INTERNATIONAL LAW STUDIES
Published Since 1895

Malware, a Device Under the 1988 SUA Convention

Michael Petta

100 INT'L L. STUD. 110 (2023)

Volume 100

2023

Published by the Stockton Center for International Law

ISSN 2375-2831

Malware, a Device Under the 1988 SUA Convention

Michael Petta[*]

CONTENTS

* Retired U.S. Coast Guard Commander and judge advocate; former Deputy Chair of the Stockton Center for International Law.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, the U.S. Coast Guard, or the U.S. Naval War College.

I. INTRODUCTION

In 1988, the International Maritime Organization (IMO)[1] modernized international law in response to a vexing problem of the time—maritime terrorism. Before then, because not all crimes against vessels amounted to piracy under international law, many violent acts at sea were beyond the reach of piracy's universal jurisdiction, leaving too much potential for maritime criminals to escape justice. To close this gap and facilitate international prosecutions of those who illicitly endanger navigation, IMO member States enacted the 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (1988 SUA Convention).[2]

More than three decades later, the 1988 SUA Convention still retains practical value and may be useful to address a more modern problem—cyberattacks against commercial vessels. The 1988 treaty prohibits various acts against shipping, including the placement of a *device* on a ship when likely to cause damage that could endanger the ship's navigation. Exploring whether this specific prohibition extends into the digital domain is this article's focus.[3]

It begins by underscoring the cyber threat that endangers maritime shipping today. It then highlights a broader threat, maritime terrorism, that troubled the international community in the 1980s and explores how the IMO's 1988 SUA Convention sought to address that problem. Returning to modern day, the article looks at the existing international regulatory framework meant to mitigate cyber threats and examines whether State parties of SUA may prosecute, via domestic legislation enacted pursuant to the 1988 treaty,

1. Originally named the International Maritime Consultative Organization, the body was renamed in 1982. *See* IMO, *Brief History of the IMO*, https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx (last visited Mar. 3, 2023).

2. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, T.I.A.S. No. 95-306, 1678 U.N.T.S. 221 [hereinafter 1988 SUA Convention].

3. Some use the term "SUA" as shorthand for the 1988 SUA Convention and its three subsidiary protocols: the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, T.I.A.S. No. 95-306, 1678 U.N.T.S. 304, Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Oct. 14, 2005, and Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, Oct. 14, 2005. While these three protocols are critical in the fight against maritime crime, they are beyond the focus of this article. This article's sole focus is the set of offenses enumerated in the 1988 treaty, which remains in place today.

maritime malware[4] cases that happen to breach the international regulatory framework. Finally, the article concludes that malware qualifies as a device under the treaty and advocates for the 166 State parties to incorporate SUA prosecutions into their maritime cyberattack response plans.

II. CYBER THREATS AGAINST THE MARITIME TRANSPORTATION SYSTEM

Cyber threats against the maritime transportation system (MTS)[5] are well-known. Since at least 2011, the European Union has considered cyber threats to be a rising menace in the maritime sector.[6] In 2013, the President of the United States pronounced cyber threats to be one of the most serious security challenges for critical infrastructure, including the MTS.[7] Two years later, the U.S. Coast Guard warned the public of "real and growing" cyber threats in the maritime industry.[8] In 2017, the IMO followed suit in guidelines addressing maritime cyber risks, urging the international community to "take

4. The term "malware" is an amalgam of the words "malicious" and "software." Malware is a purpose-made software used to illicitly access and adversely impact computer systems. The dictionary defines malware as "software that is intended to damage or disable computers and computer systems." *Malware*, NEW OXFORD AMERICAN DICTIONARY (3d ed. 2010). *See also* National Institute of Standards and Technology, Computer Security Resource Center, Glossary, *Malware*, https://csrc.nist.gov/glossary/term/malware (last visited Mar. 3, 2023); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 566 (Michael N. Schmitt gen. ed., 2017); RAEF MEEUWISSE, THE CYBERSECURITY TO ENGLISH DICTIONARY (4th ed. 2018).

5. The maritime transportation system (MTS) is "a network of maritime operations that interface with shoreside operations at intermodal connections as part of overall global supply chains or domestic commercial operations. The various maritime operations within the MTS operating network have components that include vessels, port facilities, waterways and waterway infrastructure, intermodal connections, and users." U.S. Dep't of Homeland Security, *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security* (Oct. 2005), https://www.dhs.gov/sites/default/files/publications/HSPD_MTSS Plan_0.pdf.

6. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR (Nov. 2011), https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/.

7. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013). The United States considers there to be sixteen different sectors that make up the nation's system of critical infrastructure. The transportation systems sector is but one of those sixteen and the MTS is a component of the transportation sector. *See generally* Cybersecurity & Infrastructure Security Agency, *Transportation Systems Sector*, https://www.cisa.gov/transportation-systems-sector (last visited Mar. 3, 2023).

8. U.S. Coast Guard, *Cyber Strategy* (June 2015).

the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization."[9]

The vulnerabilities related to digitization deserve emphasis. In business and industry, computers have historically been used as part of information technology systems, particularly those that manage data and information, such as word processing and emails. Technological advancements have led to computers now being an integral part of operational technology systems, those used for monitoring and controlling physical devices and industrial processes, such as the position of a lever or the starting of an engine.[10] The prevalence of operational technology systems on commercial vessels, along with the increased access that comes from greater reliance on the internet, makes commercial vessels particularly vulnerable to cyberattacks. A digital disruption to a vessel's navigational, engineering, or operational controls could "impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment and impede the ship's operation."[11] The accelerated digitization of the MTS, triggered in part by the coronavirus pandemic, only compounds this vulnerability.[12]

The threat is as real as the vulnerabilities. Just days after the IMO's 2017 resolution, Maersk, the global shipping giant, suffered a major cyberattack, leading its chairman to admit the maritime industry had been naive about cyber threats.[13] Certainly, the 2019 malware attack on a deep-draft commercial vessel bound for the Port of New York and New Jersey[14] proves the cacophony of warnings is more than theoretical. The one-thousand-foot ship was hit by a particularly destructive type of malware known as Emotet.[15] This

9. Int'l Maritime Org. [IMO], MSC-FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*, annex ¶ 1.2 (July 5, 2017).

10. THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS VERSION 4, at 5–6, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (last visited Mar. 3, 2023).

11. *Id.* at 8–9.

12. IMO, *Coronavirus (COVID-19)—Accelerating Digitalization of Maritime Trade and Logistics—A Call to Action*, Circ. Letter No. 4204/Add.20 (June 5, 2020).

13. 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.

14. James Rundle, *U.S. Coast Guard Warns Shipping Industry on Cybersecurity*, WALL STREET JOURNAL (July 11, 2019), https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402.

15. James Rundle, *Coast Guard Details February Cyberattack on Ship*, WALL STREET JOURNAL (July 26, 2019), https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401.

type of malware rapidly spreads across a network and sets itself as a gateway for other malware to infiltrate further and infect the system. Emotet allows perpetrators to remotely and synchronously control infected computers across a network.[16] It has been considered "one of the top cyber threats in the world."[17] Needless to say, port authorities feared the harm Emotet could cause the vessel's operational technology systems and what it could mean for the navigable channels if that deep-draft vessel lost control in one of the busiest and most economically significant ports in the United States.[18] Fortunately, although the malware degraded information technology systems, the vessel's operational technology systems were spared.[19]

This 2019 malware attack on a large commercial vessel was not an isolated incident. To the contrary, just months after the attack, the U.S. Coast Guard published Marine Safety Information Bulletin 04-19, entitled *Cyber Adversaries Targeting Commercial Vessels*, to warn the maritime industry of other actual malware intrusion attempts against commercial vessels and of malicious software being specially designed to disrupt shipboard systems.[20] In 2022, maritime stakeholders worldwide continued the drumbeat, reporting to the IMO that "[b]etween February and May of 2020 alone, the maritime industry overall suffered a fourfold increase in cyberattacks and [by 2020] those attacks against operational technology (OT) systems specifically increased by 900% since 2017."[21] This is to say, cyber threats against the MTS

16. Cybersecurity and Infrastructure Security Agency, Alert TA18-201A, *Emotet Malware* (last revised Jan. 23, 2020), https://www.cisa.gov/uscert/ncas/alerts/TA18-201A; Europol, *World's Most Dangerous Malware EMOTET Disrupted Through Global Action* (Jan. 27, 2021), https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action; Press Release, U.S. Dep't of Justice, *Emotet Botnet Disrupted in International Cyber Operation* (Jan. 28, 2021), https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

17. U.S. Dep't of Justice, *supra* note 16 (quoting FBI Special Agent Robert R. Wells).

18. Rundle, *Coast Guard Details February Cyberattack on Ship*, *supra* note 15.

19. U.S. Coast Guard, Marine Safety Alert 06-19, *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels* (July 8, 2019), https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf.

20. U.S. Coast Guard, Maritime Safety Information Bulletin 04-19, *Cyber Adversaries Targeting Commercial Vessels* (May 24, 2019), https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf.

21. IMO, *IAPH Cybersecurity Guidelines for Ports and Port Facilities*, Doc. FAL 46/23/2 (Mar. 1, 2022) (International Association of Ports and Harbors (IAPH) presentation to the IMO Facilitation Committee of IAPH's finalized first edition of its cybersecurity guidelines for ports and port facilities).

have long been and continue to be a "vexing and growing problem"[22] in the maritime community.

III. CRIMES AGAINST COMMERCIAL NAVIGATION: THE *ACHILLE LAURO* CASE

Naturally, the maritime community has faced and overcome other difficult problems. Looking back a few decades we see that terrorist acts against vessels once perplexed States. This is because, as will be detailed below, the law of the sea failed to provide the international community with a reliable and homogenous framework for exercising criminal jurisdiction over non-piratical acts against vessels.

A. International Criminal Jurisdiction

Generally, international law recognizes five theories under which a nation may exercise criminal jurisdiction over an offender: territoriality, nationality, passive personality, the protective principle, and universality.[23] Jurisdiction based on territoriality covers acts that take place in a nation's territory, including its territorial sea.[24] A State's nationality jurisdiction, sometimes referred to as personal jurisdiction, covers offenses committed by nationals of that State, even when outside the State's territory.[25] The passive personality theory bases jurisdiction on the nationality of the victim.[26] Meanwhile, the protective principle, known by some as target State jurisdiction, provides jurisdiction over offenses committed outside the State by individuals who are not nationals of the State, but which have effects against the national security

22. Atlantic Council, Webinar: *Security at the Maritime Edge*, Remarks by Rear Admiral Mark H. Buzby, U.S. Navy (Ret.), Administrator of the U.S. Maritime Administration, YOUTUBE (Sept. 24, 2020), https://www.youtube.com/watch?v=nqFsOZs3QQ0 (comments at minute 7:25).

23. Rivard v. U.S., 375 F.2d 882, 885 (5th Cir. 1967); U.S. v. Ali, 885 F. Supp. 2d 17, 25 (2012); Malvina Halberstam, *Terrorism on the High Seas: The Achille Lauro, Piracy and the IMO Convention on Maritime Safety*, 82 AMERICAN JOURNAL OF INTERNATIONAL LAW 269, 296–300 (1988) (discussing jurisdictional disagreements over the draft convention).

24. David Freestone, *The 1988 International Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 3 INTERNATIONAL JOURNAL OF ESTUARINE & COASTAL LAW 305, 309–11 (1988) (discussing jurisdictional obligations of contracting parties to the 1988 SUA Convention).

25. *Id.*

26. *Id.*

or governmental functions of the State (such as espionage or counterfeiting).[27]

Universal jurisdiction, meanwhile, grants prosecutorial power to all nations, even when a State has no nexus, territorially or otherwise, to the offense.[28] An act of piracy, unique to the maritime domain, is the quintessential example of an offense subject to universal jurisdiction.[29] Generally, under the law of the sea, an act of piracy requires the illicit act to launch from a private ship for private ends against another ship on the high seas.[30] As will be shown below in the discussion of *Achille Lauro*, piracy law's nuances are a key reason international prosecution of maritime terrorists proved troublesome.[31]

Alongside these five jurisdictional theories sits another jurisdictional concept unique to the maritime domain—flag State jurisdiction. Some characterize flag State jurisdiction as an extension of territoriality, while others view it as its own, sui generis, independent jurisdictional basis.[32] Regardless of any such debate, flag State jurisdiction is a bedrock precept in the law of the sea[33] because it grants each nation jurisdiction over crimes taking place

---

27. *See* Halberstam, *supra* note 23, at 296–99 (discussing the protective principle and referring to the State whose conduct a terrorist seeks to affect as the target State); *see also* AMERICAN LAW INSTITUTE, 1 RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES 240 (1986).

28. Halberstam, *supra* note 23, at 299.

29. *Id.*

30. United Nations Convention on the Law of the Sea art. 101(a)(i), Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]; *See* Felicity Attard, *IMO's Contribution to International Law Regulating Maritime Security*, 45 JOURNAL OF MARITIME LAW AND COMMERCE 479, 501 (2014) (discussing "private ends" and "two ships" elements of piracy).

31. Attard, *supra* note 30, at 502; *see* Helmut Tuerk, *Combating Terrorism at Sea—The Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 15 UNIVERSITY OF MIAMI INTERNATIONAL AND COMPARATIVE LAW REVIEW 337, 345 (2008) (discussing the UN Secretary General's conclusion that the "two-vessel requirement" and "private ends" criterion make piracy law generally inapplicable to acts of maritime terrorism); *see also* Halberstam, *supra* note 23, at 276–91 (discussing considerable differences among scholars as to whether politically motivated acts constitute piracy and concluding such acts should be viewed as beyond piracy's reach).

32. *See* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 408 cmt. b & reporters' note 3, § 432 reporters' note 4 (2018); *see also* 1 RESTATEMENT (THIRD) of the FOREIGN RELATIONS LAW OF THE UNITED STATES, *supra* note 27, § 402 cmt. h, § 502 reporters' note 3.

33. Tullio Treves, *The Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 2 SINGAPORE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 541, 542 (1998); Freestone, *supra* note 24, at 307.

on ships flying its flag regardless of the location of the vessel.[34] If the offense takes place on a vessel in another State's territorial sea or coastal waters, criminal jurisdiction, generally speaking, runs concurrently between the flag and coastal States.[35] On the high seas, meanwhile, jurisdiction over offenses is left exclusively in the hands of the flag State.[36]

B. The Achille Lauro Hijacking

Tragedy often magnifies gaps in the law. Such is the case with the hijacking of an Italian-flagged cruise ship, *Achille Lauro*. The 1985 hijacking underscored how the law's theories on international criminal jurisdiction left potential for acts of maritime terrorism to escape justice.

On October 3, 1985, *Achille Lauro* departed Genoa, Italy for an eleven-day cruise in the Mediterranean Sea.[37] The ship, with about seven hundred and fifty passengers, planned port calls across Italy, Egypt, and Israel.[38] A small cruise ship by today's standards, *Achille Lauro* followed minimal security practices; at most, passport checks.[39] People and parcels were not searched for weapons.[40] Consequently, four Palestinian radicals easily disguised themselves as tourists and mixed with legitimate passengers to board and depart with the vessel in Genoa.[41]

Four days after they boarded, the four men, armed with machine guns and hand grenades, seized control of the vessel and threatened death to the passengers should Israel not release fifty Palestinian prisoners.[42] Tragically, they followed through with their threat and killed a U.S. passenger, Leon Klinghoffer.[43] A day after the murder, the four radicals turned themselves

---

34. UNCLOS, *supra* note 30, art. 92; Convention on the High Seas art. 6, Apr. 29, 1958, 13 U.S.T. 2312, T.I.A.S. No. 5200, 450 U.N.T.S. 11.

35. RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, *supra* note 32, § 502 cmt. d.

36. UNCLOS, *supra* note 30, art. 92; Convention on the High Seas, *supra* note 34, art. 6.

37. MICHAEL K. BOHN, THE ACHILLE LAURO HIJACKING: LESSONS IN THE POLITICS AND PREJUDICE OF TERRORISM 2–4 (2004).

38. *Id.*

39. *Id.*

40. *Id.*

41. William E. Smith, *Terrorism: The Voyage of the Achille Lauro*, TIME (Oct. 21, 1985), http://content.time.com/time/subscriber/article/0,33009,960163,00.html.

42. *Id.*

43. BOHN, *supra* note 37.

over to Egyptian authorities near Port Said, putting an end to the violent hijacking.[44]

Once the radicals turned themselves over to Egyptian authorities, governmental entities began jockeying for position over the fate of the terrorists.[45] The five primary political bodies involved were: Italy, the flag State; Egypt, the coastal State where the crimes occurred and with physical custody of the hijackers; Israel, the target State (i.e., the nation the hijackers sought to coerce); the United States, the murder victim's home country; and the Palestine Liberation Organization, the political body with a patrimonial interest over the offenders.[46] These entities held dissimilar views and competing interests over custody, jurisdiction, extradition, and prosecution of the hijackers.[47] For instance, Egypt initially refused Italy's and the United States' extradition requests. This disagreement intensified to the point that an Egyptian airliner carrying the hijackers and their mastermind was forced by U.S. fighter jets to land in Sicily, where it was surrounded by United States' special forces, who were themselves surrounded by about three hundred Italian law enforcement officers.[48] Fortunately, cooler heads prevailed and Egypt surrendered the hijackers, but not the mastermind, to Italy.[49] The hijackers were eventually tried and convicted in Italy.[50]

Apprehending and prosecuting the alleged mastermind, Abu El-Abas,[51] proved equally volatile. Despite the United States' extradition requests, Italy[52] allowed El-Abas to flee into Yugoslavia.[53] The United States then requested the extradition of El-Abas from Yugoslavia, but Yugoslavian authorities refused. In 1986, Italy convicted him in absentia while he remained at large.[54]

---

44. *Id.* at 15.

45. *Id.* at 20–21.

46. *Id.*

47. Attard, *supra* note 30, at 503.

48. *Id.*; BOHN, *supra* note 37, at 31–33.

49. BOHN, *supra* note 37, at 20–21.

50. *Id.* at 93, 96.

51. Sources refer to Abu El-Abas by various names, such as Mohammed Abbas, Abu Abbas, and Abu Khaled. He is referred herein as Abu El-Abas, consistent with how he was named in the 1985 United States' arrest warrant. *See id.* at xv, 12–13.

52. During the hijacking, El-Abas stayed ashore but later accompanied the hijackers on the Egyptian airliner. Like them, he was handed over to Italian authorities in Sicily. *Id.* at 43.

53. Jordan J. Paust, *Extradition and United States Prosecution of the Achille Lauro Hostage-Takers: Navigating the Hazards,* 20 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 235, 236 (1987).

54. *Id.*

The *Achille Lauro* affair underscored a problem with seeking justice in maritime terrorism cases—and maritime crimes in general: not all illicit acts against vessels at sea amount to piracy under international law.[55] Subversive actors do not necessarily need another ship to launch a strike. They may, as happened to *Achille Lauro*, board in port and consummate the attack from within the vessel itself. Likewise, illicit actors, such as the radicals who killed Leon Klinghoffer, may be driven by political motives, not private gain. Although various countries had legitimate bases for criminal jurisdiction over the Palestinian radicals, none could faithfully rely on piracy law's robust universal jurisdiction to secure criminal accountability.[56] Because terrorism was viewed as a global scourge of the time,[57] this lack of reliable criminal accountability across the globe left too much potential for maritime terrorists to escape justice, a problem the international community sought to remedy.

IV. THE 1988 CONVENTION FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE SAFETY OF MARITIME NAVIGATION

Well before Italy convicted the hijackers, the international community at-large took steps to address the jurisdictional issues brought to light by the *Achille Lauro* hijacking.[58] Specifically, just two months after the hijackers gave themselves up to Egyptian authorities, the United Nations General Assembly asked the IMO "to study the problem of terrorism aboard or against

55. Attard, *supra* note 30, at 502; *see* Tuerk, *supra* note 31, at 345 (discussing the UN Secretary General's conclusion that the "two-vessel requirement" and "private ends" criteria make piracy law generally inapplicable to acts of maritime terrorism); *see also* Halberstam, *supra* note 23, at 276–91 (discussing considerable differences among scholars as to whether politically motivated acts constitute piracy and concluding such acts should be viewed as beyond piracy's reach).

56. On October 12, 1985, the United States filed a piracy charge against the hijackers, but scholars consider that charge to be invalid. *See* Paust, *supra* note 53, at 255 (pointing to general concurrence that the United States' piracy charge was per se invalid); *see* Attard, *supra* note 30, at 502 (stating that the United States wrongly charged the hijackers with piracy on the high seas).

57. *See generally* H.R. Con. Res. 228, 99th Cong. (1985), *reprinted in Documents Concerning the Achille Lauro Affair and Cooperation in Combatting International Terrorism*, 24 INTERNATIONAL LEGAL MATERIALS 1509, 1562–63 (1985) (in which Congress catalogs the vast number and tragic impacts of terrorist acts over the ten preceding years).

58. *See* Attard, *supra* note 30, at 504–5 (discussing the SUA Convention's genesis as an instrument meant to address the jurisdictional vulnerabilities associated with piracy law under the Law of the Sea).

ships with a view to making recommendations on appropriate measures."[59] The IMO, in turn, formed a committee to consider certain draft measures submitted by Italy, Egypt, and Austria.[60] These draft measures evolved into the 1988 SUA Convention, adopted at a conference in Rome in March of that year.[61]

A. The 1988 SUA Convention's Pedigree

The adoption of the 1988 SUA Convention was significant because the convention was the first instrument to make subversive acts against ships, particularly non-piratical acts that endangered navigation, internationally prosecutable.[62] Generally, the 1988 SUA Convention achieves this by enumerating various criminal offenses against shipping, distributing jurisdiction over those offenses among all State parties, promoting cooperation in preventing such offenses, and then obligating parties to apprehend, extradite, and prosecute offenders.[63] According to the treaty's preamble, IMO member States took this pioneering step in part because "unlawful acts against the safety of maritime navigation jeopardize the safety of persons and property, seriously affect the operation of maritime services, and undermine the confidence of the peoples of the world in the safety of maritime navigation."[64] At present, 166 States are party to the treaty.[65]

Although the 1988 SUA Convention was a first in the maritime context, it was not without forebearers. Rather, the convention was modeled on a family of treaties designed to thwart terrorist acts. This group included the 1963 Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft, the 1971 Montreal Convention for the Suppres-

59. G.A. Res. 40/61, ¶ 13 (Dec. 9, 1985).

60. Halberstam, *supra* note 23, at 270.

61. Glen Plant, *The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, 39 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 27, 28 (1990); Tuerk, *supra* note 31, at 343–45.

62. Plant, *supra* note 61, at 29; Tuerk, *supra* note 31, at 343–45.

63. Rosalie Balkin, *The International Maritime Organization and Maritime Security,* 30 TULANE MARITIME LAW JOURNAL 1, 7–8 (2006).

64. 1988 SUA Convention, *supra* note 2.

65. IMO, STATUS OF IMO TREATIES 444 (Sept. 29, 2021), https://wwwcdn.imo.org/localresources/en/About/Conventions/StatusOfConventions/Status%20-%202021.pdf.

sion of Unlawful Acts Against the Safety of Civil Aviation, the 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons Including Diplomatic Agents, and the 1979 International Convention Against the Taking of Hostages.[66] Evolving as a response to international terrorism, this family of treaties is sometimes referred to as "anti-terrorist" conventions[67] or "counter terrorist" conventions.[68]

Not only do these treaties share a similar genesis—acts of terrorism—they also share a fundamental trait meant to deter such acts—they employ the *aut deder aut judicare* principle.[69] Specifically, to "ensure that [those who commit covered offenses] will not find safe haven, at least not in the territory of those States that are parties to the Convention,"[70] this group of treaties contains prosecute or extradite stipulations designed to leave "no hiding-place" for fugitives.[71] Because of this shared trait, in addition to their anti-terrorism moniker, the 1988 SUA Convention's pedigree is also known as the "extradite or prosecute" conventions.[72]

B. The 1988 SUA Convention's Enumerated Offenses

As mentioned earlier, the 1988 Convention expressly criminalizes various acts against shipping. Specifically, Article 3 of the treaty prohibits unlawful and intentional control or seizure of a vessel by force, threat, or intimidation.[73] It also prohibits a set of unlawful and intentional acts when likely to *endanger the safe navigation of a ship*. This set of "endanger navigation" offenses includes violence against people on board; destruction or damage to the vessel or its cargo; *placement of a destructive or damaging device* or substance; destruction or serious damage to navigation facilities; and communication of false

66. Attard, *supra* note 30, at 506–7; Tuerk, *supra* note 31, at 343; *see* Terry Richard Kane, *Prosecuting International Terrorists in United States Courts: Gaining the Jurisdictional Threshold*, 12 YALE JOURNAL OF INTERNATIONAL LAW 294, 300–7 (1987) (inventorying multilateral counterterrorist conventions).

67. Halberstam, *supra* note 23, at 292.

68. Freestone, *supra* note 24, at 306.

69. Attard, *supra* note 30, at 507.

70. Balkin, *supra* note 63, at 8.

71. Freestone, *supra* note 24, at 306.

72. Plant, *supra* note 61, at 28.

73. 1988 SUA Convention, *supra* note 2, art. 3.

information.[74] Finally, Article 3 criminalizes the injuring or killing of any person in connection with any of the previously enumerated offenses.[75]

Under the law of the sea, for an illicit act against a vessel to become a piratical act, the target vessel must be on the high seas at the time of the offense.[76] The 1988 SUA Convention's enumerated offenses are not so geographically limited. Rather, Article 4 of the treaty provides that an illicit act against a ship may become a SUA offense "in all possible areas of the sea: the high seas, the exclusive economic zone, the territorial sea, and even internal waters."[77] As long as the target vessel's voyage has a planned or consummated international element, the ship's location at the time of the attack is not dispositive as to the applicability of Article 3's offenses.[78]

To make SUA's enumerated offenses enforceable among its 166 State parties, Article 5 of the Convention requires them to incorporate Article 3's offenses into their domestic law. The United States, for example, codified the 1988 SUA offenses in 18 U.S.C. § 2280, entitled Violence Against Maritime Navigation.[79] The offenses in U.S. domestic law are nearly identical to those in Article 3.[80] Again, it is the specific prohibition against *placing a destructive or damaging device on a ship*, as written in paragraph 1(d) of Article 3 in the 1988 treaty and section (a)(1)(D) of 18 U.S.C. § 2280, upon which this article focuses.

C. The 1988 SUA Convention's Jurisdictional Suite

Aside from its enumerated offenses, the 1988 SUA Convention's true advance in prosecuting maritime crimes derives from its fusion of the aforesaid theories of international criminal jurisdiction. The Convention ultimately codifies these various theories into seven different bases for exercising jurisdiction over maritime offenses.[81] In sum, Article 6 of the treaty grants[82] jurisdiction to a State when the offense occurs against or on board a ship flying

74. *Id.*
75. *Id.*
76. UNCLOS, *supra* note 30, art. 101(a)(i).
77. Treves, *supra* note 33, at 546.
78. *Id.*
79. 18 U.S.C. § 2280(a)(1) (2015).
80. *Id.*
81. 1988 SUA Convention, *supra* note 2, art. 6.
82. As noted by various scholars, while the treaty grants jurisdiction under seven theories, it breaks those bases into two camps: obligatory in the case of territorial, national, mere

its flag (flag State); in a State's territory or territorial sea (territoriality); by a national of that State (nationality); by a stateless person who routinely resides in that State (quasi-nationality); against a national of that State (passive personality); to coerce the State (protective principle); and when an offender is later present in its territory.[83]

Importantly, the last basis listed above, presence in a State's territory, which hints at universal jurisdiction by treaty in the sense that it provides signatories jurisdiction over an offender even when a State has no other nexus to the crime.[84] Meaning, even if a contracting party has no claim to jurisdiction under the flag of the vessel, territoriality, nationality, passive personality, or the protective principle, that State still gains jurisdiction once an offender enters its territory.[85] Mere presence[86] in the territory, in and of itself, is enough.[87] In United States' domestic law, interestingly, it does not matter how the offender arrives in the United States' territory.[88]

Like piracy law's brand of jurisdiction, the 1988 SUA Convention's jurisdictional suite reaches far across the international community. Unlike piracy law, however, the 1988 SUA Convention is agnostic about an attacker's motivations, launch point, and target location.[89] The 1988 treaty's jurisdictional reach extends across all areas of the sea and applies equally to pirates, common criminals, terrorists, and State sponsored actors alike,[90] regardless from where they mount their attack. This is all to say, for those party to the

---

presence, and flag State jurisdiction; and discretionary in the case of quasi-national, passive personality, and protective principle jurisdiction. Treves, *supra* note 33, at 550; Tuerk, *supra* note 31, at 351.

83. 1988 SUA Convention, *supra* note 2, art. 6; Treves, *supra* note 33, at 550.

84. *See* Freestone, *supra* note 24, at 310 (characterizing the universality principle as being based on simple custody of the offender).

85. Treves, *supra* note 33, at 550–51.

86. The United States' jurisdiction is based on mere presence but differs slightly from the 1988 SUA Convention. Article 6 of the convention bases such jurisdiction on when an offender "is present" in a territory. Meanwhile, the United States hinges this jurisdiction on when an offender is "later found" in its territory. *Compare* 1988 SUA Convention, *supra* note 2, art. 6 *with* 18 U.S.C. § 2280(b)(1)(c).

87. Treves, *supra* note 33, at 550–51.

88. U.S. v. Shi, 396 F. Supp. 2d 1132, 1136 (2003).

89. *See* Treves, *supra* note 33, at 542–45 (characterizing the 1988 SUA Convention as an instrument meant to apply to common crimes at sea that do not fit into piracy's "very narrow" definition).

90. *See* Plant, *supra* note 61, at 33 (discussing how drafters of the 1988 SUA Convention viewed Article 3's term "any person" as applying to any person, even State sponsored actors).

treaty, jurisdiction over the convention's enumerated offenses is as robust, if not more so, than jurisdiction under piracy law.

D. Custody, Extradition, and Prosecution Under the 1988 SUA Convention

As a complement to its robust jurisdictional suite, the 1988 SUA Convention also provides robust authorities for apprehending and prosecuting maritime criminals. For instance, when an alleged offender is present in a State's territory Article 7 empowers and requires that State party, when circumstances warrant, to take the offender into custody or to ensure the offender's presence at judicial proceedings.[91] Meanwhile, Article 10 empowers and requires a State party, if it does not submit the respective case for prosecution under its domestic law, to extradite any alleged offender present in its territory.[92] When States have an existing extradition treaty, the 1988 SUA Convention's Article 3 offenses are considered extraditable offenses under the treaty.[93] When no extradition treaty exists between nations, the 1988 SUA Convention represents, in and of itself, a legal basis for extradition.[94]

Having recounted the IMO's SUA-response to maritime terrorism in the 1980s, we can return to the present and see if this decades-old treaty has a place when it comes to the current cyber problem across the MTS.

V. THE INTERNATIONAL MARITIME ORGANIZATION'S REGULATORY FRAMEWORK FOR MITIGATING CYBER THREATS

In the recent past the international community has taken steps to address the threat of cyberattacks against the MTS. Naturally, the ideal way to protect targets from any attack, cyber or kinetic, is to prevent the attack from ever reaching its destination. As of today, consequently, the global community chiefly employs prophylactic, regulatory-styled guidelines to harden ships' computer systems and mitigate the likelihood of a cyber strike. Like the 1988 SUA Convention, these guidelines fall under the purview of the IMO.

In 1948, via the Geneva Conventions, member States of the United Nations created the IMO to foster international cooperation, promote vessel

91. 1988 SUA Convention, *supra* note 2, art. 7.1.
92. *Id.* art. 10.1.
93. *Id.* art. 11.1.
94. *Id.* art. 11.2.

safety and efficiency standards, and maximize worldwide availability of "international shipping services to the commerce of the world."[95] Consisting of 174 member States, the IMO continues this mission today as the global legislative body for regulating safe, secure, and sustainable shipping worldwide.

Few legal instruments embody the IMO's purview over commercial shipping[96] greater than the International Convention for the Safety of Life at Sea (SOLAS).[97] Adopted partly in response to the infamous sinking of RMS *Titanic*, SOLAS sets "minimum standards for the construction, equipment and operation of ships, compatible with their safety."[98] Fundamentally, SOLAS regulates the behavior of ship owners, masters, and crews to ensure vessels are fit for international voyages and protected from at-sea calamities.

SOLAS's protective benefits are not limited to safeguarding vessels from marine accidents. IMO member States have also drawn from SOLAS guidelines meant to guard against cyber-attacks. These guidelines reside in two chapters of SOLAS—Chapter IX, Management for the Safe Operations of Ships, and Chapter XI-2, Special Measures to Enhance Maritime Security. These two SOLAS chapters embody what are commonly known as the International Safety Management Code and the International Ship and Port Facility Security Code, respectively.[99]

Adopted in response to a 1987 ferry accident in Belgium, the International Safety Management Code sought to clean up a sloppy safety culture in the shipping industry.[100] Meanwhile, following the 9/11 terrorist attacks, the International Ship and Port Facility Security Code hardened physical security

---

95. Convention on the Intergovernmental Maritime Consultative Organization, Mar. 6, 1948, 9 U.S.T. 621, T.I.A.S. No. 4044, 289 U.N.T.S. 3 (the organization's name was later simplified to the International Maritime Organization).

96. At the time of this writing, 166 countries, representing about 99 percent of the world's shipping tonnage, are parties to SOLAS and its preventative regime.

97. After its initial adoption in 1914, SOLAS evolved via various conventions. As the last such convention was adopted in 1974, the treaty is commonly referred to as SOLAS 1974. This article uses the terms SOLAS and SOLAS 1974 synonymously.

98. International Convention for the Safety of Life at Sea, 1974, Nov. 1, 1974, 32 U.S.T. 47, 1184 U.N.T.S. 277 (as amended).

99. *See* IMO, Doc. Res. MSC 428(98), *Maritime Cyber Risk Management in Safety Management Systems* (June 16, 2017), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (affirming that safety management system enacting under SOLAS's ISM Code should take into account cyber risk management); *see also* IMO, Doc. MSC 102/9, *Measures to Enhance Maritime Security* (Mar. 10, 2020) (recognizing that security measures implemented via SOLAS's ISPS Code should protect against terrorism and other illicit acts, such as cyber-attacks).

100. IMO, ISM CODE, at v. (2018 ed.).

across the MTS by requiring ships and servicing facilities to implement preventive security measures.[101] Despite different origins and themes (i.e., safety versus security), the two codes share a central trait—each is a risk-assessment regime designed to mitigate dangers to international shipping.

Under the International Safety Management Code ship owners and operators must safeguard against *all* identified risks, even the cybersecurity variety.[102] Similarly, the International Ship and Port Facility Security Code encourages ship owners to assess and mitigate any security vulnerabilities, including those in the cyber domain.[103] Risk assessments under both codes must be routine and documented.[104] Mitigation measures under both codes must be approved by a vessel's flag State.[105] Failure to assess and mitigate such risks under either code exposes vessel ownership to potential penalties, also chiefly administered by the flag State.[106] These two risk-based regimes are the prevailing instruments used by the international community to shield vessels from cyberattacks.

VI. MALWARE, A DEVICE UNDER ARTICLE 3 OF THE SUA CONVENTION

While the International Safety Management and International Ship and Port Facility Security Codes' prophylactic guidelines foster a degree of protection for commercial ships, they cannot, naturally, guarantee such attacks will not occur. Maritime targets will be struck by hackers.[107] In light of this reality, nations may benefit from response plans that contemplate the apprehension, extradition, and prosecution of international maritime hackers. If malware were viewed as a device under Article 3 of the 1988 SUA Convention, the

101. IMO, GUIDE TO MARITIME SECURITY AND THE ISPS CODE, at xv (2012 ed.).

102. *See* IMO, Doc. Res. MSC 428(98), *supra* note 99 (affirming that safety management system enacting under SOLAS's ISM Code should take into account cyber risk management).

103. *See* IMO, Doc. MSC 102/9, *supra* note 99 (recognizing that security measures implemented via SOLAS's ISPS Code should protect against terrorism and other illicit acts, such as cyber-attacks).

104. *See generally* International Convention for the Safety of Life at Sea, ch. IX, XI-2, Nov. 1, 1974, 32 U.S.T. 47, 1184 U.N.T.S. 277 (as amended).

105. *Id.*

106. *Id.*

107. *See* Tuerk, *supra* note 31, at 355–56 (explaining that the International Ship and Port Facility Security Code's technical security framework does not guarantee terrorist attacks will not occur).

treaty would provide, *prêt-à-porter*, a foundation upon which States could build criminal accountability into their plans.

A. The Vienna Convention on the Law of Treaties General Rule of Interpretation

Surely, the drafters of the 1988 SUA Convention were not contemplating malware when they criminalized the placement of devices on ships. That said, they left the word "device" undefined and open for interpretation.[108] As such, the international rules for treaty interpretation in the Vienna Convention on the Law of Treaties (VCLT) are instructive. The VCLT provides that a treaty "shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[109] The VCLT contemplates a good faith, holistic look at a treaty's text, its context, and its aim.[110] Applying the VCLT to the 1988 SUA Convention strongly suggests malware qualifies as an Article 3 device.

B. Ordinary Meaning of the Word "Device"

The Oxford English Dictionary of 1988, the year the SUA Convention was adopted, provides a modest definition of the word device: "a thing that is made or used for a particular purpose."[111] This definition has remained nearly the same through the years, with a more recent Oxford dictionary similarly defining a device as "a thing made or adapted for a particular purpose."[112] Under these plain definitions, whether something is a device seems to hinge simply on whether it performs some function by design.

---

108. Among the previously mentioned five anti-terrorist conventions, the 1971 Montreal Convention also uses the word "device," prohibiting the placement of such on aircraft. Just like the 1988 SUA Convention, however, the 1971 Montreal Convention also leaves the term undefined.

109. Vienna Convention on the Law of Treaties art. 31, May 23, 1969, 1155 U.N.T.S. 331.

110. MARK E. VILLIGER, COMMENTARY ON THE 1969 VIENNA CONVENTION ON THE LAW OF TREATIES 435–36 (2009).

111. *Device*, THE OXFORD PAPERBACK DICTIONARY, (3d ed. 1988).

112. *Device*, NEW OXFORD AMERICAN DICTIONARY (3d ed. 2010).

C. The Word "Device" in Context

According to the VCLT, understanding the plain meaning of a word is not enough. One must also look at the word in context. As for the 1988 SUA Convention, the word device appears to be used in the context of weapons.[113] After all, the treaty was a response to an armed attack and criminalized acts against vessels often perpetrated with weapons—those involving force, threats, violence, destruction, damage, injury, and death.

In the weapons context, a group of experts has previously analyzed whether malware qualifies as a device. Namely, the International Group of Experts on the international law applicable to cyber operations has analyzed a corpus of international law to understand how certain international norms translate in the cyber domain.[114] The group's resulting publication, known as the *Tallinn Manual*, represents the world's most authoritative guidebook on cyber operations and international law, in both the law of armed conflict and peacetime legal regimes. The *Tallinn Manual* includes two rules suitable for present purposes—Rule 103 on the general means of warfare and Rule 106 on booby-traps.

Rule 103 looks at both the "means" and "methods" of warfare, terms of art associated with the law of armed conflict.[115] While the SUA Convention is outside the law of armed conflict sphere, aspects of Rule 103 easily translate to a peacetime treaty like the 1988 SUA Convention because, as the *Achille Lauro* tragedy illustrates, weapons used in armed conflict are often the same used to commit unlawful acts in times of peace. Hence, Rule 103's conclusion about "cyber weapons" is germane. Importantly, Rule 103 considers an object a weapon based not on its form, tangible or intangible, but on its design and function.[116]

Rule 106 arrives at a similar conclusion when examining the Mines Protocol—an international instrument on mines, booby-traps, and other devices.[117] The Mines Protocol is the second annex to the 1981 Convention on Certain Conventional Weapons, a treaty adopted to regulate global weapons

---

113. Even the *New Oxford American Dictionary* embraces the idea that the word device is sometimes synonymous with the word weapon, offering "a bomb or other explosive weapon" as an illustrative example of a device. *Id.*

114. TALLINN MANUAL 2.0, *supra* note 4, at 1.

115. *Id.* at 452.

116. *Id.*

117. Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, Oct. 10, 1980, 1342 U.N.T.S. 168.

use.[118] As part of a conventional weapons treaty, the Mines Protocol[119] understandably employs and defines various weapons-centric terms. The protocol's definition of the word booby-trap is instructive.

The Mines Protocol defines a booby-trap as "*any device* . . . designed, constructed or adapted to kill or injure and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act."[120] Operating from this definition, Rule 106 of the *Tallinn Manual* asks whether something intangible, particularly malware, can be a device.[121] Contending "there is no reason as a matter of law to differentiate between a physical object . . . and cyber means of achieving an equivalent objective," Rule 106 characterizes malware as a type of cyber booby-trap and then expressly concludes malware qualifies as a device under the Mines Protocol.[122]

Based on the *Tallinn Manual's* persuasive view, as reflected in Rule 103 and Rule 106, when it comes to weapons, what makes something a *device* is its design and its function, not its form. This harmonizes seamlessly with the plain meaning of the term, as used in both 1988 and present-day. Recalling that malware is merely software intended to damage or disable, it follows that malware, at its core, is merely a type of cyber device, a digital tool made or used to cause harm in the digital world.

---

118. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 137.

119. The Mines Protocol was amended on May 3, 1996, but the amendment was equally silent about cyber operations.

120. Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 2, Oct. 10, 1980, 1342 U.N.T.S. 168 (emphasis added).

121. Rule 106 of the *Tallinn Manual* explores more than the meaning of the word device. Rather, the rule is about the degree to which Mines Protocol restrictions apply to booby traps, particularly those of the cyber variety. Naturally, to understand the reach of such restrictions, the experts had to first answer whether a device must be tangible. If only tangible things were devices, there would be no basis to examine how those restrictions operate in cyberspace. Conversely, if intangible things (e.g., malware) were to qualify as a device, then there would be reason to examine how the protocol's booby trap restrictions apply to cyber operations.

122. TALLINN MANUAL 2.0, *supra* note 4, at 457–59.

D. Giving Effect to the SUA Convention's Object and Purpose

As the VCLT teaches, for the above interpretation to survive, it must give effect to the 1988 SUA Convention's object and purpose.[123] The interpretation "may not lead to a result that 'weakens the [treaty's] system of protection.' "[124] If an Article 3 device were to include cyber devices, such as malware, would that give effect to the treaty's object and purpose or weaken its system of protection?

Because the 1988 SUA Convention was adopted in direct response to a terrorist act, it is logical to conclude the object and purpose of the treaty is simply to thwart terrorism. Likewise, because the treaty was put in place to expand jurisdiction over maritime offenses, it is equally logical to conclude the Convention's object and purpose is to ensure international outlaws have no place to hide. Indeed, many scholars treat the Convention's "anti-terrorist" and "extradite or prosecute" underpinnings as part and parcel to its aim.[125] Of note, Judge Helmut Tuerk, Vice-President of the International Tribunal for the Law of the Sea, and Dr. Rosalie Balkin, former Director of Legal Affairs and External Relations at the IMO, go so far as to explicitly and compellingly state that the treaty's object and purpose is "to deal with acts of terrorism and to provide a legal framework for the apprehension and prosecution of alleged terrorists."[126]

While leading authorities discuss thwarting terrorism and prosecuting outlaws as the aim of the 1988 SUA Convention, a broader view exists. Particularly, another prominent theory is that the object and purpose is simply to protect international shipping. Returning to its preamble, the 1988 SUA Convention recognizes itself as a response to "the problem of terrorism

---

123. COMMENTARY ON THE 1969 VIENNA CONVENTION ON THE LAW OF TREATIES, *supra* note 110, at 428.

124. *Id.* at 428 n.51 (quoting Proposed Amendments to the Naturalization Provision of the Constitution of Costa Rica, Advisory Opinion OC-4/84, Inter-Am. Ct. H.R. (ser. A) No. 4, ¶ 24 (Jan. 18, 1984), https://www.corteidh.or.cr/docs/opiniones/seriea_04_ing.pdf.

125. *See* Halberstam, *supra* note 23, at 296 (referring to States' opinions that "the purpose of the convention is to ensure that certain acts do not go unpunished"); Freestone, *supra* note 24, at 306–7 (describing the convention's aim as "the suppression of terrorist acts related to maritime navigation . . . [with] the general principle of 'extradite or try' "); Attard, *supra* note 30, at 505 (referring to the convention as a response to "the urgent need for a legal instrument that would help prevent and suppress acts of maritime terrorism" and stating the convention's precise aim is to avoid perpetrators escaping prosecution).

126. Tuerk, *supra* note 31, at 356 (quoting Balkin, *supra* note 63, at 24).

aboard or against ships."[127] However, the treaty's preamble also proclaims a broader intention—"the prevention of *all* unlawful acts against the safety of maritime navigation,"[128] not just those committed by terrorists.[129]

Judge Tullio Treves, Professor of International Law at the University of Milan and Judge at the International Tribunal for the Law of the Sea, advanced this line of thinking in a 1998 article. In that article, he concluded "that safety of navigation was one of the main concerns of the parties."[130] He arrived at this conclusion based on the treaty's preambular text, the enumerated offenses' collective focus on acts constituting "a danger to the safe navigation" of ships, and "[t]he very fact that the Convention was negotiated within the framework of the IMO."[131] According to his rationale, because of its grave importance to the international community, the MTS deserves protection against *all acts* that "endanger navigation." As he put it, "[n]otwithstanding the reasons and history of its adoption, it would seem the Rome Convention[132] can apply to many cases of violence at sea [against maritime navigation] that have nothing to do with terrorism and which belong to the wider category of common crimes."[133]

Observing that jurists have described the 1988 SUA Convention's object and purpose differently is not to suggest these are competing views. Thwarting terrorism, punishing international outlaws, and safeguarding maritime navigation are not mutually exclusive goals.[134] That is, the 1988 SUA Convention, by fortifying criminal jurisdiction across the globe following an uptick in maritime terrorism cases, aims to protect global shipping from a range of destructive behaviors that endanger navigation, whether common crimes or terrorist acts.

---

127. 1988 SUA Convention, *supra* note 2, pmbl.

128. *Id.*

129. As reflected in its 2003 prosecution of a Chinese national, the United States embraces this broader view and does not limit the 1988 SUA Convention's reach to only terrorist acts. In that case, a United States court concluded the 1988 SUA Convention's offenses, as codified in domestic law, do not include a terrorism element. The court found the defendant's non-terrorist crimes squarely fit as SUA offenses because they jeopardized the safety of maritime navigation. U.S. v. Shi, 396 F. Supp. 2d 1132, 1134–35 (2003).

130. Treves, *supra* note 33, at 544.

131. *Id.* at 544–45.

132. In his 1998 article, Judge Treves refers to the 1988 SUA Convention as the Rome Convention, ostensibly because it was adopted in Rome. *Id. passim.*

133. *Id.* at 544.

134. *See* COMMENTARY ON THE 1969 VIENNA CONVENTION ON THE LAW OF TREATIES, *supra* note 110, at 427 ("Indeed, a treaty may have many object and purposes").

Holistically speaking, interpreting the term device in Article 3 as including malware seems to pass the VCLT's test with flying colors. Malware is purposefully designed and used for a particular function—to illicitly access and adversely impact computer systems—and thus, in both ordinary and contextual usage, qualifies as an Article 3 device. Relying on this interpretation to expand criminal jurisdiction over bad actors who use malware to endanger maritime navigation would surely "send a very clear message . . . that such acts will not be tolerated"[135] and thus give effect to the treaty's overall object and purpose while enhancing, not weakening, its system of protection.

VII. CONCLUSION

Cyber threats and vulnerabilities across global shipping are well known and well present. These threats and vulnerabilities are compounded by the MTS's increased functional dependence on computers for engineering, operations, and navigation. To harden ships against cyberattacks, the global community chiefly employs prophylactic guidelines via the International Safety Management Code and the International Ship and Port Facility Security Code to regulate industry behavior. Experience shows, however, that regulating industry behavior is not always enough. Commercial vessels will still fall prey to cyberattacks.

The 1988 SUA Convention provides, *prêt-à-porter*, a robust jurisdictional suite and authorities for apprehension, extradition, and prosecution of offenses that arise in all areas of the sea. Just as the treaty arose over the maritime domain to address the problem of terrorism, today it stands ready to address cyberattacks, whether committed by terrorists, State actors, or common criminals. Knowing hackers will breach the international regulatory framework and successfully strike commercial vessels, SUA's 166 State parties should prepare to introduce prosecutorial decision-making under the 1988 treaty into their current cyberattack response plans.

135. *See* Balkin, *supra* note 63, at 31 (describing the SUA Convention as a deterrence-based complement to the International Ship and Port Facility Security Code).