S. economy. A single ship can carry cargo worth $700 million.[20] Interfering with navigation systems aboard the thirteen hundred ships that have proven vulnerability to spoofing attacks has the potential to prevent cargo worth over nine hundred billion dollars from reaching the intended destination. Multiply that impact by several voyages cancelled or delayed while a ship undergoes repairs following an incident caused by faulty navigation equipment, and the results are disastrous.

Just five days after the spoofing event in the Black Sea, malware resembling a variant of ransomware, devastated world markets by seizing corporate computer systems including those operated by Maersk, the world's largest container ship company.[21] The attack cost Maersk three-hundred million dollars and damaged various businesses worldwide ranging from

---

[15] *Id*.

[16] Michael Jones, *Spoofing in the Black Sea: What Really Happened?*, GPS WORLD (Oct. 11, 2017), https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

[17] C4ADS, ABOVE US ONLY STARS: EXPOSING GPS SPOOFING IN RUSSIA AND SYRIA (2019), https://www.c4reports.org/aboveusonlystars [herein after *Above Us Only Stars*].

[18] *2020-016-Various-GPS Interference*, U.S. DEP'T OF TRANSP. MAR. ADMIN. (Sept. 22, 2020), https://www.maritime.dot.gov/msci/2020-016-various-gps-interference.

[19] *See* Jones, *supra* note 16; *UT Professor Hacks Drone's GPS System*, KERA NEWS (July 2, 2012), https://www.keranews.org/texas-news/2012-07-02/ut-professor-hacks-drones-gps-system.

[20] Sharon Silke Carty, *When Cargo Gets Lost at Sea, Firms Can See Big Losses and Shortages*, USA TODAY (Aug. 4, 2006), https://usatoday30.usatoday.com/money/world/2006-08-03-cargo-problems-usat_x.htm.

[21] *10 Largest Containership Companies in the World in 2021*, MARINE INSIGHT NEWS NETWORK, (Aug. 25, 2021), https://www.marineinsight.com/know-more/10-largest-container-shipping-companies-in-the-world/.

Cadbury Chocolate[22] to Durex Condoms,[23] costing a total of ten billion dollars.[24] But for Maersk's luck in finding an unaffected server in Ghana, the damage may have been exacerbated, potentially ruining Maersk and thousands of businesses that rely on it to transport goods to downstream consumers.[25]

Like the spoofing incident in the Black Sea, the attack on Maersk's network is not an isolated event. In early April 2020, Mediterranean Shipping Company, the second largest containership company in the world, was hit by a network outage.[26] Initial assessments conclude that the outage was caused by a cyberattack.[27] In September 2020, another top ranked container line with strong ties to shipping interests in the U.S., suffered a malware attack that required the company to cut off external access to applications that facilitate bookings and other inputs necessary to meet merchant demands.[28]

II. WHAT LEGAL REGIME APPLIES?

The SUA Convention, addressing acts against maritime navigation, and the Budapest Convention, addressing cybercrime, provide complementary frameworks for addressing transnational crime. While the SUA Convention broadly addresses the concern of interference with vessel navigation, the Budapest Convention addresses interference with computer systems.[29] These, and other authorities that may allow for cybercrime prosecution, should be buttressed by a protocol that demands corporate reporting, evidence sharing, and accountability.

International law determines jurisdiction to prescribe crimes by assessing

---

[22] Liam Tung, *Petya Attack Caused $140m Hit on Cadbury Parent Mondelēz's Q2 Revenues*, CSO ONLINE (Aug. 3, 2017), https://www2.cso.com.au/article/625588/petya-attack-caused-140m-hit-cadbury-parent-mondel-z-q2-revenues/.

[23] Reckitt Benckiser, *Massive Cyber-Attack Could Cost Nurofen and Durex Maker £100m*, THE GUARDIAN (Jul. 6, 2017), https://www.theguardian.com/business/2017/jul/06/cyber-attack-nurofen-durex-reckitt-benckiser-petya-ransomware.

[24] Greenberg, *supra* note 8.

[25] *Id*.

[26] Costas Paris, *Mediterranean Shipping Co. Hit by Network Outage, Considering Potential Cyberattack*, WALL ST. J. (Apr. 10, 2020), https://www.wsj.com/articles/mediterranean-shipping-co-hit-by-network-outage-considering-potential-cyberattack-11586523861.

[27] *Id*.

[28] JOC Staff, *Cyber Attack Cripples CMA CGM Website*, JOC (Sep. 28, 2020), https://www.joc.com/maritime-news/container-lines/cyber-attack-cripples-cma-cgm-website_20200928.html.

[29] *See* SUA Convention, *supra* note 9, preamble, art. 3; Budapest Convention, *supra* note 10, preamble, arts. 4, 5, 8.

five core principles[30] – law of the territory affected, law of the offender's country, law of the national affected, law of the country with protected rights, and law of the global community recognized through universal jurisdiction.[31] In the case of a crime committed against a commercial ship on the high seas, the country where the ship is registered (also called the ship's flag state) is recognized with jurisdiction to enforce law and regulation aboard its ships.[32] However, few flag states have sufficient law enforcement resources and shipping companies have little interest in tying their ships up with investigatory efforts, especially if it means holding their vessels from preciously needed time to transport cargos.[33]

More and more, port states, the countries where merchant ships load and land their cargoes, are asserting jurisdiction over criminal acts affecting shipping.[34] As the world's largest importer,[35] the U.S. has particular interest in exercising its port state jurisdiction to ensure goods are transferred efficiently and the country is protected from uncertain threats that may exist aboard foreign ships entering U.S. waters.[36] As the U.S. takes on this role, it is increasingly reliant on mechanisms that allow it to coordinate with foreign

---

[30] In the U.S., jurisdiction is categorized as authority to prescribe (make) laws; authority to apply (adjudicate) law; and authority to compel compliance (enforce) law. *See* RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (AM. LAW. INST. 2018).

[31] *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 402, 402 cmts. a-g, 404 (AM. LAW INST. 1987).

[32] *See* United Nations Convention on the Law of the Sea arts. 92, 94, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994) [hereinafter UNCLOS]. *See also* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 501.

[33] *See* THE FLETCHER SCHOOL OF LAW AND DIPLOMACY, LAW OF THE SEA: A POLICY PRIMER 53-54, 56 (John Burgess et al., 2017); Costas Paris, *Global Shipping Faces Troubling New Smuggling Questions: As Containers Get Bigger, Drug Smugglers Are Growing Bolder in Hitching Rides on Commercial Supply Chains*, WALL ST. J. (Jan. 6, 2020), https://www.wsj.com/articles/global-shipping-faces-troubling-new-smuggling-questions-11578330634.

[34] *See generally* Yaodong Yu, Yue Zhao & Yen-Chiang Chang, *Challenges to the Primary Jurisdiction of Flag States Over Ships*, 49 OCEAN DEV. & INT'L. L. 85 (2018).

[35] In 2017, the U.S. imported goods worth $2.16 trillion, making it the largest importer in the world. *See United State*s, OBSERVATORY OF ECON. COMPLEXITY (last visited Aug. 14, 2021), https://oec.world/en/profile/country/usa/.

[36] See *A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security Before the Coast Guard and Maritime Transportation Subcomm. of the H. Comm. on Transportation and Infrastructure,* 114th Cong. 101 (2015) (statement of Professor Stephen E. Flynn, Ph.D.), for a discussion concerning security vulnerabilities in U.S. intermodal supply chains.

governments, especially when pursuing criminal sanctions.[37]

In the context of a cybercrime impacting commercial shipping, the SUA Convention, as implemented, criminalizes interference with navigation and ship systems impacting the vessel's safety.[38] The Budapest Convention, as implemented, criminalizes interference with computer systems.[39] These agreements establish mechanisms to outlaw interference with a ship's navigation system, its cargo systems, or even its personnel management systems.[40]

Though the SUA Convention and the Budapest Convention establish sound structures to address evolving criminal issues, the global nature of cybercrime and the disunity of law across the world pose challenges to law enforcement. Especially when addressing rapidly changing technological domains such as those that apply in global shipping, unilateral government efforts create an uneven patchwork of enforcement.[41] That inconsistent legal landscape then results in insufficient notice of the laws that will be applied in the cyber domain, economic tensions between trade partners, and, in some cases, diplomatic tensions between governments with conflicting expectations.[42] As evidenced by the Budapest Convention, even multilateral agreements can produce uncertain results when transnational obligations are implemented domestically with varying interpretations.[43] However, by

---

[37] *See Maritime Security and Navigation*, U.S. DEP'T OF STATE, https://2009-2017.state.gov/e/oes/ocns/opa/maritimesecurity//index.htm (last visited Aug. 14, 2021)*; A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security*, *supra* note 36, at 12. *See generally International Efforts to Combat Maritime Piracy: Hearing Before the Subcomm. on Int'l Orgs, Hum. Rts. & Oversight of the H. Comm. of Foreign Affs.,* 111th Cong. (2009).

[38] SUA Convention *supra* note 9, art. 3

[39] Budapest Convention *supra* note 10, art. 8.

[40] As defined by articles 4 and 5 of the Budapest Convention, interference includes damaging, deleting altering, or suppressing data. *See* Budapest Convention *supra* note 10, arts. 4, 5.

[41] Lijun Zhao, *Uniform Seaborne Cargo Regimes – A Historical Review*, 46 J. MAR. L. & COM. 133, 165 (2015) (calling for harmonized cargo liability regimes that are flexible enough to adapt to technological developments). Uniformity has always been a cornerstone of maritime and global commerce; efficiencies gained through technological advancements only reinforce demand for the historical principles of uniformity Justice Story articulated in *De Lovio v. Boit*, 7 Fed Cas. 418 (No. 3776) (C.C.D. Mass 1815).

[42] Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 777 (2016) (*citing* OFFICES OF THE U.S. ATTORNEYS, CRIMINAL RESOURCE MANUAL § 279(B) (1997) as evidence of diplomatic costs imposed by conflicts of law between countries).

[43] See Jonathan Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, 40 MONASH L. REV. 698, 733 (2014), for a discussion recognizing disparate interests in the cyber domain where some parties may be singularly focused on cybercrime, but others see the Budapest Convention and similar agreements as part

agreeing to the obligations set out in these conventions, countries that are interconnected by trade and technology can coordinate to level expectations. The result is that even where laws are not in lockstep, all parties are on notice when action may be taken against one of their citizens or commercial ships registered in the country.

A. The SUA Convention

The SUA Convention is a model for multilateral law enforcement coordination. It was formed to address the emerging threat of maritime terrorism and its globalized impact.[44] While cybercrime in the maritime industry was an unforeseen problem at the time the SUA Convention went into force, the Convention creates a framework for international coordination and information sharing that is useful for other law enforcement efforts including cybercrime.[45]

In October 1985, four members of the Palestinian Liberation Front (PLF) hijacked a cruise ship named the *Achille Lauro* and ordered it to get underway.[46] Over the course of the three-day hijacking, the captors killed a handicapped American passenger and threatened to blow up the ship.[47]

When the ship was released and the captors were apprehended, a series of jurisdictional concerns unfolded. Of primary importance, it was unclear whether the hijacking could be prosecuted as a piratical act because the accepted definition of piracy requires that the act is committed by one ship against another for "private ends."[48] The *Achille Lauro* hijacking was executed by terrorists disguised as passengers aboard the ship rather than pirates boarding from a separate vessel.[49] The perpetrators also committed their crimes for political ends which may be distinguished from personal or private benefits derived from criminal acts.[50] While this type of politically

---

of a broader information security effort.

[44] *See* SUA Convention, *supra* note 9, preamble.

[45] *See id.*

[46] Gregory V. Gooding, *Fighting Terrorism in the 1980's: The Interception of the Achille Lauro Hijackers*, 12 YALE J. INT'L L. 158, 164 (1987).

[47] *Id*.

[48] Piracy is defined by five elements: 1) an illegal act of violence, detention, or depredation, 2) committed for private ends, 3) by the crew or passengers of a private ship or aircraft, 4) against a ship or aircraft, or property, 5) on the high seas or outside the jurisdiction of any state. UNCLOS, *supra* note 32, art. 101; Convention on the High Seas art. 15, Apr. 29, 1958, 13 U.S.T. 2312, 450 U.N.T.S. 82.

[49] Malvina Halberstam, *Terrorism on the High Seas: The Achille Lauro, Piracy and the IMO Convention on Maritime Safety*, 82 AM. J. INT'L L. 269, 269 (1988).

[50] *Id*. at 289 (discussing the hostage takers' motivations in seeking the release of PLF prisoners).

motivated attack was not unique,[51] the global community recognized it was poorly equipped to respond on this occasion, causing world leaders to rally for implementation of the SUA Convention as a way of criminalizing terrorist events occurring on ships at sea.[52]

1. SUA Offenses

Though created to prosecute and prevent maritime terrorist acts like the ones that occurred on the *Achille Lauro*, the SUA Convention, as adopted, mandates steps that apply broadly in an effort to prevent any unlawful and intentional act that would interfere with a vessel's safe navigation.[53] Under Article 3, parties to the Convention agree to impose criminal offenses for specific acts including (1) seizure or control over a ship by force or threat of force, (2) violent acts likely to endanger the safe navigation of the ship, (3) destruction of the ship or its cargo in a manner that is likely to endanger the safe navigation of the ship, (4) placing a device on a ship which endangers or is likely to endanger the navigation of a ship, or (5) destruction or serious damage to navigational devices which may endanger the safe navigation of a ship.[54] Depending on the specific circumstances of a cyber-related incident impacting a merchant ship or a shipping company, these offenses would be chargeable as unlawful control of a ship, damage to the ship or its cargo, or interference with navigational facilities.[55]

2. SUA as Implemented Under U.S. Law

In the U.S., the SUA Convention and a related protocol for unlawful acts against the safety of fixed platforms on the Continental Shelf were agreed to with the advice and consent of the Senate without reservation within two years of being signed in 1988.[56] The Convention was then directly implemented into domestic law through certain provisions in the Violent

---

[51] *See* Dennis L. Bryant, *Historical and Legal Aspects of Maritime Security*, 17 U.S.F. MAR. L.J. 1, 1-3 (2004) (describing a 1961 incident where a cruise ship was attacked by a Portuguese rebel group).

[52] *See* Larry A. McCullough, *International and Domestic Criminal Law Issues in the Achille Lauro Incident: A Functional Analysis*, 36 NAVAL L. REV. 53, 60, 72-78 (1986).

[53] The SUA Convention Preamble provides that it was designed in consideration of the "need for all States, in combating unlawful acts against the safety of maritime navigationFalse" SUA Convention, *supra* note 9, preamble.

[54] *Id.* art. 3.

[55] *See id.*

[56] *See generally* Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, and the accompanying Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, both signed at Rome on March 10, 1988, S. Consideration of Treaty Doc. 101-1, 101st Cong. (1989).

Crime Control and Law Enforcement Act of 1994.[57]

Offenses under the law largely reflect the same order and scheme established in the Convention. As codified, the law establishes jurisdiction over acts against ships in three cases: (1) where the vessel is subject to U.S. jurisdiction or the criminal is subject to U.S. jurisdiction as a national or resident of the U.S.; (2) where a U.S. national is seized, threatened, injured or killed; or (3) where the offender is "later found in the United States after such activity is committed."[58] These jurisdictional elements would permit U.S. prosecution in a case that involves a foreign flagged vessel in U.S. waters.[59] They would also establish jurisdiction over offenses committed on a foreign flagged vessel where the flag state waives jurisdiction over the case.[60] However jurisdiction is established, a case involving a cyber-related offense will generally require coordination with other countries because prosecutors and investigators need access to foreign located data as well as other evidence located abroad.[61]

Since the SUA Convention went into force in the U.S., it has been applied in the prosecution of approximately seven cases in the U.S. and at least twelve cases worldwide.[62] Five of the cases in the U.S. involved violent acts at sea off the coast of Somalia.[63] Two other U.S. cases applied SUA Convention crimes to generally violent maritime events.[64] The criminal motivations of thieves and kidnappers off the Somali coast are often referred to as piratical, but the specific facts of the cases show that the general crime of interfering with a vessel's navigation is aptly applied to certain circumstances that may

---

[57] *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, § 60019, 108 Stat 1796, 1975-79 (1994) (codified at 18 U.S.C.§ 2280).

[58] 18 U.S.C. § 2280(b).

[59] *See, e.g.,* United States v. Jho, 534 F.3d 398, 403 (5th Cir. 2008) (enforcing oil pollution laws against foreign flagged vessels for violations occurring in U.S. waters).

[60] *See* United States v. Bustos-Useche, 273 F.3d 622, 626 (5th Cir. 2001) (affirming U.S. jurisdiction over drug trafficking crimes where Panama consented to U.S. law enforcement over a Panamanian freight ship).

[61] *See* Johann-Christoph Woltang, *Cyber Warfare*, *in* MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW (online ed., 2021).

[62] *See* E-mail from Brian Wilson, Deputy Dir., U.S. Global Maritime Operational Threat Response Coordination Center, U.S. Dep't of Homeland Security to author (Feb. 3, 2020, 17:24 EST) (on file with author).

[63] *See* United States v. Shibin, 722 F.3d 233, 238 (4th Cir. 2013); United States v. Salad, 908 F. Supp. 2d 728, 729 (E.D. Va. 2012); Muse v. Daniels, 815 F.3d 265, 266 (7th Cir. 2016); United States v. Ali, 718 F.3d 929, 944 (D.C. Cir. 2013); United States v. Said, 3 F. Supp. 3d 515, 521 (E.D. Va. 2014) *rev'd on sentencing grounds,* 798 F.3d 182, 200 (4th Cir. 2015).

[64] *See* United States v. Shi, 525 F.3d 709, 719 (9th Cir. 2008) (involving murder on the high seas aboard foreign fishing vessel); United States v. Zaraboz, 378 Fed. Appx. 939, 940 (11th Cir. 2010).

not always constitute piracy.[65]

3. SUA and the Cyber Nexus

Spoofing incidents like the one that occurred in the Black Sea in 2017 are chargeable under legislation giving effect to the SUA Convention because spoofing constitutes serious interference with the operation of navigational facilities and the interference may be executed using communications known to be false which endanger the safe navigation of a ship.[66] Spoofing is a general term used to describe an electronic communication from an unknown source disguised as a known and trusted source.[67] The incidents that occurred in the Black Sea were a form of spoofing known as "GPS Spoofing," a term that refers to interference with global positioning satellite transmission signals, intending to project false location data.[68]

There is significant overlap between technology that interferes with communications in cyberspace and capabilities like GPS spoofing that interfere with communications via the electromagnetic spectrum.[69] Cyberattacks are defined, in part, as attacks conducted through cyberspace to disrupt, disable, destroy, or maliciously control a computing environment.[70] GPS Spoofing can be executed through the electromagnetic spectrum to disrupt and maliciously control shipboard computing environments that rely on navigation systems to function properly. GPS Spoofing can also be executed via cyberspace, but even when executed via the electromagnetic spectrum, it has an impact on operations in cyberspace.[71]

A spoofing attack is both a form of control over a ship by force and serious

---

[65] *See, e.g., Said*, 3 F. Supp. 3d at 521 (where defendants accused of piracy and unlawful acts of violence against a person on a vessel shot AK-47 assault rifle at vessel they presumably did not recognize as U.S. Navy warship). *See also* Brian Wilson, *The Turtle Bay Pivot: How the United Nations Security Council is Reshaping Naval Pursuit of Nuclear Proliferations, Rogue States, and Pirates*, 33 EMORY INT'L L. REV. 1, 63 (2018).

[66] SUA Convention, *supra* note 9, art. 3.

[67] *See What is Spoofing?*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/spoofing (last visited Aug. 14, 2021).

[68] Maria Korolov, *What is GPS Spoofing? And How You Can Defend Against It*, CSO (May 7, 2019), https://www.csoonline.com/article/3393462/what-is-gps-spoofing-and-how-you-can-defend-against-it.html.

[69] Catherine A. Theohary and John R. Hoehn, *Convergence of Cyberspace Operations and Electronic Warfare*, CONGRESSIONAL RESEARCH SERVICE (Aug. 13, 2019), https://fas.org/sgp/crs/natsec/IF11292.pdf.

[70] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY COMPUTER SECURITY RESOURCE CENTER, *Cyber Attack*, https://csrc.nist.gov/glossary/term/Cyber_Attack (last accessed Jun. 6, 2021).

[71] *See What is GPS Spoofing? And How You Can Defend Against It*, *supra* note 67 (cyberattacks against networked systems).

interference with the operation of a vessel endangering the safe navigation of the ship.[72] Electronic systems are now the primary means of navigation for mariners.[73] Using global positioning system (GPS) electronics, a properly equipped merchant ship should generally be able to plot a position on a chart within three to six feet of its actual position.[74] While the prudent mariner must regularly consult auxiliary navigation systems, the modern merchant ship incorporates GPS data into a myriad of computer systems that rely on accurate information to avoid chaos and ensure the orderly movement of a ship from port to port.[75] Merchant vessel automation connecting navigation systems to automatic steering and propulsion systems make it possible for a cyber-intruder to temporarily control a ship's movement.[76] Therefore, spoofing constitutes an exercise of control over the ship because manipulating the navigational equipment prospectively causes a vessel's course to be manipulated.

Even where spoofing is temporary and reversable, it seriously damages maritime navigational facilities and endangers a ship's safety. Minimal interference with navigational equipment can drastically change a ship's intended course, sending it toward danger.[77] Temporary interference with a ship's navigation can be a serious problem because larger ships have so much momentum that maneuvering back to the intended course or stopping can require miles of unobstructed waterway.[78] Therefore, where navigational interference is not refined or significant enough to purposefully control a ship, it nonetheless constitutes a violation of the SUA Convention because minimal interference with navigational equipment seriously interferes with a ship's operation.

Interference with land-based navigation systems may also, under certain circumstances, constitute a violation of the SUA Convention. The Convention and U.S. law provide that unlawful and intentional damage to maritime navigational facilities are criminal acts if the acts are likely to

---

[72] Andrej Androjna et al., *Assessing Cyber Challenges of Maritime Navigation*, J. MAR. SCI. & ENGINEERING, Oct. 2020, at 1, 8.

[73] NATHANIEL BOWDITCH, THE AMERICAN PRACTICAL NAVIGATOR: AN EPITOME OF NAVIGATION 1 (1995).

[74] WILLIAM J. HUGHES TECH. CTR. WAAS T&E TEAM, GLOBAL POSITIONING SYSTEM (GPS) STANDARD POSITIONING SERVICE (SPS) PERFORMANCE ANALYSIS REPORT SUBMITTED TO FEDERAL AVIATION ADMINISTRATION GPS PRODUCT TEAM 21 (2014), https://www.nstb.tc.faa.gov/REPORTS/PAN86_0714.pdf.

[75] BOWDITCH, *supra* note 73, at 1.

[76] Androjna, *supra* note 72, at 8.

[77] *See, e.g., id.*

[78] KNIGHT'S MODERN SEAMANSHIP 264 (John V. Noel et al. eds., 18th ed.1988).

endanger a ship's safe navigation.[79] The U.S. Coast Guard operates or partners with twelve vessel traffic services across the country which rely on radar detection, closed circuit television, and automated information systems to track vessels navigating U.S. coastal waterways.[80] Damage to any of those electronic devices could present a significant concern for vessels transiting the confined waterways where these traffic services exist. Very minimal interference would likely endanger the safe navigation of a ship, thus constituting a violation of the Convention and U.S. law.

4. The SUA Convention as a Model for International Coordination

There are several reasons why cybercrimes are challenging to prosecute, but one of the main reasons is that evidence is inevitably located abroad.[81] Additional coordination through international organizations would help parties prosecute cases using the SUA framework. That type of coordination is critical when addressing cybercrime, where evidence of offenses may exist in the country where the offense occurred, in the country (or countries) where a server is housed, and in the country where the impact is realized.[82]

In order to constitute a crime under the Convention, the violator's actions must be both intentional and unlawful.[83] In the context of a cybercrime, where offenses are often transnational, it may be challenging to prove the intent behind some foreign, land-based miscreant interfering with a GPS signal.[84] Even if a country impacted by the interference is able to obtain jurisdiction over the perpetrator, identifying the intent of his actions may require close coordination and evidence sharing with the country where the perpetrator committed his acts.

Understanding the motivation for cybercrimes is a key component to cybercrime investigations and prosecutions and, as exemplified by the

---

[79] 18 U.S.C. § 2280(a); SUA Convention, *supra* note 9, art. 3.

[80] *Vessel Traffic Services*, U.S. COAST GUARD NAVIGATION CTR. OF EXCELLENCE (NAVCEN), https://www.navcen.uscg.gov/?pageName=vtsMain (last visited Aug. 14, 2021).

[81] *See, e.g.,* United States v. Microsoft Corp., 138 S. Ct. 1186, 1187-88 (2018) (per curiam) (vacating and remanding as moot litigation over whether the U.S. Department of Justice can obtain data stored abroad after obtaining a warrant because the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was enacted while litigation was ongoing to amend the Stored Communications Act and ensure prosecutorial access to data located abroad).

[82] Marcus Rogers*, Forensic Evidence and Cybercrime*, *in* THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE 433, 434 (Thomas J. Holt & Adam M. Bossler eds., 2020).

[83] SUA Convention, *supra* note 9, art 3.

[84] On the difficulties of evidence coordination in transnational cases, see Kalen Fredette, *International Legislative Efforts to Combat Child Sex Tourism: Evaluating the Council of Europe Convention on Commercial Child Sexual Exploitation*, 32 B. C. INT'L & COMP. L. REV. 1, 24 (2009).

Achille Lauro case, intergovernmental coordination is key to identifying motives the global community finds criminally offensive. Cyber-threats to commercial shipping may be the result of acts by cyberterrorists, state-sponsored adversaries; industrial spies and organized crime groups; hacktivists; or hackers.[85] Member states may take distinct views on the criminality or severity of these motivations.[86] An organization that understands each state's nuanced views and approach to prosecuting cybercrime will be able to mediate concerns and coordinate between governments to see justice through in the most effective way possible. Such an organization should be established by expanding on the strong foundation established under the SUA Convention.

The SUA Convention requires parties to provide assistance to criminal proceedings, take measures to prevent offenses from occurring, and share relevant information with a country that establishes jurisdiction.[87] These requirements have the practical benefit of ensuring that a country with jurisdiction over a SUA offense will have resources at its disposal to effectively prosecute the case, but the provisions also create a mechanism for coordination that will develop mutual understanding of laws impacting transnational activity. A country with jurisdiction over a cybercrime impacting the maritime industry could leverage these provisions or similar provisions existing in the Budapest Convention.

B. The Budapest Convention

The Budapest Convention also creates a framework for taking enforcement measures against those who cause interference, but it addresses interference with computers, rather than with a ship's navigation system.[88] The Convention's provisions establish both specific obligations to make particular crimes prosecutable as well as procedural obligations to create a uniform system that ensures those prosecutions may be carried out in a judicially sound manner.[89] Chapter II, Section 1 of the Budapest Convention

---

[85] *Cyber Threat Source Descriptions,* CYBER INFRASTRUCTURE SEC. AGENCY (CISA), https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions#nat (last visited Aug. 14, 2021).

[86] For example, industrial espionage is criminalized in the United States but not in the United Kingdom. Joseph V. DeMarco, *Europe's Weaker Laws Against Trade Secret Theft Means Corporate Espionage Often Goes Unpunished*, BUSINESS INSIDER (Aug. 5, 2011, 4:54 PM), https://www.businessinsider.com/europes-lack-of-trade-secret-theft-protection-laws-means-coprorate-espionage-often-goes-unpunished-2011-8.

[87] SUA Convention, *supra* note 9, arts. 12-14.

[88] Budapest Convention, *supra* note 10, arts. 2-8.

[89] *See, e.g.,* SUA Convention, *supra* note 9, art. 9 (requiring parties to adopt measures to establish criminal offenses against child pornography thereby creating a specific criminal

identifies substantive criminal law agreed to by parties to the treaty while Chapter III creates a framework for international cooperation.[90] Substantive crimes addressed by the Convention are organized into five titles that establish a basis for criminal conduct constituting (1) violations against systems and data integrity;[91] (2) computer-specific crime related to fraud and forgery;[92] (3) content-related offenses such as a requirement to outlaw child sexual abuse material;[93] (4) intellectual property offenses;[94] and (5) ancillary offenses including aiding and abetting, corporate liability, and sanctions.[95] The offenses included in these titles mirror crimes enacted under the Computer Fraud and Abuse Act (CFAA), the bedrock statue for prosecuting computer crimes in the U.S.[96]

Like the SUA Convention, the Budapest Convention establishes criminality based on intent and unlawfulness, the prosecution of which requires evidence that must be obtained through close coordination with partnering countries.[97] The Convention has been adopted by sixty-five countries, recognized by several international organizations, and influenced several others.[98] While it is difficult to precisely identify every instance where a country implemented and exercised Budapest Convention provisions to prosecute a case, it has been recognized as the legal basis for extraditions both to and from the U.S.[99] That said, the Convention's influence has not

---

offense); *id.* art. 20 (establishing procedural obligations with regard to collecting data and records trafficked through a Party's territory).

[90] Budapest Convention, *supra* note 10, arts. 2-35.

[91] *Id.* art. 4.

[92] *Id*. arts. 7-8.

[93] *Id.* art. 9.

[94] *Id.* art. 10 (requiring parties to enact legislation or other measures criminalizing copyright and related rights).

[95] *Id.* art. 11.

[96] *See* AMERICAN BAR ASSOCIATION, #CYBERSPACEIRL: RULE OF LAW APPROACHES TO VIRTUAL THREATS (May 2019), https://www.americanbar.org/content/dam/aba/directories/roli/misc/aba-roli-cyberspace-irl-paper.pdf.

[97] *See* Budapest Convention, *supra* note 10, art. 6.

[98] *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/parties-observers (last visited Aug. 14, 2020). *See generally* Clough*, supra* note 43 (discussing the Budapest Convention's influence on non-party states).

[99] *See, e.g., In re* Matter of Extradition of Ricardo Alberto Martinelli Berrocal, No. 17-22197-Civ-TORRES, 2017 WL 3776953, *4-5 (S.D. Fla. Aug. 31, 2017) (ordering the extradition of Ricardo Martinelli Berrocal, former President of Panama, based in part, on violations of Panamanian law that support Panama's status as a party to the Budapest Convention). *See also* U.S. Dep't Just. Off. of Pub. Aff., *Nigerian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy*, Press Release 19-1366 (Dec. 9, 2019), https://www.justice.gov/opa/pr/nigerian-

harmonized cyberlaw globally, and cybercrime continues to flourish, in part, because governments fail to unify their enforcement efforts.

1. Prosecuting Under the Budapest Convention

In the context of a ransomware or malware attack on a shipping company, data interference or computer system interference would constitute a violation of the Budapest Convention.[100] Data is defined by the Budapest Convention as "facts, information, or concepts in a form suitable for processing in a computer system."[101] A computer system is a "device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data."[102] Under Article 4 of the Budapest Convention, parties are required to adopt legislation or other measures to establish a criminal offense for the intentional "damaging, deletion, deterioration, alteration or suppression of computer data . . . ."[103] Separately, seriously "hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data" must also constitute an offense under a party's laws."[104]

The Budapest Convention may apply to attacks on both operational technologies (OT) used in the maritime industry to monitor and control physical mechanisms like ruder control systems, and it may apply to informational technologies (IT) that manage data and communications.[105] Examples of IT systems shipping companies and their customers rely on include container tracking systems that ensure parties know where shipboard cargo is located[106] and systems that identify the effect that cargo might have on the ship's stability.[107] An attack against the computer system used to manage containers on a ship constitutes a violation of the Budapest Convention's terms when data in the system is impacted and when the system

citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business-email.

[100] *See* Budapest Convention, *supra* note 10, art. 4.

[101] *Id*. art. 1(b).

[102] *Id*. art. 1(a).

[103] *Id*. art. 4.

[104] *Id*. art. 5.

[105] The Guidelines on Cyber Security Onboard Ships, https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf.

[106] *Container Tracking*, TRACK-TRACE, https://www.track-trace.com/container (last visited Aug. 14, 2021).

[107] *Computerized Vessel Management Systems*, MAR. REP. & ENGINEERING NEWS, https://magazines.marinelink.com/Magazines/MaritimeReporter/198501/content/computerized-management-systems-203183 (last visited Aug. 14, 2021).

as a whole is affected.[108] Similarly, the same provisions make it unlawful to interfere with a vessel's navigational equipment.[109] Spoofing alters the computer data that would normally display the ship's correct position and therefore constitutes a violation of the Budapest Convention even when executed through the electromagnetic spectrum.[110] The Russian government was likely responsible for both the Black Sea spoofing attack and the Notpetya virus that shut down Maersk Shipping's networks.[111] However, both state sponsored and non-state sponsored cybercriminals have the capability to execute similar attacks.[112]

2. Coordination Under the Budapest Convention

Criminal acts identified under the Budapest Convention are an important aspect of countering cybercrime, but what may be more important are the coordination mechanisms established by the Convention. Cybercrimes are exceptionally difficult to investigate and prosecute, in part, because evidence is deleted, overwritten, and hard to access.[113] The Budapest Convention establishes many of the same evidence-sharing obligations adopted under the SUA Convention, but also creates obligations to ensure that parties can collect data that will help investigations and prosecutions before the data is lost.[114]

Russia is one of the countries bucking the trend of cybercrime coordination. Russia claims that the Budapest Convention would violate its sovereignty because the agreement provides mechanisms for parties to assist with official investigations and share information from concluded investigations.[115] In particular, Russia points to Article 20, which requires

---

[108] *See* Budapest Convention, *supra* note 10, art. 5.

[109] *See id.*

[110] *See id.*; Goward, *supra* note 7.

[111] *See* Goward, *supra* note 7; Greenberg, *supra* note 8. *See also* Press Release, Department of Justice, Remarks By Assistant Attorney General for National Security John C. Demers On Announcement of Charges Against Russian Military Intelligence Officers, Department of Justice Press Release, https://www.justice.gov/opa/speech/remarks-assistant-attorney-general-national-security-john-c-demers-announcement-charges (Oct. 19, 2020) (presenting charges against Russian military officers from Unit 74455 for conspiring to launch malware including NotPetya).

[112] *See* Public-Private Analytic Exchange Program, Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf (2019) (cyber-weapons and capabilities available to state and non-state actors).

[113] *See* Agnieszka McPeak, *Disappearing Data*, 2018 WIS. L. REV. 17, 60-61 (2018).

[114] *See* Budapest Convention, *supra* note 10, arts. 17-21; SUA Convention, *supra* note 9, art. 8.

[115] Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional*

parties to adopt measures necessary to empower competent authorities to "compel a service provider . . . to collect . . . traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer."[116] Article 32 allows parties to access open source data and access other stored data without authorization of the party hosting that data.[117] Russia drafted a counter-proposal to the Budapest Convention that gives governments priority over data within their borders and would limit information sharing between countries.[118]

Despite Russia's objections, the Budapest Convention is highly deferential to a party's sovereignty, developing mechanisms for assistance that are executed in concert with the domestic law of the requested State.[119] To the extent Russia has concerns that the obligations present an imposition on its sovereignty, it could join the sixty-five member states that submitted reservations and declarations.[120] Of course, a reservation or declaration cannot overcome the purpose of the treaty, but there does not appear to be any objection from Russia or other countries that runs against the Convention's stated purpose of fostering rapid and well-functioning cooperation to counter crime in the digital age.[121]

Like all conventions, the Budapest Convention's domestic implementation may result in disparate interpretations, but by joining the treaty, parties step closer to agreement on criminal enforcement. Just as the SUA Convention leaves room to implement laws that further define a country's understanding of what constitutes control of a ship, the Budapest Convention leaves room for parties to interpret the acts that constitute "*alteration*, *suppression*, or *hindering*" computer networks or systems, as those terms are used in the

---

Challenges, 43 YALE J. INT'L L. 191, 217 (2018).

[116] Budapest Convention, *supra* note 10, art. 20(b)(i).

[117] *Id*. art. 32.

[118] Press Release, The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, Draft United Nations Convention on Cooperation in Combating Information Crimes, https://www.rusemb.org.uk/fnapr/6394 (Feb. 20, 2018).

[119] *See, e.g.,* Budapest Convention, *supra* note 10, art. 25. *Compare* Clause 1 demanding mutual assistance only to the "widest extent possible," *and* Clause 4 providing that mutual assistance will be "subject to the conditions provided for by the law of the requested Party." *Id.*

[120] *See Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=wA2zL52h (last visited Aug. 14, 2021).

[121] *See* CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW 340 (6th ed. 2017) (discussing reservations in the context of the International Covenant on Civil and Political Rights (ICCPR) and international obligations to make reservations consistent with the "object and purpose" of the treaty).

Budapest Convention.[122] A common understanding of these terms would naturally draw the conclusion that the Budapest Convention prohibits interference with a network or system used to track containers.[123] Similarly, spoofing a ship's navigation display would violate a common understanding of these terms. Therefore, the SUA Convention and the Budapest Convention provide leeway where member states may differ on specific circumstances, but they also set a baseline for violations that cannot be overcome without violating the object and purpose of the treaties.

C. Comparing Criminal Conventions – the Budapest-SUA Framework

Both the SUA Convention and the Budapest Convention contain obligations critical to preventing, responding to, and prosecuting cybercrimes affecting the maritime industry. Both conventions envision extraterritorial application by member states, and both generally address criminal conduct committed under the subject matter of the conventions while also addressing specific criminal acts.[124] Most importantly though, they both identify specific obligations to coordinate with and assist prosecuting states.[125] The conventions are both designed for addressing cybercrime affecting the maritime industry, but the enforcement provisions have not done enough to address the maritime cybercrimes mentioned in the beginning of this paper. They also have yet to have a significant impact on cybercrime throughout the world. Obligations should be improved by establishing requirements for companies to report cyber-attacks and for parties to coordinate between governments in pursuing cybercrimes.

Cybercrime is committed without regard to national borders, sometimes by multiple actors.[126] Accordingly, perhaps more than any other type of crime, cybercrime requires coordination at all levels — from investigators through to the judiciary. In his book, "The Court and The World: American Law and the New Global Realities," Justice Breyer remarks on the similarities between problems faced in U.S. and foreign courts.[127] He finds that an exchange of ideas between American and foreign judges helps to reinforce the application of the Constitution in accordance with American

---

[122] *See* Budapest Convention, *supra* note 10, arts. 4-5 (emphasis added).

[123] *See id.*

[124] *See id.* art. 9.

[125] *See id.* art. 25.

[126] U. S. DEP'T OF JUSTICE OFFICE OF LEGAL EDU. (OLE), PROSECUTING COMPUTER CRIMES, 117-18, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[127] STEPHEN BREYER, THE COURT AND THE WORLD: AMERICAN LAW AND THE NEW GLOBAL REALITIES 351 (2015).

values.[128] There may be no better place to start with the exchange of those ideas than at the center of U.S. intercourse with other countries: global trade. For the reasons discussed, cyber-vulnerabilities in the maritime industry present the most threatening concerns for global trade and are therefore ripe for discussion between governments.

III. SHORING UP PROSECUTORIAL CAPABILITIES

Cybercrime is ubiquitous. Yet, for a host of reasons, law enforcement agencies worldwide fail to prosecute these cases.[129] The Budapest Convention and the SUA Convention address many of the primary concerns with prosecuting cybercrime cases in the maritime industry. Both conventions address jurisdictional problems, facilitate prosecutions with evidence-sharing requirements, and impose mutual assistance obligations.[130] What they lack are reporting requirements that allow law enforcement officials to be informed and coordinate as proficiently as the criminals they are pursuing.[131] While the conventions impose state obligations to share information, they do not transfer the reporting requirements to persons and entities under the state's jurisdiction.[132]

A typical company experiences 130 cybersecurity breaches each year.[133] Unfortunately, relatively few of these attacks are reported, and there is therefore little data for security experts to use in order to develop solutions to counter evolving threats.[134] Receiving reports from companies impacted by cyberattacks and investigating them to the fullest extent possible opens the door to understanding the latest cybercrime tradecraft so that criminal cases may be pursued.

---

[128] *Id*.

[129] Roger A. Grimes, *Why It's So Hard to Prosecute Cyber Criminals: The Bad Guys Are Wreaking Havoc. Why Can't They Be Brought to Justice?*, CSO ONLINE (Dec. 6, 2016, 3:00 AM), https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html.

[130] *See* Budapest Convention, *supra* note 10, arts. 22-25; SUA Convention, *supra* note 9, art. 6-7, 10, 12.

[131] *See generally* Jerry Mickles, Dark Web: Problems Law Enforcement Investigations Face on the Dark Web (2016) (Ph.D. Dissertation, U. of Ariz.) (on file with ProQuest) (describing the different layers of information available to predators depending on where they search in the Deep Web).

[132] *See generally* Budapest Convention, *supra* note 10; SUA Convention, *supra* note 9.

[133] THE WHITE HOUSE, COUNCIL OF ECONOMIC ADVISERS, *The Cost of Malicious Cyber Activity to the U.S. Economy* 6 (Feb. 2018), available at https://www.hsdl.org/?view&did=808776.

[134] *Id*. at 30-32.

A. Vessel Reporting Requirements – A Model for Implementing Cybercrime Coordination

The U.S. currently has mechanisms in place to require cyberattack reporting. Those mechanisms should be reinforced to specifically apply to cyber incidents and they should be reinforced with international coordination through buy-in from trade partners. Vessels arriving in U.S. ports are required to notify the U.S. Coast Guard of any hazardous condition that "may adversely affect the safety of [the vessel]."[135] In December 2016, the U.S. Coast Guard issued a policy notice advising vessel operators that reporting requirements include physical breaches, cyber-related breaches, and suspicious activity.[136] These reporting requirements parse the line between common-occurrence phishing or spam attempts (which need not be reported) and those network incursions that pose a serious concern for vessel safety.[137]

The SUA Convention should have a protocol that imposes similar obligations to report security breaches and suspicious activity. The protocol would establish uniform definitions and a standard that applies to private operators worldwide. Armed with that information, nation-states where ships are registered, and states where these ships load and unload their cargoes, will share evidence with other parties and be prepared to engage in coordinated pursuit of criminal actors. Given the prevalence of cyber-related crimes, a central database should be created for countries that are parties to the SUA Convention. That database may be used to share cyber threat information and identify commonalities between cyber intrusions. With such a system in place, governments and law enforcement specialists will be better equipped to identify and deter cybercrimes throughout the maritime industry and beyond.

Assuming that reporting requirements and coordination reap positive results in the maritime industry, there is good reason to think that trade partners in other sectors will recognize the benefits of harmonizing cybercrime laws. As a result, similar reporting and coordination requirements could be adopted as a protocol to the Budapest Convention, extending the same counter cybercrime benefits across all transnational trade industries.

B. Overcoming Challenges to Developing Coordination Responsibilities

For a host of reasons, private companies have been reluctant to report cyber-attacks. Some are pessimistic, thinking that reporting is unlikely to

---

[135] 46 U.S.C. § 2306 (as implemented through 33 C.F.R. pt. 160 and 33 C.F.R. § 101.305 requiring notification of security incidents and breaches of security).

[136] Policy Letter from P.F. Thomas, Rear Admiral, U.S. Coast Guard, to Distribution, U.S. Coast Guard (Dec. 14, 2016).

[137] *Id.*

result in perpetrators being apprehended; some companies think that reporting will expose vulnerabilities; some view reporting and investigations as a constraint on corporate resources; and some companies simply do not trust the government with information that may be required to adequately investigate such attacks.[138] Such views to resist singular, coordinated government action, only expose these companies to inevitable harm.[139] They are symptomatic of an overly confident defensive system that is bound to fail with a single point of weakness. Despite developing efforts to prevent and overcome cyber vulnerabilities, a Department of Homeland Security (DHS) report found that cyber-attacks against critical infrastructure increased 383% in a single year.[140] What will put these companies and the global economy on offense is a proactive front against the perpetrators of cybercrime. Consistently, the vast majority of cyber-attacks are executed for criminal purposes.[141] Accordingly, the current state of affairs is unsustainable. More must be done to prevent and deter cyber-attacks that can have a devastating effect on the economy. Companies resist coordination against cyber-enemies at their own peril and the peril of society's dependence on the timely and reliable shipment of goods. To prevent future attacks and damage to global economies, maritime transportation companies, more than any other sector of the economy, must lend a hand by reporting attempts to invade their cyber-systems and networks.

C. A Proposal to Retake the Reins of Economic Security

Commentators have suggested requiring cybercrime reports from companies.[142] However, those proposals suggest mandatory reporting for all sectors and companies, which is an overwhelming task to consider.[143] A mandate that spans all companies and sectors would yield a massive amount of data, all of which must be stored and analyzed. Mandated worldwide cyberattack reporting and coordination directly aimed at the maritime industry, will gain more traction than proposals that address the issue for all

---

[138] Dan Swinhoe, *Why Businesses Don't Report Cybercrimes to Law Enforcement*, CSO (May 30, 2019, 3:00 AM), https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

[139] *See id.*

[140] Christian Pedersen, *Much Ado about Cyber-Space: Cyber-Terrorism and the Reformation of the Cyber-Security*, 7 PEPPERDINE POL'Y REV. 1, 19 (May 1, 2014).

[141] Paolo Passeri, *February 2020 Cyber Attacks Statistics*, HACKMAGEDDON (Mar. 19, 2020), https://www.hackmageddon.com/2020/03/19/february-2020-cyber-attacks-statistics/.

[142] Don Jergler, *Why Mandating Cyber Reporting, Basic Coverage Makes Sense: Cyence Exec*, INSURANCE JOURNAL (Oct. 9, 2017), https://www.insurancejournal.com/news/national/2017/10/09/466070.htm.

[143] *See id.*

transnational companies because the mandate is specific and tailored. By segmenting the problem and presenting a test case in one of the most vulnerable sectors, universal efforts to counter cybercrime through reporting and coordination will be more successful.

A protocol to the SUA Convention will highlight the pragmatism and utility in advancing greater prosecutorial efforts to combat cybercriminals. By implementing the appended proposal, parties and corporations within their jurisdiction will be able to judge the effectiveness of a more aggressive regime. The proposal adopts two key aspects of U.S. law: (1) required reporting and (2) coordinated responses. It advances those characteristics on a global scale so that prosecutorial efforts can dexterously engage cybercriminals in their own realms across the globe.

As discussed, ships arriving in U.S. ports are required to report cyber-attacks that may seriously impact the vessel or its cargo.[144] However, the vast majority of these ships are registered in foreign countries that the ships rarely (if ever) visit.[145] Therefore, opportunities for the country responsible for the ship to oversee and reinforce compliance with reporting requirements are limited.[146]

1. The Challenges of Shipping Regulation

Commercial ships are regulated by organizations known as "registries," which are established by countries to identify a vessel's nationality and the regulations it is subject to under that country's jurisdiction.[147] Each registry is represented by a flag that denotes the "flag state" or ship nationality.[148] Registries (or flag states) are responsible for ensuring that ships are manned, equipped, documented, and operated in accordance with internationally accepted regulations.[149] Despite attempts to create a uniform system of maritime regulation,[150] the shipping industry is known for reducing operating

---

[144] 46 U.S.C. § 2306 (2020).

[145] *See* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT HANDBOOK OF STATISTICS: BUILDING, OWNERSHIP, REGISTRATION AND RECYCLING OF SHIPS 76, 79 (2020) (citing UNCTAD Stat (UNCTAD, 2020a)).

[146] *The State of the U.S. Flag Maritime Industry*: *Hearing before the Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, U.S. House of Representatives* (Jan. 17, 2018) (Statement of Mark H. Buzby, Maritime Administrator).

[147] UNCLOS, *supra* note 32, arts. 91, 92.

[148] *See id.* art. 91(1) (providing that "[s]hips have the nationality of the State whose flag they are entitled to fly. There must be a genuine link between the State and the ship." By flying the flag of the State where the vessel is registered, vessels advertise their flag state).

[149] *See id.* art. 94 (prescribing the duties of flag states).

[150] *See* R.R. CHURCHILL & A.V. LOWE, THE LAW OF THE SEA 265 (3d ed. 1999).

costs by flagging commercial ships under registries that demand lower fees and impose less stringent regulation and oversight.[151] The options for minimizing costs are so obvious that over forty percent of the world's shipping is conducted under the regulation of three registries.[152] Those registries have limited resources to oversee the fourteen thousand plus vessels they are responsible for, but their oversight efforts may be supported by the port states where ships visit to load and offload cargo.[153] When a ship enters a foreign country, that country may refer matters to the flag state and require the ship to remedy nonconformance with safety regulations.[154]

Cyber threats like the virus that ravaged Maersk and other companies must be identified and addressed by flag states and port states because those viruses present threats that expand beyond the maritime domain, impacting interconnected transportation systems.[155] An amendment to the SUA Convention presents an opportunity for port states and flag states to prosecute cybercrimes. The U.S.'s method of implementing SUA Convention discussed in Section II.A.2 above, provides a good example of how trans-jurisdictional offenses can be effectively prosecuted by the country with the greatest interest in the crime. By broadly establishing jurisdiction over persons "found in the United States" who have committed a cybercrime impacting the maritime industry, an international agreement would put offenders on notice that their crimes will not go unpunished.[156] Similarly, an instrument that enables experts to identify trends and evolving vulnerabilities early on, will help secure an industry that is critical to global economies.

The legality of action taken against noncompliant ships will be supported by flag states, those countries where ships are registered, enforcing reporting requirements as a consequence of their treaty obligations. If, due to limited resources, the flag state is unable to support a shipping company's reporting requirements, port states (countries where the ship loads and unloads cargo) can facilitate reporting or enforcement.[157] As long as the flag state is a party to the protocol, enforcement expectations will not be offensive to the flag

---

[151] *Id*. at 258.

[152] *Shipping and the World Trade: The World's Major Shipping Flags*, INT'L CHAMBER OF SHIPPING, https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-the-worlds-major-shipping-flags/ (last visited Aug. 14, 2021).

[153] *See* UNCLOS*, supra* note 32, art. 218 (providing rules of enforcement by port states).

[154] *See* YOSHIFUMI TANAKA, THE INTERNATIONAL LAW OF THE SEA 355 (3d ed. 2019) (remarking on a port State's ability to take enforcement action even where a violation is committed on the high seas based on treaties agreed to by the port state and the flag state).

[155] *See* Greenberg, *supra* note 8.

[156] 18 U.S.C. § 2280(b)(1)(C).

[157] *See* Arron N. Honnibal, *The Exclusive Jurisdiction of Flag States: A Limitation on Pro-Active Port States?*, 31 INT'L J. MARINE & COASTAL L. 499, 529-30 (2016).

state's sovereignty.

2. An International Coordination Model

In addition to cyberattack reporting requirements, the U.S. also has a well-established system for coordinating cyber-crime analysis and countermeasures. The U.S. Coast Guard receives reports of cyber-attacks affecting ships arriving in U.S. ports, but another DHS agency, the Cybersecurity and Infrastructure Security Agency (CISA), coordinates the U.S. response to cyber-related vulnerabilities affecting critical infrastructure across the country.[158] Cyber-attacks reported to CISA are received by the National Risk Management Center (NRMC) which will plan, analyze, and collaborate to address significant risks to U.S. critical infrastructure.[159] NMRC executes its mission without disclosing proprietary information or imposing additional risks on the companies that report attacks.[160] The varying implications of and reporting requirements for a cyber attack on specific industries must be assessed through the expertise of Sector Risk Management Agencies.[161]

When implemented by states unilaterally, even the most effective cybercrime enforcement laws are limited in their ability to overcome the transglobal problem of cybercrime. A global center with a mission similar to the NRMC would have the benefit of seeing and understanding threats that are bound for U.S. borders. The establishment of such a center would also recognize the borderless threat presented by malicious cyber actors.

Several entities currently attempt to support cybercrime enforcement measures by coordinating transnationally. For instance, the International Criminal Police Organization (INTERPOL) does much of the same work NMRC does on an international level.[162] With the advantage of mandatory

---

[158] *About CISA,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about-cisa (last visited Aug. 14, 2021).

[159] *Id*.

[160] *National Risk Management Center*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/national-risk-management (last visited Aug. 14, 2021).

[161] *Sector Risk Management Agencies*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sector-risk-management-agencies. (last visited Aug. 14, 2021). The Transportation System Sector is one of the Sector Risk Management Agencies and it is co-managed by the Transportation Security Administration and the United States Coast Guard, giving cognizance to the Coast Guard for the maritime component of the transportation sector. *See* Transportation Systems Sector-Specific Plan 2015, Department of Homeland Security and Department of Transportation, https://www.cisa.gov/publication/nipp-ssp-transportation-systems-2015.

[162] *Cybercrime*, INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime (last visited Aug. 14, 2021).

reporting from shipping companies worldwide, a coordination center could analyze potential threats and align investigatory efforts while simultaneously responding to the threat with recommendations to companies on how they may manage risk. In sum, a protocol that establishes an international coordination center to receive, analyze, and act upon cyber-threats in the maritime industry, serves as a prophylactic against vulnerabilities that present a grave concern for global markets while also serving as a model for corporations world-wide to join in the effort to coordinate an offensive against cybercriminals.

IV. IMPLEMENTING A GLOBAL INITIATIVE

The SUA Convention was proposed and adopted through the International Maritime Organization (IMO),[163] a United Nations specialized agency with expertise in maritime safety and regulation.[164] The U.S. and 173 other Member States are represented at the IMO.[165] One hundred fifty six IMO members, including the landlocked countries of Slovakia, Switzerland, and Mongolia, are parties to the SUA Convention.[166] Yet, with this strong consortium supporting its mandate, the IMO's contributions to cybersecurity have been limited to issuing guidance, referring members to trade organizations, and encouraging risk management assessments.[167]

A SUA Convention protocol relating to mandatory reporting and coordination requirements for cyberattacks would be negotiated through a resolution proposed to the Maritime Safety Committee (MSC), one of the five IMO committees.[168] Domestically, the Secretary of State would authorize U.S. representatives to propose, negotiate, sign, and enter the protocol into force.[169] That process would require a robust analysis of

---

[163] SUA Convention, *supra* note 9.

[164] *Introduction to IMO*, INT'L MAR. ORG., www.imo.org/en/About/Pages/Default.aspx (last visited Aug. 14, 2021).

[165] *Member States, IGOs, and NGOs*, INT'L MAR. ORG., www.imo.org/en/About/Membership/Pages/Default.aspx (last visited Aug. 14, 2021).

[166] *Status of Conventions: Ratifications by State*, INT'L MAR. ORG., https://www.imo.org/en/About/Conventions/Pages/StatusOfConventions.aspx (last updated May 18, 2021).

[167] *Maritime Cyber Risk*, INT'L MAR. ORG., https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (last visited Aug. 14, 2021) (providing links to IMO issued guidance, guidance issued by interest groups, and MSC Resolution 428(98), advising that after January 1, 2021, flag state administrations "should" take cyber risk management into account when conducting annual verifications of a company's Document of Compliance).

[168] *Structure of IMO*, INT'L MAR. ORG., www.imo.org/en/About/Pages/Structure.aspx (last visited Aug. 14, 2021).

[169] CONG. RESEARCH SERV., S. PRT. 106-71, TREATIES AND OTHER INT'L AGREEMENTS: THE ROLE OF THE UNITED STATES SENATE (2001).

Constitutional authority to obligate the U.S. to the terms of the agreement.

A. Constitutional Authority for the Protocol

Of the 4,500 or so words in the U.S. Constitution, only eighteen of them, addressing Congress's authority to "define and punish Piracies and Felonies committed on the high seas, and Offenses against the Law of Nations," are expressly devoted to the government's authority to prosecute crimes committed outside U.S. borders.[170] Congress more frequently relies on its foreign commerce authority to criminalize extraterritorial misdeeds.[171] Foreign commerce is increasingly invoked as the constitutional basis for congressional authority; so much so that it is often considered broader than domestic commerce authority.[172] Foreign commerce and constitutional authority to regulate merchant shipping are so integral to federal control that state efforts to regulate in the field are generally preempted.[173]

In the wake of atrocities that took place on the *Achille Lauro*, the U.S. identified federal authority to adopt and implement the SUA Convention as well as a protocol that made the agreement's provisions applicable to fixed platforms on the continental shelf.[174] While the SUA Convention was drafted to address the specific problem of criminalizing terrorism aboard ships, it also addressed the broader problem of intentional, criminal acts interfering with a ship's navigation.[175] Accordingly, a protocol that requires reporting and coordinating responses to cyber-attacks would not be offensive to the spirit of the original convention.

In the U.S., domestic instruments are in place to implement the terms of the appended draft protocol requiring parties to mandate reporting and

---

[170] U.S. CONST. art. I, § 8, cl. 10.

[171] *See, e.g.,* United States v. Baston, 818 F.3d 651, 668 (9th Cir. 2016), *cert. denied*, 137 S. Ct. 850 (2017) (holding that extraterritorial jurisdiction exists under the Foreign Commerce Clause where the perpetrator engaged in transnational sex trafficking).

[172] *See* United States v. Park, 938 F.3d 354, 371 (D.C. Cir. 2019) (where the Court relied on "evidence that the Founders intended the scope of the foreign commerce power to be [] greater' than its interstate counterpart" (citing Japan Line, Ltd. v. Cty. of L.A., 441 U.S. 434, 448, n.13 (1979)).

[173] Craig H. Allen, *Federalism in the Era of International Standards: Federal and State Government Regulation of Merchant Vessels in the United States (Part 1*), 29 J. MAR. L. & COM. 335, 368-69 (1998).

[174] *See* Review of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988, and its Protocol, 2002 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 3, § B(1)(e) at 104-10; U.S. DEP'T OF STATE, MULTILATERAL TREATIES IN FORCE AS OF JANUARY 1, 2020, https://www.state.gov/wp-content/uploads/2020/08/TIF-2020-Full-website-view.pdf (last updated Jan. 1, 2020).

[175] *See* SUA Convention, *supra* note 9, preamble, art. 3.

coordinate such reporting through a single agency.[176] The proposed draft protocol would standardize reporting requirements across the maritime industry and establish mechanisms for reporting to an international agency. Given that most ships arriving in the U.S. are registered in foreign countries, such a requirement would have little impact on U.S. companies.[177] Therefore, from the U.S.'s perspective, implementing the protocol would strengthen existing requirements to report hazardous conditions and clarify that those hazardous conditions include cyber incidents impacting ships.[178] As a party to the Budapest Convention, the U.S. also enacted measures authorizing it to share reports of data interference and system interference with parties.[179] Accordingly, neither the corporate reporting requirement nor the multilateral report sharing aspect of the protocol would offend existing authorities under the laws of the U.S.

B. U.S. Courts and a Coordinated Prosecution

One of the chief benefits of a protocol that creates a global cybercrime reporting and coordination body is that it can assist with preventing conflict between sovereigns working to prosecute cybercrimes. The concept of universal jurisdiction establishes that some offenses are so hard to reach and so heinous that jurisdiction exists in any state regardless of the victim's nationality, the perpetrator's nationality, the perpetrator's residence, or whether the prosecuting country was affected by the act.[180] If any crimes fall within universal jurisdiction, cybercrimes are certainly among them because cybercrime transcends national boundaries and damages economies on a global scale.[181] However, one of the problems with universal jurisdiction is that it may create confusion if more than one state initiates an investigation or criminal proceedings over the same criminal for the same act.[182] A global

---

[176] *See* Status of the U.S.-Flagged Vessels in U.S.-Foreign Trade: Hearing Before the Subcomm. on Coast Guard and Mar. Transp. of the H.R. Comm. on Transp. and Infrastructure, 111st Cong. 7 (2010) (statement of David Matsuda, Mar. Administrator., Dep't of Transp.) (testifying that U.S.-flag ships now carry less than two percent of the nation's international trade).

[177] *See* 46 U.S.C. § 2306.

[178] *See id.*

[179] *See, e.g.,* Budapest Convention, *supra* note 10, art. 23.

[180] DAVID J. LUBAN ET AL., INTERNATIONAL AND TRANSNATIONAL CRIMINAL LAW 175, 177 (3d ed. 2019).

[181] *See* Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 695 (2007).

[182] Scholars have also criticized universal jurisdiction on the more fundamental basis that historical examples of universal jurisdiction actually have a jurisdictional link. *See generally* Matthew Garrod, *Unraveling the Confused Relationship Between Treaty Obligations to*

cybercrime coordination body will mitigate the problem of jurisdictional overlap and confusion cursing universal jurisdiction. By assessing facts in light of the law of the territories impacted, laws in the offender's nation state, laws of country where individuals were impacted, a coordination body will identify the state with adequate evidence, legal structures, and state interest in prosecuting the case.[183] With that type of analysis in hand, a coordination body can advance its case while simultaneously taking into consideration equities other jurisdictions want addressed.

The question still remains though – if the U.S. has a jurisdictional link to a cybercrime that victimizes a merchant ship, how will domestic courts treat evidence coordinated by an international entity? In any case where spoofing like that occurring in the Black Sea is attributed to a person "later found in the United States,"[184] the U.S. could leverage the SUA Convention to prosecute the case. Even if the culprit is extradited or subject to extraordinary rendition, U.S. law authorizes prosecution.[185] If successful in obtaining custody of the culprit, U.S. officials would then be charged with obtaining evidence to prosecute the case. The evidence needed for such a prosecution could be located all over the world.[186] Rules of evidence authorize letters rogatory "to an international tribunal, officer or agency . . . ."[187] However, the process of obtaining evidence through letters rogatory is known for substantial delays incurred through the process of coordinating between

---

Extradite or Prosecute and "Universal Jurisdiction" in Light of the Habrè Case, 59 HARV. INT'L L. J. 125 (2018) (arguing that treaty-based jurisdiction creates extraterritorial investigation and prosecution power, whereas universal jurisdiction is an impractical concept).

[183] *See* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 402.1 (AM. LAW INST. 2018) (reflecting the five core jurisdictional principles in international law: territoriality, nationality, passive personality, protectivity, and universality).

[184] 18 U.S.C.§ 2280(b)(1)(C).

[185] *Id. See* United States v. Shi, 525 F.3d 709, 723 (9th Cir. 2008) (holding that the Maritime Safety Conventions implemented by 18 U.S.C. § 2880 expressly bestows the prosecution power over foreign offenders to all signatory states).

[186] *See* Beverly Ford, *Cybercrime's Worldwide Scope*, 4 QNLNCCT 10 (Nov. 2008).

> If a local prosecutor wants to obtain Internet records pertaining to the use of a particular IP number on a particular date and time in Brussels, Belgium, that local prosecutor most probably will be making a request to the Office of International Affairs and Department of Justice. That office will then engage the procedures of the Mutual Legal Assistance Treaty between the United States and Belgium in order to ascertain what may be done and in what time frame.

Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 384 (2002).

[187] 28 U.S.C. § 1781(b)(2).

governments.[188] A global cybercrime coordination agency could serve as both the coordinator for purposes of information and for evidence used in U.S. courts. In that capacity, the coordination center would be familiar with chain of custody and similar requirements, ensuring that the case can be successfully prosecuted wherever the criminal is indicted.

C. Overcoming Problems Abroad

Cybercrime experts complain that transglobal cybercrime is not being effectively prosecuted because cybercrime laws are not in harmony, even for countries that adopted the Budapest Convention.[189] In fact, instead of promoting coordinated responses to the global issue of cybercrime, many states like Russia and China insist that information relevant to a cybercrime prosecution should remain with the individual sovereign states where the evidence resides.[190] Fortunately, the global community is striking back by declaring it an international norm for States to cooperate and assist with cybercrime prosecutions.[191] These declarations warn that isolationist behavior increases the risk of "escalation and retaliation in cyberspace."[192] Those are the very issues that could lead to cyber-attacks on global shipping and subsequent devastation to global economies.

The Council of Europe's Global Action on Cybercrime Extended (GLACY+) is one initiative that seeks to harmonize cybercrime legislation.[193] Its experience in coalescing best practices, investigation policies, and spearheading initiatives to implement cybercrime legislation along with INTERPOL should be built upon by a United Nations agency that will collect cyberattack reports, analyze evolving cyberthreat trends, and coordinate prosecutions globally. A global coordination agency with the benefit of worldwide reporting, coupled with the capabilities that GLACY+

---

[188] *See, e.g.,* E. Charles Routh, *Dispute Resolution – Representing the Foreign Client in Arbitration and Litigation*, *in* FUND. INT. BUS. TRANS. 1, 7 (2008).

[189] Alison Peters, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, THIRD WAY (May 27, 2020), https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.

[190] Shanghai Cooperation Org., *Agreement Between the Government of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security* 206 (June 16, 2009), http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf.

[191] *See* The Grp. of Seven, *G7 Declaration on Responsible States Behavior in Cyberspace* 1 (Apr. 11, 2017), https://www.mofa.go.jp/files/000246367.pdf (declaring that norm-abiding states will engage in cooperative approaches to fight cybercrime).

[192] *Id*.

[193] *Global Action on Cybercrime Extended (GLACY)+*, COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/glacyplus (last visited Aug. 14, 2021).

shares, would build upon the multilateral assistance treaty (MLAT) concept used by the U.S. to coordinate evidence sharing between states effectively and efficiently.[194] That type of efficiency is especially important in the context of cybercrimes where evidence is often fleeting and difficult to trace. Though many nation states may object to these initiatives, global acceptance will inevitably lead to noncooperative states being isolated, consequently narrowing the number of cybercriminal safe havens and restricting cybercriminals' ability to operate freely around the world.

The reporting requirements and coordination established by this protocol should be flexible enough so that, if successful, they can be adopted for broader impact through amendments to the Budapest Convention. A similar protocol to the Budapest Convention would establish reporting and coordinating through a singular international agency. With that type of coordination in place, transglobal companies can much more effectively counter cybercrime.

CONCLUSION

A cyber-attack on the maritime industry could cause more severe harm than an attack on any other sector of commercial trade. Cyberattacks impact shipping companies, the hundreds of interested parties with cargo on board their ships, thousands of downstream businesses, and millions of consumers world-wide. Domestic and global reliance on maritime transportation could be crippled by attacks on a company's networks or attacks on the ships themselves.

To date, the most common reaction to cyber threats has been a call for awareness, increased information security practices, and other defensive measures. Yet, the threat persists and grows without a corresponding counterreaction. While defensive measures are moderately effective in preventing the most basic attacks, they are not able to defeat motivated criminals looking to take advantage of vulnerabilities in international law and cyber law.

Coordinated Government efforts to gather evidence and investigate cybercrime have a positive track record. INTERPOL, Europol, and Eurojust, have worked together to assist with cybercrime prosecutions in more than forty countries.[195] These organizations have also made significant advances

---

[194] *See* COUNCIL OF EUR., C-PROC ACTIVITY REPORT FOR THE PERIOD OCTOBER 2016 – SEPTEMBER 2017, SG/Inf(2017)42, at 12, http://rm.coe.int/090000168076bd28; Allison Peters & Anisha Hindocha, *US Global Cybercrime Cooperation: A Brief Explainer*, THIRD WAY (Jun. 26, 2020), https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer.

[195] Maria Korolov, *Global Cybercrime Prosecution a Patchwork of Alliances*, CSO (Mar. 1, 2017, 3:00 AM), https://www.csoonline.com/article/3174439/global-cybercrime-

in sharing information between trade partners. Accordingly, they understand the laws that may be applied to effect cybercrime prosecutions. This paper recommends that member states should adopt the attached reporting and coordination protocol to the SUA Convention as a measure to enhance current efforts and aggressively pursue cyberthreats.

The SUA Convention was created to attack the novel threat of the day – terrorism aboard ships. Today, it should be developed by addressing the threats of tomorrow – cyber threats that have the potential to cripple global economies. By creating a protocol that both mandates cyber-attack reporting and establishes a coordination center to address these threats, the SUA Convention's legacy of protecting shipping interests globally will live on. It will also serve as an example of global coordination that will be beneficial to all transnational organizations.

If a SUA Convention protocol to mandate corporate reporting and data coordination is adopted and implemented, the prosecutions achieved through its global coordination mechanisms will inspire transnational trading partners outside the maritime industry to adopt a coordination and reporting protocol. They could do so by implementing a protocol much like the one appended, only tailored to the Budapest Convention rather than the SUA Convention.

---

prosecution-a-patchwork-of-alliances.html.

PROPOSED PROTOCOL

Protocol To The Convention
(The Reporting and Coordination Protocol)

PREAMBLE

THE STATES PARTIES to this Protocol,

BEING PARTIES to the Suppression of Unlawful Acts Against the Safety of Maritime Navigation Convention (SUA Convention),

ACKNOWLEDGING that cybercrime presents a ubiquitous threat to global trade and the worldwide economy,

CONSCIOUS of obligations to share information pursuant to Articles 8, 12, and 14 of the SUA Convention and 25-35 of the Budapest Convention,

CONSIDERING the importance of the International Convention for the Safety of Life at Sea and the International Port Facility Security (ISPS) Code,

CONSIDERING FURTHER resolutions 68/552 and 68/247 on the implementation of recommendations to proactively implement cybersecurity measures,

BELIEVING that it is necessary to adopt provisions supplementary to those of the Convention to suppress additional terrorist acts of violence against the safety and security of international maritime navigation and to improve its effectiveness,

HAVE AGREED as follows:

ARTICLE 1

For the purposes of this Protocol:
(1) "Suspicious Activity" means an observed behavior indicating a threat to vessel operations, its personnel, or its cargo; executed through telecommunications equipment, computer systems, or networks.

(2) "Breach of Security" means unauthorized access to telecommunications equipment, computer and networked systems, unauthorized root or administrator access to security and industry control systems, successful phishing attempts, or malicious insider activity that could

allow outside entities access to internal information technology systems linked to vessel navigation or affiliated with cargo. Instances of viruses, Trojan Horses, worms, zombies, or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers. Any denial-of-service attacks that adversely affect or degrade access to critical services that are linked to security plan functions.

(3) "International Commercial Sea Trade" means commercial trade by a company primarily engaged in business that requires goods or merchandise to be imported or exported to or from another country using commercial vessels.

ARTICLE 2

(1) Parties to this Protocol will establish an International Cybercrime Coordination Office (ICCO) responsible for receiving cyber incident reports including reports of suspicious activity and breaches of security; coordinating information and evidence sharing between governments; and pursuing harmonization of cybercrime law for the international maritime industry.

(2) The ICCO will establish a secure database containing reports of cyber-attacks affecting international commercial sea trade.

(3) The ICCO will establish a coordination office cognizant of State Party laws and agreements between States to facilitate the prosecution of transnational cybercrimes impacting the maritime industry.

ARTICLE 3

(1) Each Party shall adopt legislative and other measures as may be necessary to establish reporting requirements for any business within its jurisdiction engaged in international commercial sea trade. Parties will establish procedures necessary for businesses to report suspicious activity or breaches of security to its competent authority.

(2) Competent authorities will report suspicious activity, breaches of security, and investigation reports to the International Cybercrime Coordination Office (ICCO).

ARTICLE 4

(1) States Parties will investigate reports of suspicious activity or breaches of security to the degree necessary to ensure the safety of ships engaged in

international voyages or seek assistance necessary to conduct such investigations.

(2) States Parties unable to conduct an investigation or needing technical or other assistance will coordinate with the ICCO and other states as necessary to identify and counter cyberthreats impacting maritime transportation.

(3) Information obtained as a result of an investigation will be promptly shared with States Parties and coordinated through the ICCO to identify findings and recommendations that may be used to prosecute those responsible for interfering with computers, networks, or telecommunications systems or aiding in such impacts that disrupt international commercial sea trade.