NOTES

STATE-SPONSORED RANSOMWARE THROUGH THE LENS OF MARITIME PIRACY

Evans F. Horsley

TABLE OF CONTENTS

I. INTRODUCTION 670

II. BACKGROUND INFORMATION 671
- *A. Background on State-Sponsored Economic Cyberattacks* 671
- *B. The History of Maritime Piracy* 673
- *C. Contemporary Understanding of Laws on Maritime Piracy* 675

III. ANALYSIS 677

IV. CONCLUSION 681

I. INTRODUCTION

Until the last few decades, conflicts between nation-states were confined to four domains: land, water, air, and space.[1] Common to each of these domains is the fact that they are all physical divisions with relatively distinct borders. It was not until recently when we added the fifth domain, cyberspace, that laws had to be adapted to deal with an entire realm of activity that only exists intangibly.[2] Cyberattacks are unique in that the individuals actually perpetrating the assaults do not need to be present within the physical arena they are targeting, and they do not require the extensive training or heavy artillery required for the success of most military operations.[3] The Ponemon Institute reported in 2016 that American companies lost on average $17.36 million per year to cyberattacks, but the thieves only needed a few computers to carry out their attacks.[4]

In May 2017, North Korea was linked to the WannaCry cyberattacks that targeted personal computers in over 150 countries.[5] WannaCry ransomware held computers hostage until the ransom, which was paid in the cybercurrency "bitcoin," was proffered. If the ransom was not paid, all of the files on the computer would be destroyed.[6] The use of this type of state-sponsored cyberattack, the sole purpose of which was to extort money, was unprecedented, at least in the domain of cyberspace.[7]

However, state backing of robbers on the high seas has a long and storied history stretching back for thousands of years to the Ancient Greeks.[8]

[1] *War in the Fifth Domain*, THE ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792.

[2] *Id.*

[3] Mathew C. Waxman, *Cyber Attacks as "Force"" Under UN Charter Article 2(4)"*, 87 INT'L L. STUDIES 43, 45 (2011).

[4] Eric J. Rightmier, *The Effect of State-Sponsored Attacks on the Private Sector*, PROQUEST LLC (April 2017), https://search.proquest.com/openview/9554a2b3a5afb733e07914a233c7d30e/1?pq-origsite=gscholar&cbl=18750&diss=y.

[5] Charles Riley & Samuel Burke, *Intelligence Agencies Link WannaCry Cyberattack to North Korea*, CNN BUS. (June 16, 2017), http://money.cnn.com/2017/06/16/technology/wannacry-north-korea-intelligence-link/index.html.

[6] *What Is WannaCry Ransomware?*, FOX NEWS (May 23, 2017), http://www.foxnews.com/tech/2017/05/15/what-is-wannacry-ransomware.html.

[7] Reuters, *Cybersecurity Experts Fear Continued Spread of 'Unprecedented' Ransomware Attack*, FORTUNE TECH (May 14, 2017), http://fortune.com/2017/05/14/ransomware-wanna-cry-wannacry-cyber-attack-nhs/.

[8] Daud Hassan & Sayed M. Hasan, *Origion, Development and Evolution of Maritime Piracy: A Historical Analysis*, 49 INT'L J. L., CRIME AND JUST. 1, 2 (Jan. 12, 2017), http://www.sciencedirect.com/science/article/pii/S1756061616300878?via%3Dihub.

Throughout this time, nations have alternatively "treated pirates as combatants, enemies or criminals."[9] Currently, there is no uniform definition of piracy at the domestic level, and there are debates regarding the efficacy of the international definition provided in Article 15 of the 1958 Geneva Convention on the Law of the Sea (HSC) and Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS).[10] Nevertheless, it is the position of this Note that the newer form of economic aggression displayed in the WannaCry attack is not a new concept, and state-sponsored ransomware can be understood in the context of maritime piracy.

The objectives of this Note are to provide a brief review of the evolution of maritime piracy and legal approaches to it, and to analyze the new state-sponsored economic cyberattacks through the lens of this longstanding international crime. State-sponsored ransomware attacks are cyberattacks which are either funded by a government or executed by its agencies primarily for the purpose of monetary gain. These attacks are a new concept, but the underlying action is an old one. These ransomware attacks are just state-sponsored piracy in a new domain. As such, it is logical to conceptualize ransomware attacks under the preexisting legal framework for maritime piracy.

II. BACKGROUND INFORMATION

In order to conceptualize state-sponsored cyberattacks under the history and laws surrounding maritime piracy, we must first possess a basic understanding of the subjects involved. Cyberspace is new to the technological age, and the laws governing this new domain remain largely unrefined. Similarly, the current domestic laws and international treaties governing piracy, which have only been in place for about the last century, are in many ways fundamentally different from the legal philosophies on piracy that predominated most of modern history. The effect of these contemporary changes underpins the analysis of this Note.

A. Background on State-Sponsored Economic Cyberattacks

State-sponsored cyberattacks differ from those perpetrated purely by individuals in a number of key aspects beyond the mere fact that a country rather than an individual is behind the assault. These differences can make state-sponsored attacks both more damaging and harder to defend against.[11] Unlike

[9] *Id.* at 8.

[10] *Id.* at 4.

[11] Maria Korolov, *10 Deadliest Differences of State-Sponsored Attacks*, CSO ONLINE (Dec. 1, 2014), https://www.csoonline.com/article/2852855/advanced-persistent-threats/10-deadliest-differences-of-state-sponsored-attacks.html.

cybercriminals, countries will not necessarily target marketable cyber material. Instead, they will usually attempt to gain information that will benefit the national interest in some manner. Perhaps the most immediately obvious example of the type of data a government will attempt to gain is political information stored in embassies or governmental agencies that may be important for national security reasons. However, states may also target private companies to access trade secrets in a bid to help their domestic producers, as was the case in the Chinese UglyGorilla attacks on five U.S. companies, including the United States Steel Corporation, in 2014.[12]

State-sponsored attackers are also more likely to have large, well-organized teams, and these teams are capable of working around the clock.[13] Not only can states perpetuate attacks all day and night, but they are also capable of maintaining penetration into foreign systems—undetected—for long periods of time.[14] As of 2014 "84 percent of the reported attack discoveries were made by third parties."[15] In contrast, private hackers do not typically have the resources or the inclination to target more secure networks or to continue a hack long-term.[16]

Article 2(4) of the United Nations (UN) Charter states "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[17] This prohibition on the threat or use of force is a succinct provision, but its impact on state responses towards disfavored actions of other nations is far-reaching. Generally, this article restricts military attacks unless a state is acting in self-defense or with authorization from the UN Security Council.[18] In contrast, the self-defense exception is typically not permitted for economic and diplomatic assaults or pressure.[19] In other words, a state cannot respond with physical force when the assault itself was not physical. This proposition usually holds true even if the targeted state suffers tremendous costs.[20]

With regard to cyberwarfare, Article 2(4) has been interpreted to prohibit cyberattacks that cause physical consequences if the effects reach a certain severity threshold, but the same is not true of cyberattacks aimed at causing

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] U.N. Charter art. 2, ¶ 4.

[18] Ido Kilovaty, *Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter*, 4 J. L. & CYBER WARFARE 210 (2015).

[19] Waxman, *supra* note 3.

[20] *Id.*

economic harm.[21] The current use of force scholarship commonly understands this distinction as one between "kinetic" cyberattacks (KCAs), which produce "direct or indirect physical consequences,"[22] and non-kinetic cyberattacks, which produce only non-physical harm.

For example, a Twitter hack in 2013 announcing an explosion in the White House and the death of President Obama caused the Dow Jones index to plummet 145 points, costing approximately $150 billion. This incident would not have fallen under the Article 2(4) prohibition because it was not a KCA.[23] On the other hand, in 1982, hackers tampered with software that controlled the pump speeds and valve settings of a Soviet pipeline, leading to a massive explosion,[24] which would be considered a kinetic cyberattack, and thus would be encompassed by Article 2(4).

The 2017 WannaCry attack targeted preexisting programming weaknesses in computers running on Microsoft operating systems across dozens of countries.[25] The ransomware was capable of infecting both home computers and the networks of larger organizations, leading to the loss of sensitive information, financial losses, disruption to regular operations, and harm to some organizations' reputations.[26] The attack was unprecedented in scope, but despite the fact that it was a state-sponsored effort to steal from individuals and private entities in cyberspace,[27] it was not a KCA as most scholarship understands it. WannaCry was economically motivated aggression and as such would almost certainly not be actionable under Article 2(4) as it is presently interpreted. However, WannaCry highly resembles our historical understanding of maritime piracy and privateering in many significant ways.

B. The History of Maritime Piracy

While many pirates during the "Golden Age" of maritime piracy were true outlaws, there existed a large system of state-sponsored piracy.[28] From Queen Elizabeth I's Sir Francis Drake, often referred to by the Queen as "my pirate," to the Barbarossa Brothers, who were sponsored by the Ottoman Sultan, looting enemy ships was a common practice from the 1400s through the late

[21] Kilovaty, *supra* note 18, at 213.

[22] *Id.* at 212.

[23] *Id.* at 211.

[24] THE ECONOMIST, *supra* note 1.

[25] Supreet Kaur Sahi, *A Study of WannaCry Ransomware Attack*, 4 IJERCSE 5 (2017), https://technoarete.org/common_abstract/pdf/IJERCSE/v4/i9/Ext_89621.pdf.

[26] *Id.* at 6.

[27] Reuters, *supra* note 7; *see also* Kilovaty, *supra* note 18, at 212-13.

[28] Jesse Greenspan, *8 Real-Life Pirates Who Roved the High Seas*, A&E TELEVISION NETWORKS (Sept. 19, 2012), http://www.history.com/news/8-real-life-pirates-who-roved-the-high-seas.

1700s.[29] On the other hand, laws from around the same time period often required pirates to be tried and executed aboard the capturing warship.[30] The scourge of the pirate, whether under the protection of a flag or otherwise, has plagued sovereign nations for nearly as long as merchants have been sailing the high seas, and while it has been eradicated in some areas for a time, it has never been fully eliminated.[31]

As most Romans and Greeks understood, pirates were considered "belligerent[s]."[32] This was in the context of war, and sailors looting ships were largely considered to be acting as enemy combatants.[33] The Ancient Queen Teuta of Illyria "authorized her subjects' ships to 'plunder all whom they fell in with.' . . . This eventually led to uncontrolled piracy in the Adriatic."[34] In time, Queen Teuta's sanctioning of her subjects' plundering caused a war between Illyria and Rome.[35] On the other hand, not all sovereigns condoned piracy by their citizens. King Minos of Crete "is credited as the first [ruler] to establish a strong naval fleet to [suppress] piracy."[36] A clear pattern emerged in ancient times: Piracy flourished when governmental regimes were weak, and it retreated in the face of strong sovereigns.[37]

In more recent history, we have the example of piracy on the Barbary Coast between the 16th and 18th centuries. Piracy grew most powerful under the protection of the Ottoman Empire.[38] In response to the Barbary pirates, European nations signed treaties with the Barbary regencies requiring the Europeans to pay tribute for safe passage through the seas.[39] While this was primarily an economic venture for the Barbary sovereigns, the Europeans may have felt more compelled to comply with the tribute demands due to the millions of European mariners who were captured and forced into slavery by the pirates.[40] This level of coercion is not present in the current-day ransomware attacks, though the idea of paying tribute to a state for safety in a domain is similar.

Around the same time period that the piracy in the Barbary Coast was running rampant, Spain and Portugal signed the papal Treaty of Tordesillas,

[29] *Id.*

[30] Douglas Guilfoyle & Tiffany Willey Middleton, *Law, Pirates, and Piracy*, AMERICAN BAR ASS'N (2010), https://www.americanbar.org/content/dam/aba/images/public_education/latl-pirates.pdf.

[31] Hassan & Hasan, *supra* note 8, at 2.

[32] *Id.*

[33] *Id.*

[34] *Id.* at 5.

[35] *Id.*

[36] *Id.*

[37] *Id.* at 6.

[38] *Id.*

[39] *Id.*

[40] *Id.*

which ultimately prohibited many other seafaring European nations from stationing their ships in the Caribbean or Indian Oceans.[41] As a result, France, Denmark, and England sanctioned privateering in order to weaken the Spanish and Portuguese who were rapidly becoming rich from trade in those regions.[42] This time period later became known as the "Golden Age" of piracy.[43]

The common thread through these examples of state-endorsed piracy is that all instances could be regarded as a type of economic warfare. The sponsoring state aimed the pirates at its enemies or rivals, simultaneously weakening its opponents and gaining an economic advantage, all without any formal wars. However, this brief history has also demonstrated that tolerance for or encouragement of piracy only leads to its growth, which makes it difficult to eradicate in the long run.[44]

The Barbary pirates were not eliminated until the 1800s, after the United States waged two wars against them and France conquered Algiers.[45] Similarly, the piracy that American colonial governors endorsed, which came about due to the costly regulations Great Britain imposed on the colonies, only ceased when England and the colonies passed laws calling for the death penalty for pirates and their aides.[46] Even still, it took well over twenty years for the Golden Age to decline.[47]

C. Contemporary Understanding of Laws on Maritime Piracy

During the first half of the 20th century, the prevailing belief was that maritime piracy had largely disappeared.[48] For this reason, "initial attempts in the twentieth century to introduce a treaty regime against piracy [were] unsuccessful."[49] Instead, we now have an array of domestic laws coexisting with international treaties regarding piracy.[50] "Under international law, piracy is [recognized] as a domestic crime of universal jurisdiction . . . ."[51] With regard to piracy, "[u]niversal jurisdiction is an older concept having little connection

[41] *Id.* at 7.

[42] *Id.*

[43] Greenspan, *supra* note 28.

[44] Hassan & Hasan, *supra* note 8, at 8-9.

[45] *Id.* at 7.

[46] *Id.*

[47] *Id.*

[48] Lawrence Azubuike, *International Law Regime Against Piracy*, 15 ANN. SURV. INT'L & COMP. L. 43, 44 (2009).

[49] *Id.*

[50] Lucas Bento, *Toward an International Law of Piracy Sui Generis: How the Dual Nature of Maritime Piracy Law Enables Piracy to Flourish*, 29 BERKELEY J. INT'L L. 399, 455 (2011).

[51] Hassan & Hasan, *supra* note 8, at 2.

with 'modern' universal jurisdiction," which allows any apprehending state to prosecute certain crimes that shock the conscience of humanity, such as genocide and war crimes.[52] The older conception allowed any state to take law enforcement action on the high seas against any vessel suspected of piracy, even vessels flagged to foreign states.[53] As such, all sovereign countries could exercise jurisdiction over piracy, but they had to do so only through their respective domestic criminal justice systems.[54]

Among the most contested issues under this regime is the actual definition of the term "piracy" itself.[55] In *United States v. Smith*[56] and *United States v. Brig Malek Adhel*,[57] two landmark Supreme Court cases heard in the mid-1800s, the United States defined piracy as "robbery, or forcible depredation, upon the sea."[58] But U.S. statutes from the same time period added a stipulation to this definition: piracy should be defined by the "law of nations," which would include treaties regarding piracy.[59] While the Supreme Court in the 1800s was creating a definition meant to be interpreted as adhering to the law of nations, we have since created new treaties that alter that definition. Similar provisions are seen in the domestic laws of England and Australia, though other countries define piracy without reference to the law of nations.[60] For example, the domestic law of the Philippines requires "the act . . . take place in the state's territorial waters to constitute piracy."[61]

The language "law of nations" is present in the United States Constitution, and was invoked in relation to piracy long before any multilateral treaty involving the crime ever came into being.[62] Nevertheless, the international community attempted to create a more uniform approach to maritime piracy with the enactment of two treaties in the mid-twentieth century, of which the United States is party only to the Geneva Convention.[63] Both Article 15 of the 1958 Geneva Convention on the Law of the Sea (HSC) and Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS) define piracy as:

[52] Guilfoyle & Middleton, *supra* note 30, at 293.
[53] *Id.*
[54] *Id.*
[55] Azubuike, *supra* note 48, at 46.
[56] United States v. Smith, 18 U.S. 153, 154 (1820).
[57] Harmony v. United States, 43 U.S. 210, 232 (1844).
[58] Hassan & Hasan, *supra* note 8, at 3.
[59] *Id.*
[60] *Id.*
[61] *Id.* at 4.
[62] *Id.* at 3.
[63] Guilfoyle & Middleton, *supra* note 30.

> (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> > (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
> >
> > (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
>
> (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
>
> (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).[64]

Key for this Note's analysis is the fact that the action must be committed for private ends. This distinguishes piracy from the ransomware attacks perpetrated by North Korea, due to their sovereign purpose. WannaCry was more akin to the notion of privateering in the Golden Age of Euro-American piracy in that WannaCry was essentially state actors working against private individuals in an "international" domain. As such, while pirates and privateers were distinguished only by the fact that states sponsored the latter,[65] the distinction is still important when analyzing the contemporary legal framework.

III. ANALYSIS

State-sponsored cyberattacks conceptually align with the historical understanding of maritime piracy. The pirates during the Golden Age of piracy could be viewed as the equivalent of modern-day private military contractors.[66] However, military contractor activity typically tends to focus less on material theft and more on strategic military advancement. The state-sponsored pirates that existed before the 1900s, while endorsed by monarchs, were primarily attempting to enrich themselves and their sponsor. Similarly, the goal of the WannaCry ransomware attack was to enrich North Korea.

[64] Hassan & Hasan, *supra* note 8, at 4.

[65] *Id*. at 2.

[66] Guilfoyle & Middleton, *supra* note 30.

A common theme between these cyberattacks and historical state-sponsored piracy is the indiscriminate nature of the taking.[67] North Korea's WannaCry ransomware attack did not just target other state actors. It also hit private companies and individuals in over 150 separate countries.[68] While on a national scale India was one of the hardest hit countries, companies like FedEx, Nissan, and railway companies in Germany and Russia, as well as at least sixteen NHS organizations in the United Kingdom, were badly affected.[69] Additionally, a large number of Chinese colleges and students were struck in the attack.[70] This single state-sponsored malware attack hit governmental entities, private companies, and individual people, and was motivated by economic gain.

Another similarity between cyberattacks and historical maritime piracy is the relatively low costs needed to perpetuate assault. The probability of a pirate being tried and successfully prosecuted was low, in part due to the "elusiveness and anonymity of a ship in the expanse of [the ocean]."[71] The same difficulties are presented by cybercrime. Attacks in cyberspace are hard to track, and even if the guilty party is identified, numerous jurisdictional issues must be addressed before a trial can occur.[72]

Prior to the treaties on piracy that were drafted in the 1900s, there were several approaches to handling piracy. Alfred H. Rubin and others argue that piratical actions by states were merely the states exercising a right to seize passing ships in order to levy taxes against them.[73] The pitfall of this "tax" justification is that piracy was a violent seizure of merchandise from non-citizens, leaving the question of whether these countries had jurisdiction to act.[74]

However, playing into this understanding of the role of piracy was the idea of negotiating tributes for safe passage, as was seen along the Barbary Coast.[75] In a way, payment after a ransomware attack is like paying tribute. However, in order to use tributes as a preventative measure, the attacking sovereign would need to openly own its involvement in the economic assault. As would be expected, North Korea continues to deny any involvement in the

[67] J. L. Anderson, *Piracy and World History: An Economic Perspective on Maritime Predation*, 6 J. WORLD HIST. 175, 176 (1995).

[68] Riley & Burke, *supra* note 5.

[69] Savita Mohurle & Manisha Patil, *A Brief Study of Wannacry Threat: Ransomware Attack 2017*, 8 INT'L J. ADVANCED RES. COMPUTER SCI. 1938, 1939 (2017).

[70] *Id.* at 178.

[71] Anderson, *supra* note 67, at 178.

[72] Deb Shinder, *What Makes Cybercrime Laws so Difficult to Enforce*, CBS TECHREPUBLIC (Jan. 26, 2011), https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/.

[73] Anderson, supra note 67, at 177.

[74] *Id.* at 178.

[75] Hassan & Hasan, *supra* note 8, at 6.

WannaCry cyberattack, calling accusations by the British government "'a wicked attempt' to tighten international sanctions on the country."[76] And it seems unlikely that other countries would be any more willing to openly admit to such antagonistic behavior.

Additionally, one of the primary historical problems with paying tributes and accepting a semi-regime of piracy is that maritime predation tends to escape the control of the sponsoring nation. For example, the promotion of piracy by the ancient Illyrian Queen Teuta, who "[authorized] her subjects' ships to 'plunder all whom they fell in with,'" eventually led to "uncontrolled piracy" in the Adriatic.[77] These concerns are precisely the reason why the U.S. government has a general policy against negotiating with kidnappers.[78] Logically, conceding to pay incentivizes the enemy to continue extorting ransoms from the United States. Therefore, sacrificing a few people in the short term may better serve the state in the long run.

Historically, states are more successful in driving out piracy when they take a strong stance against the activity, state-sponsored or private. King Minos of Crete is credited as the first ruler to establish a strong naval fleet with the goal of stopping maritime piracy, and he was successful at suppressing it.[79] In 1698, England passed the Piracy Act, which imposed the death penalty for the crime of piracy.[80] "Between 1716 and 1726, a large number of pirates were executed in public under the new legislation," and approximately 100 years later, the United States fought in the Barbary Wars to end piracy in the Barbary Coast.[81] At some periods in history, justice against pirates was so swift and decisive that those found to be pirates could be tried and executed aboard the capturing warship.[82]

When the pirates were tried and executed aboard the capturing warship, the punishing nation was exercising jurisdiction in the high seas. Analogous to this situation in the high seas is the internet, which could be conceptualized as international waters. If countries could track attackers back to their home IP addresses, they could immediately launch a counterattack. Because the counterattack would not necessarily ever exit cyberspace, whether the retaliating country would have the jurisdiction to mete out a punishment against their attacker on the spot is debatable.

[76] *North Korea Calls UK WannaCry Accusations 'Wicked'*, BBC NEWS (Oct. 31, 2017), http://www.bbc.com/news/world-asia-41816958.

[77] Hassan & Hasan, *supra* note 8, at 5.

[78] Adam Taylor, *The Logic of Not Paying Ransoms*, WASH. POST (Aug. 21, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/08/21/the-logic-of-not-paying-ransoms/?utm_term=.4a9021105f47.

[79] Hassan & Hasan, *supra* note 8, at 5.

[80] *Id.* at 7.

[81] *Id.*

[82] Guilfoyle & Middleton, *supra* note 30, at 292.

If nations approached state-sponsored ransomware attacks in such a direct fashion, determining which level of force the UN Charter Article 2(4) Use of Force provision would allow in such cases would be difficult. When retaliating against another country, state actions move beyond the punishment of criminals and into more strategic waters: "[T]here is no clear consensus on how [a retaliating country] could legally respond, whether with armed force, its own cyber attack, or some other measure."[83] But, the history of maritime piracy seems to suggest countries should strike back with a cyberattack that cripples the original assaulter's ability to continue its cyber-predation or risk the expansion of economic cyberpiracy.

Looking at the issue through a more modern piracy lens, analyzing responses to ransomware attacks under the current definition of maritime piracy, as found in HSC Article 15 and UNCLOS Article 101, is difficult because the act must be committed for private ends to constitute piracy.[84] Ransomware attacks like WannaCry do meet the definitional deprivation requirement, but state-sponsored ransomware attacks are by their nature not meant for private ends, as they are acts perpetuated by the government for a public purpose. However, subpart (c) of the definition of piracy includes "any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b)."[85] Therefore, if a state were to direct and pay a private entity to carry out a ransomware attack, the attack could potentially still fall within this definition.

If that premise is accepted, then the retaliating state would have the authority under UNCLOS to seize the property or information stored on the attacker's computer, which is analogous to the pirate's ship.[86] This seizure would take place remotely, so the chances of actually apprehending the hacker behind the attack would be slim. However, it would authorize a retaliating country to have a defense that is both legally viable and an adequate threat, as countries like North Korea may be less likely to attempt ransomware hacks if they know it could be legal for another country to steal their information in return.

If that premise is not accepted, the analysis would turn on the UN's Article 2(4) provision on the use of force, which as discussed in the Introduction, has several significant flaws when it comes to purely economic cyberattacks. Primarily, this article restricts military attacks unless a nation is acting in self-

[83] Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 25 BERKLEY J. INT'L L. 191 (2009).

[84] *See* Hassan & Hasan, *supra* note 8, at 4.

[85] *Id.*

[86] *See Legal Framework for the Repression of Piracy Under UNCLOS*, U.N. DIV. FOR OCEAN AFFAIRS AND THE LAW OF THE SEA (Sept. 9, 2010), http://www.un.org/depts/los/piracy/piracy_legal_framework.htm.

defense or with authorization from the UN Security Council.[87] The self-defense exception is typically not permitted for economic and diplomatic assaults or pressure.[88] As such, a state generally cannot respond with physical force when the assault itself was not physical, even if the targeted state suffers tremendous costs.[89]

IV. CONCLUSION

The newer form of economic aggression displayed in the WannaCry attack is not a new concept, and state-sponsored ransomware can be understood in the context of maritime piracy. Prior to the 1900s, nations frequently allowed maritime piracy to flourish and often even sponsored the predatory practice. The history of these regimes demonstrates that society as a whole is better off if states take a hard stance against maritime piracy. In many ways, ransomware attacks are to the internet what pirates traditionally were to the seas, so countries would be best served by striking back against these types of economic cyberattacks unequivocally.

However, modern treaties regarding maritime piracy restrict the definition of piracy to private actions for the benefit of private parties.[90] Therefore, modeling the approach to cyber threats (and any potential treaties within that realm) off of the current piracy treaties should be done with a critical eye towards the potential shortcomings of these treaties as applied in the cyber realm. For example, the provision requiring that the illegal acts be committed for private ends does not translate as well to the cyber realm as it does to the physical seas. If state troops board an American vessel, even if the state's purpose in authorizing the boarding is purely mercenary, the boarding is still an act of physical aggression that easily falls within the provisions of other relevant treaties, such as UN Article 2(4). But if the allegorical equivalent occurs in cyberspace, there is no physical violence to accompany the state-sponsored thievery, forcing states to work around the language in current treaties in order to find a legal retaliation.

The world as a whole has an abundance of experience dealing with maritime piracy. The understanding that thousands of years of marine pillaging has given us, both in the form of our more traditional understandings and in the form of our modern-day approach, should guide us as we begin tackling the domain of cyberspace, and more specifically, state-sponsored cyberattacks against private parties.

[87] Kilovaty, *supra* note 18, at 210.

[88] Waxman, *supra* note 3, at 44.

[89] *Id.*

[90] Hassan & Hasan, *supra* note 8, at 4.