How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea

Jason Petty
How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea

Jason Petty*

Abstract

Submarine internet cables play a vital role in the modern economy and transmit almost all global internet connections between countries. These cables, however, are vulnerable to interference or hacking by foreign states who seek to obtain the valuable data that passes through them. Because these cables are located on the high seas, however, no country has legal jurisdiction over large portions of them allowing for any number of states or private actors to hack into them and steal valuable information. This Comment evaluates whether states have any legal recourse under public international law against entities that hack into submarine cables. To answer this question, this Comment explores the development of public international law with respect to the high seas and evaluates public international norms for hacking and cyber operations. This Comment then argues, given the weakness of current domestic regimes with respect to submarine cable protections, the International Tribunal of the Law of the Sea can assert jurisdiction over disputes related to submarine hacking. This Comment further makes the novel argument that states can assert damage done to cables through hacking or violations of citizens’ rights to privacy through hacking present potential legal avenues to pursue liability against submarine hacking.

* J.D. Candidate, 2022, The University of Chicago Law School. The author wishes to thank his family for their support, his advisor, Professor Eric Posner, for the helpful suggestions and insights, and the entire board and staff of the Chicago Journal of International Law for their comments, review, and support.
Table of Contents

I. Introduction......................................................................................................................... 262
II. Technical Primer on Hacking and Submarine Cables .................................................... 264
III. The Shifting Dialogue Around Submarine Cable Hacking ............................................ 267
IV. International Laws Regulating Submarine Cables......................................................... 270
   A. The 1884 Convention for the Protection of Submarine Telegraph Cables ...................... 270
V. International Norms With Respect to Hacking................................................................. 277
   A. General Cyber Operations on the High Seas ................................................................. 277
   B. Incidental Effects of Submarine Cable Hacking: Cable Damage ............................... 279
   C. Incidental Effects of Submarine Cable Hacking: Violations of the International Right to Privacy .......................................................................................................................... 280
VI. The Lay of the Land of Current Scholarship ................................................................. 283
VII. Using ITLOS to Trigger Dispute Resolution: Damage and Privacy Solutions for Hacking ........................................................................................................................................ 286
   A. Jurisdiction Under ITLOS ............................................................................................. 286
   B. Using ITLOS to Protect Against Cable Damage ......................................................... 289
   C. Using ITLOS to Protect Against Violations of the Right to Privacy ........................... 291
VIII. Conclusion ..................................................................................................................... 297
I. INTRODUCTION

Contrary to popular belief, the global internet is largely comprised of a network of data cables linking states and continents and not satellite links propelling data through the air.\(^1\) In communications between continents, approximately 99% of all telecommunications is transmitted via a network of around 400 underwater, submarine cables.\(^2\) For example, to send an email from Boston to Dublin, the GTT Atlantic Cable would route your message under the Atlantic Ocean through Nova Scotia, Northern Ireland, and London before arriving in Dublin.\(^3\) This process would take place nearly instantaneously but traverse hundreds of miles of fiber optic cable under the Atlantic Ocean.

These undersea cables are only about the size of a garden hose but represent billions of dollars of productivity and information. If a ship were to drop anchor in the wrong location and sever a cable, internet service could be cut to an entire country.\(^4\) If a rogue agent elected to cut the cables to the United States, an estimated $10 trillion in daily financial transfers and vast amounts of data would be clogged up.\(^5\) Because damage to submarine cables is so devastating, the international community has devised a number of conventions and domestic protections to protect against cable damage.

More insidiously, however, these cables are also at risk of hacking and intelligence gathering because so much data flows through them. States can use submarines to make small slits in submarine cables and insert listening and data collection devices.\(^6\) These spying states then collect all the information that flows through the cables: every overseas telephone call, email, financial transfer, or data upload that passes through the internet from one country to another is collected.\(^7\) Encryption of information that passes through these cables somewhat protects against intelligence gathering, but sophisticated operators can often break encryption and can nevertheless obtain useful information through the metadata

---

embedded in encrypted transmissions. This massive amount of information provides valuable military, economic, and personal information to the hacking country. This hacking, however, is also a violation of citizens’ privacy and a violation of the hacked states’ economic and military interests.

Out of concern for this sort of hacking, in 2020 the U.S. blocked Google and Facebook from turning on a submarine cable linking the U.S. and Hong Kong. Although the 8,000 mile cable had already been laid and hundreds of millions of dollars were spent on its development, the U.S. was too concerned about potential Chinese intelligence pilfering to let the cable go live. The decision dramatically demonstrates the U.S.’s fears around submarine cable hacking have grown to exceptional new heights. And the U.S. government’s fears are not misplaced. In 2013, the British spy agency the Government Communications Headquarters (GCHQ) was found to secretly have tapped into undersea cables to gather information. In 2015, U.S. sensors detected Russian submarines near undersea cables raising concerns. And during the Cold War, the U.S. tapped into Soviet undersea cables and gathered critical intelligence as part of Operation Ivy Bells.

As the world becomes increasingly interconnected and states increasingly rely on the internet economically, hacking into internet infrastructure becomes a greater threat. The U.S., for example, has undertaken expensive and extensive efforts to remove Huawei from its domestic telecommunication infrastructure to prevent the Chinese government from spying domestically. Undersea cables, however, are not so easily protected. Undersea cables are expensive to lay,
difficult to replace, and often traverse international waters over which states do not have exclusive domain.\textsuperscript{16}

Even with such a large threat, there is an open question as to whether states can protect against submarine cable hacking. The fundamental question this Comment seeks to answer is whether states have any recourse or protections against submarine cable hacking by foreign states under public international law. This Comment argues the increasingly recognized international right to privacy can provide grounds for protecting against submarine cable hacking and that states can enforce this right through dispute resolution mechanisms for the high seas.

This Comment proceeds in five sections to develop this answer. Section II provides a brief overview of the technology behind submarine cables and the methods used in hacking these cables. Section III evaluates current attitudes in the international community with respect to submarine cable hacking and explains why norms around privacy, combined with the incredible resources required to protect cables from hacking, may lead to a shift in states’ treatment of submarine cable hacking.

Section IV explores the history of international treaties and conventions surrounding submarine cables and the high seas. Section V summarizes current public international law related to cyber operations and hacking and discusses the emergence of a newly recognized international right to privacy with respect to telecommunications and personal data. Section VI discusses current scholarly responses to submarine cable hacking to situate this Comment’s solution in present scholarship. And in Section VII, I propose a novel solution addressing the problem of submarine cable hacking using the international right to privacy adjudicated through dispute resolution mechanisms developed for the high seas. The use of the international right to privacy and this dispute resolution body is presently underdiscussed by scholars. This solution further advances the right to privacy as integral to protect against submarine cable hacking and describes how shifts in attitudes toward privacy may contribute to the creation of norms against surveillance hacking.

II. TECHNICAL PRIMER ON HACKING AND SUBMARINE CABLES

This Section describes the network of submarine cables that makes up the modern internet, the technical elements of modern submarine cable hacking techniques, and the possibility of damage by submarine cable hacking. This information is relevant to subsequent possible solutions around submarine cable hacking.

hacking because international treaties require some protections against incidental or intentional damage to submarine cables, as discussed in Section IV.

Most of the internet is formed through a network of undersea submarine cables.\textsuperscript{17} About the size of a garden hose, these cables are buried just under the ocean floor by submarine-cable laying ships and transmit internet data between countries.\textsuperscript{18} While there are some legacy cables that transmit primarily telephone or telegraph information, the majority of modern cables are fiber optic cables that can transmit dozens of Terabytes of data per second.\textsuperscript{19} While some cables are specially created for military and intelligence transmission purposes, the majority of cables are general in use and transmit commercial, government, and private commercial correspondence simultaneously.\textsuperscript{20}

Because laying and operating a cable across large bodies of water is so costly, most cables were historically financed, laid, and operated by a consortium of multiple owners. For example, the U.S., Japan, and Australia agreed in 2020 to jointly finance a cable link to the Pacific island nation of Palau at a cost of $30 billion.\textsuperscript{21} Despite this history, individual companies or governments increasingly financed and laid submarine cables.\textsuperscript{22} For example, in 2020 Google announced it was financing and constructing its own cable linking the U.S., the United Kingdom, and Spain.\textsuperscript{23}

Once laid, cables are maintained and operated by the financing consortium or the private company financing the cable project. These cable operators are responsible for maintenance and repairs for any damage to the cable. Due to their length, most modern cables are outfitted with fault monitoring systems that can detect cable breaks or points of damage for repair.\textsuperscript{24}

States are capable of spying on submarine cables. As discussed below, because the hacking of cables requires specialized equipment including submarines, most experts are concerned with government-sponsored hacking.

\textsuperscript{17} Id.
\textsuperscript{19} Klint Finley, How Google Is Cramming More Data into Its New Atlantic Cable, WIRED (Apr. 5, 2019), https://perma.cc/D49P-23GW.
\textsuperscript{21} Yohei Hirose, Japan, US and Australia to Finance Undersea Cable for Palau, NIKKEI ASIA (Oct. 28, 2020), https://perma.cc/2WXP-FH9D.
\textsuperscript{22} Marissa Alcala et al., Financing Subsea Cables in Latin America, NORTON ROSE FULBRIGHT (June 16, 2020), https://perma.cc/QPG9-QKZW.
\textsuperscript{23} Sam Shead, Google Is Building a Huge Undersea Fiber-Optic Cable to Connect the U.S. to Britain and Spain, CNBC (July 28, 2020), https://perma.cc/T3GE-N363.
\textsuperscript{24} See generally ISAAC GEISLER ET AL., DEPT OF SYS. ENG’G & OPERATIONS RES., GEO. MASON UNIV., DESIGN OF A TRANSOCEANIC CABLE SYSTEM (2015), https://perma.cc/7WPB-HRPE.
attempts.\textsuperscript{25} Third-party and private actors, however, are still considered a risk to submarine cables. When four cables linking Europe and the Middle East were simultaneously damaged, many officials and commercial operators alleged private actors had cut the cables.\textsuperscript{26} Although more sophisticated technology is required to hack a cable compared to destroying one, the threat of terrorists hacking a submarine cable remains even if not manifest to date.\textsuperscript{27}

In general, the process by which intelligence agencies tap into cables is highly secretive. There are some indications, however, as to how it is done. Some reports indicate states use specially designed submarines equipped with devices to splice into cables. In this “splicing method,” the submarine, having broken through the protective coating, installs listening devices within the fiber optic cable to collect transmitted data.\textsuperscript{28} Some commentators, however, cast doubt on this method due to the possibility of a cable operator detecting a break in data transmission through the cable.\textsuperscript{29} Some reports nevertheless indicate the techniques are sophisticated enough to not alert cable operators even when external damage to the cable is already done.\textsuperscript{30} The possibility of damage to the cable or service interruption through splicing is important in the global regulatory regime for cable protections, as will be discussed at length in Section VI.

Other hacking methods appear less obtrusive. Some intelligence analysts have speculated operators gain access to a cable at landing stations—stations fitted with signal boosting equipment and cable access features—in order to install intercept probes that capture the fiber optic light signal and make a copy of it.\textsuperscript{31} This method, and a similar one involving creating a slight curvature within the cable to siphon off data as it passes through the curve, may not alert an operator that hacking has occurred because the cable does not witness a service interruption

\textsuperscript{25} Griffiths, supra note 16.

\textsuperscript{26} Investigators ultimately determined a ship’s anchor was to blame for at least one of four simultaneously damaged cables connecting the Middle East and Europe, but many at the time alleged the cables were damaged by private actors and conspiracy theories still abound. Lily Hay Newman, \textit{Cut Undersea Cable Plunges Yemen Into Days-Long Internet Outage}, WIRED (Jan. 13, 2020), https://perma.cc/C4AF-CLBG; Kim Zetter, \textit{Undersea Cables Cut: 14 Countries Lose Web – Updated}, WIRED (Dec. 19, 2008), https://perma.cc/3TGK-EUHH.


\textsuperscript{28} New Nuclear Sub Is Said to Have Special Eavesdropping Ability, N.Y. TIMES (Feb. 20, 2005), https://perma.cc/KDM9-683P.


\textsuperscript{30} Meghan Neal, \textit{How to Hack the Backbone of the Internet}, VICE (Oct. 31, 2013), https://perma.cc/6MWG-CF3E.

\textsuperscript{31} See Khazan, supra note 13.
seen in splicing.\textsuperscript{32} While these methods involve some damage to the cable, they may not be easily identified or protected against even by wary states. Generally, while the method used may differ, most methods involve some degree of damage to the submarine cable and some degree of interference with a cable’s data transmission.

III. THE SHIFTING DIALOGUE AROUND SUBMARINE CABLE HACKING

This Section discusses why submarine cable hacking is a pressing and ripe area for solutions within public international law. As noted above, most of the world’s global powers, particularly the U.S., China, and Russia, enjoy the ability to hack into one another’s cables and may want to reserve that ability. This may indicate few states would be interested in developing norms or international public law against submarine cable hacking. Indeed, the lack of a global convention against peacetime hacking may signal a lack of state interest in curbing this behavior. The ground, however, may be shifting.

First, the volume of information, and in turn sensitive information, that passes through submarine cables is growing. Presently, submarine cables carry 95% of all international communications.\textsuperscript{33} As countries continue to develop and as crises like COVID-19 require more work and entertainment to be done remotely, global demand for internet bandwidth rises.\textsuperscript{34} In turn, submarine cable use will only increase. Global consumer IP traffic is expected to rise from 212 Exabytes per month in 2020 to 333 Exabytes per month in 2022.\textsuperscript{35} Submarine cable bandwidth and traffic are expected to rise by 40% by 2022.\textsuperscript{36} In 2020 alone, global submarine cable bandwidth rose by 35%.\textsuperscript{37} Correspondingly, the submarine cable market is expected to grow at approximately 11% by year from 2020 to 2025 increasing the market’s total value from $10.3 billion to $22 billion.\textsuperscript{38} The need for cable protection then increases as the value and flow of data increases through submarine cables.

\textsuperscript{32} Id.

\textsuperscript{33} Submarine Cables, NAT’L OCEANIC & ATMOSPHERIC ADMIN. (NOAA), https://perma.cc/2YKK-DTS3.

\textsuperscript{34} Paul Brodsky, Let’s Just Say Demand Is Thriving in the Global Bandwidth Market, TELE GEOGRAPHY DIG. (May 1, 2020), https://perma.cc/B245-M8FE.


\textsuperscript{36} Alex Vaxmonsky, New Subsea Cable Architectures Are Carrying the World’s Traffic, EQUINIX (Mar. 16, 2020), https://perma.cc/9GHL-WD9A.


\textsuperscript{38} Submarine Cable System Market Worth $22.0 Billion by 2025, PR NEWSWIRE (Feb. 27, 2020), https://perma.cc/7QTT-LM33.
Second, while covert and secretive, state hacking and cyber operations only appear to be increasing in scope and frequency. In 2013, leaks revealed the British intelligence service the Government Communications Headquarters (GCHQ) was tapping dozens of fiber optic cables processing over 600 million telephone events and 21 Petabytes of data each day.\(^\text{39}\) In 2015, American and NATO security forces became concerned with Russian submarines and spy ships increasingly patrolling areas near American submarine cables.\(^\text{40}\) And the threat of Russian activity has only increased. Russia has built out its submarine fleet,\(^\text{41}\) and a number of these submarines are claimed to be equipped with cable hacking capabilities.\(^\text{42}\)

This buildout of state capabilities to hack submarine cables has shifted states’ behavior with respect to submarine cables and hacking generally. Out of concern of Chinese hacking attempts, as mentioned above, U.S. regulators prevented the Pacific Light Cable Network connecting the U.S. and Hong Kong from going live.\(^\text{43}\) This was seen as a dramatic move because Google and Facebook had already spent over $300 million to construct the cable.\(^\text{44}\) In the commercial context, the U.S. and China agreed in 2015 to halt government support for cyber theft of corporate secrets or business information.\(^\text{45}\) In crafting the treaty, the U.S. asserted the two countries would together seek “international rules of the road for appropriate conduct in cyberspace” out of a growing concern around an arms race in cyber operations and hacking.\(^\text{46}\) While not the same as submarine cable hacking, the commercial hacking détente between China and the U.S. indicates some shift in behavior around state-sponsored hacking. The international community may be heading toward a similar watershed moment for crafting treaties around submarine cable hacking given the buildout of state hacking capabilities.

Third, citizens and states are increasingly aware of hacking and intelligence gathering conducted through submarine cables. Expressions of outrage against these methods have increased accordingly. After Edward Snowden revealed the extent of spying on U.S. citizens, thousands took to the streets to protest against

\(^{39}\) MacAskill et al., supra note 11.


\(^{43}\) Agence-France Presse, Pacific Data Cable Not Safe from China if Hong Kong Included, Says US, THE GUARDIAN (June 17, 2020), https://perma.cc/HWY2-BLAB.

\(^{44}\) Mark Harris, Google and Facebook Turn Their Backs on Undersea Cable to China, TECHCRUNCH (Feb. 6, 2020), https://perma.cc/D3YQ-55H8.

\(^{45}\) David E. Sanger & Steven Lee Myers, After a Hiatus, China Accelerates CyberSpying Efforts to Obtain U.S. Technology, N.Y. TIMES (Nov. 29, 2018), https://perma.cc/KB46-K7SG.

\(^{46}\) Id.
government surveillance.\textsuperscript{47} Human rights watch groups and the media continue to monitor and critique civilian surveillance and spying efforts, and those criticisms have only increased in recent years. The U.N. Human Rights Office of the High Commissioner has produced annual reports related to the right to privacy in the digital age and has advocated for greater recognition of the right to privacy against broad surveillance.\textsuperscript{48} As citizens, NGOs, and political bodies increasingly advocate for protections for the right to privacy, states will increasingly shift their behavior to cooperating around greater privacy protections out of fear of losing the favor of the electorate.

Fourth, cables are not capable of being monitored like other military or commercial assets. Due to their length stretching hundreds of miles in the open ocean and the number of cables traversing the sea, states would need to expend unconscionable resources to patrol for surface ships and submarines that threaten cables. While cable operators are able to observe real-time widespread disruptions in data service, sophisticated hacking agents are supposedly able to splice into submarine cables without alerting cable operators.\textsuperscript{49} To intercept cable hacking operators, a state would then need a nearby ship, or perhaps even submarine, capable of detecting and intercepting a hacking submarine. Indeed, it is difficult to fathom the resources required to patrol the 5,000 or so miles from Los Angeles to Tokyo across the Pacific for one cable let alone dozens of cables. Accordingly, spying attempts on cables are likely to succeed. NATO and British intelligence officers have acknowledged fears of Russian cable hacking in the Atlantic have grown because states cannot constantly patrol for hacking attempts.\textsuperscript{50}

Because states are unable to fully patrol against submarine hacking attempts, states may want additional tools in their foreign policy toolbox to address possible hacking attempts. As the danger posed by hacking grows and because the resources required to patrol against hacking are so immense, states will need to explore alternative means to protect cables and their sensitive data, which may include recognizing liability for hacking. By recognizing grounds for liability against submarine cable hacking, states can obtain a tool for enforcement against rogue actors when the costs and benefits are in their favor.


\textsuperscript{49} For attempts to solve this problem and a description of the technical requirements involved, see Lijuan Zhao et al., \textit{On-Line Monitoring System of 110 kV Submarine Cable Based on BOTDR}, 216 SENSORS & ACTUATORS 28 (2014); Ye Yincan et al., \textit{Submarine Cable Project Management and Maintenance Monitoring Information Systems, in Submarine Optical Cable Engineering} 259 (Ye Yincan, Jiang Xinmin, Pan Guofu, Jiang Wei eds., 2018).

\textsuperscript{50} Could Russia Cut Undersea Communication Cables?, BBC (Dec. 15, 2017), https://perma.cc/XX95-7X7M.
Fifth, while the U.S., China, and Russia, among others, may want to continue participating in hacking operations, not all states participate in hacking and not all states will want to continue to allow hacking to persist on the global stage. Landlocked states and states with less robust submarine military presences do not have the same incentives to allow submarine hacking to continue because they cannot as easily participate. Further, these states may be incidentally damaged by hacking attempts against U.S. or Russian submarine cables because their information flows through those same cables to other states. These states may then want protections against submarine hacking regardless of whether global powers, like the U.S. and China, want the practice to continue.

The geopolitical landscape and incentives around protections against cable hacking thus appear to be shifting. Accordingly, this Comment turns to international public law as a potential way to curb hacking behavior. In the following Section, this Comment examines the protections currently afforded to cables under public international law. Subsequently, this Comment evaluates current scholarly thought on solutions within the public international legal system before proposing a novel solution to the problem of submarine cable hacking.

IV. INTERNATIONAL LAWS REGULATING SUBMARINE CABLES

This Section offers an overview of the history of submarine cable protections and an overview of current submarine cable protections in public international law. The history of submarine cable protection offers strong insight into how current protections were developed. By understanding how cable protections changed over time, this Comment helps better understand the norms around cables outside of the language of international conventions. Further, the history of submarine cables can inform our understanding of the protections dispute resolution bodies are willing to extend to cables when evaluating international law.

A. The 1884 Convention for the Protection of Submarine Telegraph Cables

International protections for submarine cables began, surprisingly enough, in the 1880s with the dawn of undersea telegraph wires. Due to threats from fishermen and pirates who accidentally or intentionally severed telegraph cables, 27 states joined together to create the 1884 Convention for the Protection of

---


52 For example, the first submarine cable crossing the English Channel was cut by a fisherman who thought he discovered a new species of seaweed. Eric Wagner, *Submarine Cables and Protections Provided by the Law of the Sea*, 19 MARINE POLICY 127, 128 (1995).
Submarine Telegraph Cables. Principally, the 1884 Convention was designed to protect cables against willful or negligent damage to cables that may interrupt or obstruct telegraph signals.

The 1884 Convention, however, was limited in scope and application. Rather than develop a comprehensive international court to handle submarine cable disputes or violations of the convention, the 1884 Convention required states to create their own national regulations to protect submarine cables. Many signatory states, such as Canada, never implemented national laws in accordance with the Convention. Other participating states, like China, never signed the Convention and similarly have not developed comprehensive domestic laws in accordance with the Convention’s requirements. Where states did implement domestic laws under their Convention obligations, those protections were generally piecemeal and weak. For example, the U.S. enacted the 1888 Submarine Cable Act in response to the 1884 Convention, but fines under the statute are so small the U.S. Coast Guard does not pursue violators. There is not a single record of a criminal charge under the statute and civil fines are capped at $5,000. The signing countries in 1884 could not have anticipated the emergence of internet submarine cables or hacking into these cables to pilfer vital information. The 1884 Convention, however, may offer some recourse for this sort of misbehavior. Article II provides it is a punishable offense to “break or injure a submarine cable, willfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication.” Splicing or tapping into submarine cables requires some damage to the cable and some degree of service interruption to intercept transmitted data. Article II may then apply to submarine cable hacking.

Nevertheless, the 1884 Convention may be limited in its protective ability. First, the Convention requires states to implement domestic regimes protecting cables. Because domestic jurisdiction over foreign nationals is limited, especially on the high seas as will be discussed, these protections are limited in reach.

53 Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884 [hereinafter 1884 Convention].

54 Id. art. II (“It is a punishable offence to break or injure a submarine cable, willfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication, either wholly or partially, such punishment being without prejudice to any civil action for damages.”).

55 Id. art. XII (“The High Contracting Parties engage to take or to propose to their respective legislatures the necessary measures for insuring the execution of the present Convention, and especially for punishing, by either fine or imprisonment, or both, those who contravene the provisions of Articles II, V and VI.”).

56 Id. art. 17.

57 47 USC § 21 et seq.

58 Wagner, supra note 52, at 135.

59 1884 Convention, supra note 53, art. II.
Further, because Article II is limited solely to “telegraphic wires,” it is not clear whether damage to submarine internet cables portends liability under the Convention. While many modern cables have the ability to transmit telegraphs, most are fiber optic cables and therefore may be outside the convention’s scope. And unlike subsequent conventions, the 1884 Convention did not create a tribunal or dispute resolution body to handle these issues. States then are reliant on other states’ domestic regulations for protecting submarine cables. Regardless of its limited applicability to hacking, however, the 1884 Convention pioneered protections for submarine cables, the spirit of which have since been largely incorporated in modern treaties dealing with the high seas.


Following the 1884 Convention, the international community incorporated further protections for submarine cables in broader treaties related to the high seas. In 1958, the Geneva Conventions on the Continental Shelf and the 1958 Convention on the High Seas incorporated portions of the 1884 Convention. Namely, protections of cables from willful or culpably negligent damage and indemnification obligations for other cable owners were incorporated in these later conventions from the 1884 Convention.60

Notably, the 1958 High Seas Convention additionally codified the freedom to lay cables as a high seas freedom, expanding the protections offered by the 1884 Convention.61 Specifically, Article II holds “the high seas being open to all nations, no State may validly purport to subject any part of them to its sovereignty” and the “freedom to lay submarine cables” is one such recognized right.62 Article XXVI further affirms “States shall be entitled to lay submarine cables and pipelines on the bed of the high seas.”63 This Convention also introduced more limited rights on the continental shelf and territorial waters, a distinction to be discussed at length.64 This Convention was the first to establish a general freedom to lay submarine cables which has become central to modern treaty obligations with respect to submarine cables.

Following these intermediary conventions, in 1982 the U.N. Convention on the Law of the Sea (UNCLOS), the contemporary convention for the law of the

62 Id. art. II.
63 Id. art. XXVI.
64 Id.
Submarine Cable Hacking and Law of the Sea

Jason Petty

sea, was created.\textsuperscript{65} UNCLOS was devised over extensive negotiations to replace the 1958 conventions with a more comprehensive framework of laws and obligations.\textsuperscript{66} Generally speaking, UNCLOS divides the seas into three sections, each corresponding to distinct rights and duties of states: territorial seas, the exclusive economic zones (EEZ) and continental shelves, and the high seas. UNCLOS incorporated many of the same rights and duties with respect to submarine cables as the 1884 Convention and the 1958 conventions. To understand the rights of states under UNCLOS, this Comment will review states’ rights with respect to submarine cables in each of these three territorial zones.

A state’s territorial seas are the sea, including its bed and subsoil, for the area up to 12 miles from a state’s shores.\textsuperscript{67} States maintain sovereignty over the territorial sea and can impose their own laws over this area, including with respect to submarine cables.\textsuperscript{68} If foreign actors break the coastal state’s laws in its territorial waters, those actors would be subject to the coastal state’s jurisdiction under UNCLOS. If a foreign state hacked into or damaged the coastal state’s submarine cables within its territorial waters, those foreign hackers would be subject to the coastal state’s laws against submarine cable hacking or damage to submarine cables. For this reason, among others, states do not engage in hacking in other states’ territorial waters. Even if they did, however, most states have not crafted any protections or regulations on submarine cables within their territorial waters.\textsuperscript{69} Where states have crafted protections for intentional or negligent damage to cables, those protections are rarely enforced and are often quite weak.\textsuperscript{70}

In the second zone, coastal states can claim the EEZ and continental shelf up to 200 nautical miles past the borders of the state’s territorial seas.\textsuperscript{71} The delimiting of the precise boundaries of this zone is somewhat complicated however.\textsuperscript{72} Within this area, states enjoy certain rights to exploit natural resources or explore.\textsuperscript{73} Regardless of these rights, other states maintain general rights to

\begin{footnotesize}
\begin{enumerate}
\item UNCLOS, INT’L UNION FOR CONSERVATION OF NATURE, https://perma.cc/K8ZT-2UXV. For more information on the development of UNCLOS, see generally Myron H. Nordquist, et al., UNCLOS 1982 COMMENTARY (Myron H Nordquist et al. eds., 2012).
\item UNCLOS, supra note 65, art. II.
\item Id. art. XXI; Burnett et al., supra note 60, at 76.
\item Id at 287.
\item UNCLOS, supra note 65, art. L.VII.
\item UNCLOS, supra note 65, art. LVI.
\end{enumerate}
\end{footnotesize}
“other internationally lawful uses of the seas related to those freedoms” which can extend to submarine cables.\textsuperscript{74} UNCLOS also extends particular freedoms around submarine cables including the ability to lay submarine cables and pipelines.\textsuperscript{75} While not explicitly mentioned, this freedom likely also includes the ability to operate, repair, and inspect previously laid submarine cables.\textsuperscript{76}

States, however, do not have unfettered access to the EEZ and the continental shelf in the name of cable installation or repair. UNCLOS requires states exercising these rights to “comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law.”\textsuperscript{77} While this language is broad, this allowance permits coastal states to restrict foreign states’ activities in furtherance of their right to exploit natural resources in the EEZ or continental shelf or their right to explore the area. In practice, however, this allowance is largely curtailed, and states broadly enjoy States therefore broadly enjoy the freedom to lay submarine cables in the EEZ.

UNCLOS provides similar protections for submarine cables in the EEZ as in territorial waters, though jurisdiction is less clear. Again, similar to territorial waters, while states are required to “adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence… be a punishable offense,”\textsuperscript{78} most states have not done so.\textsuperscript{79} Unlike territorial waters, however, coastal states’ regulations in the EEZ or the continental shelf do not apply to foreign nationals who intentionally break or damage cables.\textsuperscript{80} This means states in the EEZ and the continental shelf can only hold their own citizens that injure cables liable under their domestic laws. While some states have made novel legal arguments about submarine cables as being in a protected zone of exploitation,\textsuperscript{81} the majority of states accept domestic jurisdiction does not extend to cables in the EEZ.\textsuperscript{82} In the instance of hacking, this would mean coastal states could only address domestic hackers, which, while

\textsuperscript{74} Id. art. LVIII.
\textsuperscript{75} Id. art. LXXXVIII.
\textsuperscript{76} See id. art. LXXIX (referring to the “laying or maintenance” of submarine cables and “repairing” existing cables.”); see also Burnett et al., supra note 60, at 81.
\textsuperscript{77} UNCLOS, supra note 65, art. LVIII.
\textsuperscript{78} Id. art. LXIII.
\textsuperscript{79} Beckman, supra note 69, at 288.
\textsuperscript{80} Id.
\textsuperscript{82} Beckman, supra note 69, at 288.
potentially useful for private actors, does not likely apply to the majority of hacking incidents, which are largely committed by foreign governments.

The high seas are the third zone described by UNCLOS. The high seas are defined as “all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State.” The high seas are canonically regarded as beyond the reach of states’ national jurisdiction. Accordingly, the high seas are the largest sea area and do not offer any domestic protections against hacking attempts.

The high seas, although beyond the reach of any state, are subject to applicable international treaties including UNCLOS. Broadly, the high seas are reserved for “peaceful purposes.” If hacking was considered an act of aggression, states would not enjoy that freedom on the high seas. Similarly, acts considered illegal under international treaties or conventions, like slave trading for example, would not be a permissible use of the high seas. Presently, as discussed in Section V, submarine cable hacking is considered a peaceful activity and not illegal under any international convention.

UNCLOS does not offer many protections for submarine cables on the high seas. Under UNCLOS, states maintain the freedom to lay submarine cables but must exercise this freedom in recognition of other states’ exercise of high seas freedoms. Similar to requirements for the EEZ, states are obligated under UNCLOS to craft laws and regulations that require their citizens to compensate cable owners for damage they caused to cables or pipelines. Many states have not designed laws to meet this obligation and those that have generally involve paltry compensatory payments. Again, like the EEZ, these regulations would not extend to foreign nationals on the high seas under UNCLOS.

Unlike the 1884 Convention, UNCLOS included a dispute resolution framework for conflicts between states. The International Tribunal for the Law of the Sea (ITLOS) serves as a binding dispute resolution mechanism where states are unable to reach a peaceful settlement. ITLOS has jurisdiction over “any dispute concerning the interpretation or application of this Convention which is submitted to it in accordance with this Part” including failing to comply with

---

83 UNCLOS, supra note 65, art. LXXXVI.
84 Id. art. LXXXIX (“No state may validly purport to subject any part of the high seas to its sovereignty.”).
85 Id. art. LXXXVIII.
86 Id. art. CXII.
87 Id. art. LXXXVII.
88 UNCLOS, supra note 65, art. CXIII.
89 Beckman, supra note 69, at 288; see also Wagner, supra note 52, at 135.
convention obligations. Where states have not implemented their treaty obligations, ITLOS can compel states to specifically perform or craft regulations under their UNCLOS requirements.

States are able to select ITLOS for the settlement of disputes at any time through means of written declaration, however, states must fully exhaust domestic remedies before applying for resolution through ITLOS. Therefore, if a foreign state hacks into a state’s submarine cable in its territorial waters, the injured state must seek liability under its domestic laws first where available.

ITLOS can apply the international law under UNCLOS or “other rules of international law not incompatible with this Convention.” This extends to other human rights treaties or accepted international conventions. Generally, ITLOS handles cases involving foreign sailors held without cause, but the Tribunal has exerted its jurisdiction over any number of maritime issues. As discussed in Section VII, ITLOS may be a useful vehicle for arbitrating disputes between states around submarine cable hacking and the international right to privacy.

Because UNCLOS does not offer explicit protections for cables from hacking on the high seas, the puzzle then is how to create enforcement mechanisms and norms against hacking. Because domestic jurisdiction can only be asserted in territorial waters and most states do not have robust domestic laws, trying to enforce cable protections through national laws seems impractical. Indeed, as will be discussed, scholars have consistently decried the absence of domestic protections for submarine cables. In the following Section, this Comment will explore whether other conventions in international law, rather than solely the laws of the sea, protect against submarine cable hacking. This Comment then explores possible solutions to this problem of liability using ITLOS as a possible avenue for liability.

91 UNCLOS, supra note 65, art. CCLXXXVII.
92 Id. art. CCXCV.
93 Id. art. CCLXXXVIII.
95 For example, ITLOS adjudicated the maritime boundary between Mauritius and Maldives in the Indian Ocean. See Decision Concerning Delimitation of the Maritime Boundary Between Mauritius and Maldives in the Indian Ocean (Mauritius v. Maldives), Case No. 28, Special Agreement and Notification of 24 September 2019. In another case, ITLOS provided an advisory opinion for the minimum access conditions and exploitation of fishery resources for the Sub-Regional Fisheries Commission. See Request for Advisory Opinion Submitted by the Sub-Regional Fisheries Commission, Advisory Opinion, 2 April 2015, ITLOS Reports 2015, Case No. 21.
V. INTERNATIONAL NORMS WITH RESPECT TO HACKING

This Section describes the international conventions and framework with respect to cyber operations and hacking. Generally, hacking and cyber surveillance are regarded as peacetime activities and are not limited by any international treaties or conventions. The methods employed in pursuit of these goals, however, may be deemed problematic by various conventions. This Section explores the limits of hacking techniques and cyber surveillance and discusses how shifting norms around the right to privacy may change international consensus on the viability of some surveillance tactics.

At present, there is no international framework for hacking offenses or cyber operations. While previous conventions like the Budapest Convention on Cybercrime\(^96\) tried to harmonize national laws with respect to cyber operations and provide for mutual assistance in investigating and prosecuting cyber operations,\(^97\) there is no international legal framework for cyber offenses or hacking.\(^98\)

In response to lacking a global framework, a group of preeminent international law scholars and practitioners created the Tallinn Manual\(^99\) to describe the legal norms and regulations around cyber operations and hacking.\(^100\) The Tallinn Manual is not an international convention and is not binding. Rather, the document serves as an expression of opinion of various experts versed in these topics. Accordingly, it should be considered a reflection of the law at the time of writing and not a limiting or normative statement of the law. The Tallinn Manual is also limited in scope and incorporates public, but not private or domestic, international law.\(^101\) The document, however, can provide a general insight into how the international community views current restrictions on cyber operations on the high seas and whether hacking is indeed a “peaceful use” of international waters.

A. General Cyber Operations on the High Seas

According to the Tallinn Manual, the primary basis for liability for cyber activities is territorial. Much like a state has jurisdiction over damage to cables in

---

98 Id. at 428–30.
100 Id. at 2.
101 Id. at 4.
its territorial seas, states have jurisdiction over cyber activities or hacking that occur within their territory or their territorial waters.\textsuperscript{102} The experts note tapping a state’s submarine cables in its territorial waters violated its sovereignty.\textsuperscript{103} States then have jurisdiction over hacking attempts within their territorial waters.

Tapping or hacking activities outside of a state’s territorial waters do not offer the same legal recourse. Like cable damage under UNCLOS, the EEZ and the continental shelf is subject to a complicated legal framework for cyber operations jurisdiction. Generally, if cyber operations are carried out for “peaceful purposes” and maintain “due regard to that State’s rights and duties in the zone,” they are permitted in the EEZ.\textsuperscript{104} And so long as these operations do not violate “other international legal norms... governing the circumstances,” they do not constitute a violation of state sovereignty in the EEZ.\textsuperscript{105} Hacking therefore in the EEZ, when it does not violate other international legal norms, is permissible.

On the high seas, states have even fewer rights or protections against hacking. Cable hacking attempts on the high seas do not constitute a violation of the hacked state’s sovereignty.\textsuperscript{106} Indeed, background intelligence gathering on the high seas during peacetime has long been considered legal without much debate in the international community.\textsuperscript{107} While hacking or tapping constitute more invasive techniques than radio or sonar surveillance, which have both been long accepted, most scholars believe there is no difference by conducting more “active” intelligence gathering via hacking.\textsuperscript{108} As in the EEZ, however, human rights violations that occur during cyber operations on the high seas are not permissible according to the Tallinn Manual.

As typified by the above, norms around cyber operations have either not solidified or are highly permissive of cyber operations on the high seas. Because these norms are absent, there is insufficient state practice and public international

\begin{footnotesize}
\begin{tabular}{l}
\hline
102 Id. at 51. \\
103 Id. at 257. \\
104 Id. at 233 (“In particular, employing a submarine or unmanned underwater vehicle to tap in territorial or archipelagic waters is inconsistent with the navigational regime of innocent passage as submarines are required to transit on the surface.”) \\
105 Id. at 257. \\
108 TALLINN MANUAL, supra note 99 at 257. But see Davenport, supra note 29, at 105 (“Whether UNCLOS can be used to address the mass surveillance carried out through the tapping of undersea cables is not entirely clear... Such surveillance does not fall within conventional perceptions of military activities/intelligence gathering at sea, which as mentioned above, is targeted, and aims at enhancing knowledge of the marine environment and/or the military capabilities of other State’s navies.”). \\
\hline
\end{tabular}
\end{footnotesize}
law to conclude cyber espionage is per se banned. Experts, however, agree that cyber operations or hacking may be carried out in a manner that is unlawful. Accordingly, this Comment turns to the consequences of hacking and review whether or not these effects may constitute some form of illegal or prohibited activity under public international law.

B. Incidental Effects of Submarine Cable Hacking: Cable Damage

One incidental effect of submarine cable hacking is damage to the submarine cables as a result of splicing into the cable or damaging the cable in the installation of surveillance devices. As noted above, UNCLOS mandates states craft laws to hold their citizens liable for intentional or negligent damage to submarine cables. These laws, however, are limited in jurisdiction to territorial waters. Experts notably have split as to whether the mere act of tapping cables that results in damage renders it a violation of public international law regardless of location. The majority of experts agreed states engage in these activities at their own risk and can incur liability for incidental damage. Separately, a handful of experts argued that unforeseeable damage from tapping operations would not incur liability. These experts note there is no settled case law as to whether incidental damage from cyber operations would be deemed foreseeable or intentional.

This question of liability for damage is nonetheless important. By being able to hold foreign states liable for damage incurred as a result of hacking, states can shift the cost-benefit calculus of hacking attempts by requesting damages. While this may not wholly eliminate submarine cable hacking, potential liability for damage may reduce overall hacking activity levels. It typically costs millions of dollars to repair damage to the actual cable. The economic costs associated with a down cable are hard to estimate but the losses can be extraordinary. Somalia lost internet access for three weeks due to cable damage at a cost of $130 million. Even without a total internet outage, increased bandwidth demand and slower data speed as a result of cable interference can wreak huge productivity losses. If a state was held liable for repair costs, or lost productivity, the possible costs

---

109 TALLINN MANUAL, supra note 99, at 169.
110 Id. at 170.
111 Id. at 257.
112 Id.
114 The Economic Impact of Submarine Cable Outages Can Still be Enormous, SUBCABLE WORLD (Aug. 21, 2017), https://perma.cc/TF2F-QQ7R.
associated with hacking would rise and overall hacking activity levels may fall in turn.

C. Incidental Effects of Submarine Cable Hacking: Violations of the International Right to Privacy

A second incidental effect of submarine cable hacking is the violation of citizens’ privacy by harvesting electronic data. Because hacking operators cannot control what data they siphon off, hackers will inevitably intercept citizens’ private communications and data in their operations, unless the cable is a dedicated military cable. This violation of privacy is significant because, as the Tallinn Manual experts noted, cyber operations may not be conducted in an unlawful manner. While controversial, the international right to privacy would likely be violated by these operations. Accordingly, this Comment next reviews the international right to privacy, its implications for submarine hacking, and the debate around its scope.

A number of conventions have enumerated an international right to privacy. The Universal Declaration of Human Rights introduced this principle in Article 12 that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.” The International Covenant on Civil and Political Rights (ICCPR) enumerated this right in Article 17 that “no one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence.” At its core, this right protects a “private sphere” of autonomous liberty and development that cannot be intruded on without permission by state actors, individuals, or corporations. This right has been extended to include protection of personal communications and data. The scope of this right is clear for intelligence gathering or hacking within the territory of a state. Any arbitrary electronic interception that takes place within a nation’s borders or involves that nation’s citizens violates the international right to privacy.

---

115 TALLINN MANUAL, supra note 99, at 170.  
117 Universal Declaration of Human Rights, supra note 116, art. 12.  
118 ICCPR, supra note 116, art. 17.  
The scope of this right is less clear for intelligence gathering on foreign states or foreign nationals. The U.S. has presented the most limited interpretation of the right to privacy in this context. According to the U.S., the right only attaches to citizens within a state’s territory and subject to its jurisdiction. Therefore, foreigners and citizens located abroad do not enjoy the right to privacy for U.S. surveillance activities. In the context of U.S. submarine cable hacking, this implies only U.S. citizens enjoy the right to privacy, and they only enjoy this right for submarine cable hacking conducted in the U.S.’s territorial waters. The majority of states in the international community hold the right is broader. According to the majority opinion, states “respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.” While the precise contours of the ICCPR are still debated, a number of international bodies have coalesced around the principle that a state’s obligations are maintained for foreigners and citizens alike. Under this interpretation, citizens enjoy the right to privacy for submarine cable hacking regardless of where the hacking takes place or what state conducts the hacking.

The debate around the scope of this right centers on whether a state exercises “effective control” over a person or territory in determining jurisdiction. As discussed earlier, the high seas are beyond the territorial reach of any particular state. Therefore, questions of “effective control” become more pressing as scholars consider whether a state exercises effective control over cyberspace through cables located on the high seas. This question is hotly debated. Some scholars have noted limiting effective control to solely physical territory may result in illogical results as it is not clear where cyber communications are physically located when conducted over the internet. Other scholars have argued a “virtual control,” where states are liable for those citizens whose communications it has control over, is more appropriate. In the context of submarine cables, this may be a more appropriate approach as it would ensure the equal treatment of individuals regardless of physical location, which matches the traversing and multi-state nature of submarine cables.

An international right to privacy nevertheless remains controversial. Some scholars insist an application of a universal right to privacy may undermine

---

122 Bignami, supra note 119, at 4.
125 Bignami, supra note 119, at 5.
126 Humble, supra note 124, at 13.
domestic protections against surveillance currently in place. These scholars argue a more universal definition may reduce the obligations afforded domestic citizens under current cyber privacy laws. Other scholars have argued the right to privacy is socially defined and therefore changes from context to context or society to society. Accordingly, the scope of the right at issue may not extend to protections against state surveillance for defense purposes depending on the social definition and context.

Regardless of the ongoing debate, the recognition and scope of the right to privacy appears to be shifting, as discussed in Section III, toward a greater recognition of the right to privacy. Scholars have noted international human rights cases increasingly find states’ human rights obligations follow them in acting abroad. As this recognition expands, mass surveillance is increasingly considered “arbitrary” and in contravention of the ICCPR. In a 2015 groundbreaking case, ten U.K. NGOs filed an action with the European Court of Human Rights (EChTR) arguing the U.K.’s mass surveillance system violated the right to privacy. The EChTR agreed noting the surveillance scheme’s arbitrary intelligence collection violated the right to privacy under the European Convention on Human Rights. This case is significant because it specifically addressed bulk surveillance conducted through fiber optic cables. On appeal, the EChTR dismissed the case for failing to seek appropriate domestic remedies. Nevertheless, the court’s initial ruling reflects a concerted shift in behavior toward greater privacy rights recognition. Similarly, in 2020, the Court of Justice of the European Union (CJEU) held indiscriminate government mass surveillance

---

129 Ronald J. Krotoszynski, Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law, 39 DUKE L.J. 1398, 1401–02 (1990) (where privacy is defined as “a realm of individual autonomy in recognized and accepted social contexts” that is “defined in relation to a particular society at a particular point in time”).
131 Id. at 31–52.
134 10 Human Rights Organisations v. United Kingdom, supra note 132.
violated E.U. regulations for privacy and data protection. The CJEU held surveillance should be conducted only for what is strictly necessary for national security purposes. These shifts are representative of general shifts in recognition of the right to privacy.

While cooperation for developing protections and harmonization of definitions for privacy in the internet age is ongoing, it is apparent that the right to privacy exists and is increasingly recognized in international public law. While this Comment cannot cure all the debates around the right to privacy, the solution described in Section VII provides a novel exploration of the right to privacy in cyber space that may help advance discussions elsewhere.

VI. THE LAY OF THE LAND OF CURRENT SCHOLARSHIP

This Section explores current scholarship on submarine cable protections and submarine cable hacking. This Section serves to provide context for the novelty of the solution offered in Section VII and discuss how scholars interpret currently proposed avenues for liability for submarine hacking. Scholars currently focus on protections for incidental or intentional damage to cables in order to raise the relative costs associated with hacking. Scholars, however, are pessimistic about current domestic protections toward submarine cables and generally accept submarine cable hacking as part of the international landscape. Notably, scholars have previously not used the right to privacy to frame the debate around submarine cable hacking and have not used dispute resolution mechanisms, like ITLOS, for resolving these issues.

As a summary of prior Sections, UNCLOS does not explicitly place restrictions on peacetime intelligence gathering or cyber operations on the high seas or in the EEZ. Because the high seas are not subject to any state’s domestic jurisdiction and the EEZ is subject to very limited jurisdiction, domestic laws against hacking or damage to submarine cables do not apply in these areas. Further, there is no international treaty or convention that restricts or bans cyber operations generally. Experts agree that “the bottom line is that there is no clear prohibition against the physical tapping of fiber optic cables in the EEZ [or the high seas] to be found in UNCLOS” or other international treaties.

While states generally have the freedom to conduct cyber operations on the high seas, if the method of those operations violates other international treaties or

137 Id.
139 Davenport, supra note 29, at 106.
140 TALLINN MANUAL, supra note 99, at 257.
laws, those methods are subject to liability. Scholars have therefore turned to UNCLOS Article 112 and Article 113, which describe the freedom to lay submarine cables and the obligation of states to create domestic protections for cables, as possible protections for cables. In their analyses, these scholars focus on incidental damage to submarine cables, the first indirect effect from cable hacking.

Scholars, however, are pessimistic about using Article 112 or Article 113 to protect submarine cables. While UNCLOS requires states to have domestic laws to punish intentional or negligent damage of undersea cables, most states have not imposed these regulations. For example, Canada does not have any legal protections for cables once laid. While Canadian law requires permits to lay cables and conduct periodic environmental impact reports, cable companies do not have any legal recourse under Canadian law for cables damaged by other parties. The U.N. General Assembly has even called on states to implement protections under Article 113 due to the paucity of available domestic protections against damage to cables.

And where states do have regulations, those protections are generally weak and rarely enforced. For example, U.S. federal law states parties who intentionally damage cables are subject to a maximum fine of $5,000. Repair costs far exceed this figure. Other states similarly have weak enforcement regimes. In Australia, the penalty for intentional damage of submarine cables is AUS$2,000 or imprisonment for 12 months while the penalty for negligent damage is AUS$1,000 or imprisonment for 3 months. With such insignificant protections, there are few incentives for cable owners or regulators to seek enforcement. Accordingly, there are no documented instances of prosecution under either the U.S. or Australian laws.

---

141 Davenport, supra note 29, at 106 (“Within the EEZ, the discussion above on the controversy surrounding the legality of intelligence gathering activities would also apply—the bottom line is that there is no clear prohibition against the physical tapping of fiber optic cables in the EEZ to be found in UNCLOS.”); TALLINN MANUAL, supra note 99, at 257 (minding “prejudice to the application of other international legal norms,” cable tapping is not per se illegal on the high seas).
142 TALLINN MANUAL, supra note 99, at 257.
143 Scott Coffen-Smout & Glen J. Herbert, Submarine Cables: A Challenge for Ocean Management, 24 MARINE POL’Y 441, 444 (2000).
145 Coffin-Smout & Herbert, supra note 143, at 444.
Submarine Cable Hacking and Law of the Sea

Jason Petty

Scholars and advocates have argued strengthening these domestic protections may offer some relief against hacking. As discussed in the previous Section, by increasing the costs associated with a hacking operation, the associated cost-benefit analysis shifts. Scholars have focused on increasing these protections in the absence of a new international framework against hacking. Tara Davenport noted Article 113 of UNCLOS would apply to damage done through cable tapping but that domestic protections against submarine cable damage are “woefully inadequate” and “not commensurate with the damage resulting from intentional interference.” Zoe Scanlon likewise recognized despite the “assumption underpinning UNCLOS that coastal states would recognize their clear interest in protecting submarine cables,” most states have not enacted legislation protecting cables. This contributes to an ineffective legal regime against cable damage and hacking.

While there is some appetite for bolstering domestic protections, doing so is an incomplete solution. First, the associated penalties would have to be severe in order to change the calculus of hacking states and compensate the injured cable owners. High penalties, however, may result in expensive liability for negligent, non-hacking agents like ship owners who incidentally drop anchor on a cable—the most common cable injury. High penalties may also incentivize states to cheat by refusing to pay damages or prosecute their citizens. Further, these domestic regulations could only assert jurisdiction over the citizens and ships of the regulating state or in offenses committed in its territorial waters. While hacking is easiest closest to land, the activities at issue most often do not occur in territorial waters and most commonly involve foreign actors or states as discussed in Section II.

Scholars, in recognition of these weaknesses, have generally accepted submarine cable hacking as part of the international landscape until further protections can be crafted or norms around cyber operations crystallize against mass surveillance. Scholars, however, have overlooked the second indirect effect of cyber operations on submarine cables: privacy violations. The following section offers a novel solution to the problem of submarine cable hacking by

---

148 Davenport, supra note 29, at 84, 106.


151 Wargo & Davenport, supra note 147, at 256.

152 Griffiths, supra note 16.

153 TALLINN MANUAL, supra note 99, at 257; see also, Davenport, supra note 29.
VII. USING ITLOS TO TRIGGER DISPUTE RESOLUTION: DAMAGE AND PRIVACY SOLUTIONS FOR HACKING

This Section describes the novel solution offered by this Comment with respect to submarine cable hacking. The Section first describes how the binding dispute resolution system under the International Tribunal for the Law of the Sea (ITLOS) likely has jurisdiction over submarine hacking attempts. This Section further argues, contrary to prior scholarly work, the lack of domestic protections for submarine cable hacking benefits the creation of international norms and a regime against cable hacking. This Section then proposes two solutions using ITLOS. First, ITLOS can be used to create an international regime protecting against submarine cable damage. This in turn raises the costs of submarine cable hacking and may lower hacking activity levels. Second, ITLOS can serve as a forum to argue hacking violates the international right to privacy and therefore should not be permitted even on the high seas. This analysis of the right to privacy with respect to submarine cables is novel in current scholarship and contributes to the ongoing debate about the limits of bulk surveillance collection and surveillance protections generally.

A. Jurisdiction Under ITLOS

As a preliminary matter, ITLOS likely has jurisdiction over alleged submarine hacking disputes. As referenced above, under UNCLOS, ITLOS serves as a dispute resolution mechanism between states. The jurisdiction of ITLOS is broad, encompassing “all disputes and all applications submitted to it in accordance with [UNCLOS].” To confer jurisdiction, therefore, states must have a viable link between hacking attempts and UNCLOS.

Under UNCLOS Articles 112 and 113, states have two arguments as to why ITLOS has jurisdiction over submarine cable hacking. First, states can use ITLOS for dispute resolution where other states are not abiding by their obligations to UNCLOS. Article 113 provides states must adopt laws and regulations to punish “breaking or injury” of submarine cables on the high seas “in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications.” States therefore must create domestic liability schemes to hold its citizens liable for damage to or interruption of submarine cables on the high seas. If, for example, a state has not met its UNCLOS Article 113 obligations to have domestic

154 UNCLOS, supra note 65, Annex VI, art. XXI. See generally Treves, supra note 90.
155 UNCLOS, supra note 65, art. CXIII. While fiber optic cables are not strictly telephonic, they are generally presumed to fall under Article 113.
regulations and a foreign state’s cable is damaged, the foreign state can invoke ITLOS to determine the breaching state’s cable liability. Generally, disputes between states about how to handle cable damage would sufficiently link to UNCLOS to confer jurisdiction.\textsuperscript{156}

Second, states can present arguments that protections for cables under UNCLOS are broader than the right to merely lay cables. Article 112 codifies the right for all states “to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf.”\textsuperscript{157} While not stated, it can be assumed states have the freedom to operate these cables on the high seas. If a foreign state were to violate this assumed right of operation, through hacking or cable signal disruption, an injured state may then have grounds for liability under UNCLOS. ITLOS would be a suitable body to address the violation of this right because the tribunal adjudicates the rights and responsibilities of states on the high seas.

Even if Articles 112 and 113 are not compelling enough to justify jurisdiction, ITLOS also has jurisdiction over “any dispute concerning the interpretation or application of an international agreement related to the purposes of [UNCLOS].”\textsuperscript{158} This broad language allows ITLOS to exert jurisdiction over any international treaty that affects or interacts with UNCLOS. While broad, ITLOS usually declines, however, jurisdiction absent some connection to the high seas or a subject matter of UNCLOS. Scholars have noted the specialized nature of ITLOS means the “subject matter of any agreement providing for jurisdiction of ITLOS would probably relate closely to the law of the sea, given the expertise of the judges of ITLOS.”\textsuperscript{159}

For example, in a case involving detained sailors, ITLOS asserted international human rights under other international conventions were at issue. Plaintiffs, however, had to first assert a jurisdictional link to these rights by noting that the detention that led to these violations was sanctioned under UNCLOS.\textsuperscript{160} Similarly, Italy invoked the ICCPR in its complaint to ITLOS to free Italian sailors detained by the Indian government. Italy did not invoke a stand-alone argument for release under the ICCPR but rather paired it with UNCLOS provisions against “prejudice.”\textsuperscript{161} States can similarly invoke ITLOS to clarify the obligations of states to the international right to privacy, as articulated by a number of international

\textsuperscript{156} For discussion of the general jurisdictional requirements of ITLOS, see generally Treves, supra note 90.

\textsuperscript{157} UNCLOS, supra note 65, art. CXII.

\textsuperscript{158} Id. art. CCLXXXVIII.


\textsuperscript{161} Id. at 386–91.
conventions, with respect to UNCLOS. States should then be able to obtain ITLOS jurisdiction under this more general human rights framework.

Before reaching these questions of ITLOS jurisdiction, however, ITLOS may only resolve disputes under UNCLOS “after local remedies have been exhausted where this is required by international law.”162 Subsequently, states subject to hacking must have exhausted domestic remedies before looking to ITLOS. As mentioned above, scholars have frequently noted the paucity of domestic regulations against submarine cable hacking. Many states have not implemented any domestic regulations concerning submarine cable damage, let alone hacking.163 And where those domestic protections do exist, they are often weak relative to the potential damage done by hacking attempts to a cable’s constitution.164 Because domestic protections are not typically available or are insufficient where they are available, states have generally exhausted all domestic remedies.165

And while scholars have criticized the weakness of these domestic protections and frequently recommended instituting stronger domestic regulations, the absence of these regulations actually strengthens the argument for jurisdiction under ITLOS. If domestic regulations were available, states would be obligated to pursue liability under those regulations. Because states have not implemented these regulations or have incredibly weak domestic protections, this domestic remedy is likely not available.166 Because states have therefore not complied with their requirements under UNCLOS, ITLOS has a strong case for jurisdiction as the appropriate body to handle disputes associated with these unfulfilled obligations. In this respect, the overwhelming weakness of domestic protections actually benefits states in arguing for jurisdiction before ITLOS. This observation is in contravention to scholars’ criticism of domestic cable protections.167

Once jurisdiction has been established, states can then turn to the two indirect effects of hacking—cable damage and violations of the right to privacy—to seek liability against hacking states.

162 UNCLOS, supra note 65, art. CCLXXXV.
163 Coffen-Smout & Herbert, supra note 143, at 444.
164 Id., Davenport, supra note 29, at 84.
165 There is some question as to whether weak enforcement regimes, as in Australia or the United States, would be sufficient to evade ITLOS jurisdiction. States, however, can likely still obtain jurisdiction over this question.
166 Davenport, supra note 29, at 106.
167 Id. at 84, 106.
B. Using ITLOS to Protect Against Cable Damage

States can use ITLOS to protect against hacking by enforcing liability for damages incurred from hacking. Using Articles 112 and 113 of UNCLOS, injured states can argue the offending states are not abiding by their UNCLOS requirements to create a domestic regime to punish cable damagers. Injured states can further argue offending states violate the freedom to lay and operate submarine cables. In the first instance, an injured state may use ITLOS to force the offending state to punish its wrongdoers under its own domestic jurisdiction. ITLOS can bind states to craft and administer regimes protecting cables against damage by their citizens. This may in turn increase prospective economic costs of hacking and reduce overall hacking activity levels. While states may have an incentive to cheat, the political costs from breaking with its required enforcement regime will only increase under a binding dispute resolution order from ITLOS.

States can further argue domestic protections as required under UNCLOS may not wholly protect this articulated right. If the cost of damage to cables is so expensive\(^\text{168}\) and the economic value of internet access is so great,\(^\text{169}\) states can argue the domestic regimes formulated and required under UNCLOS may not adequately protect their rights to be free from damage or interference. Accordingly, states may argue ITLOS should assert some damages or compensation requirement for intentional damage to cables from hacking.

In the second instance, states may argue the freedom to lay and operate cables under UNCLOS extends to protections against interference by foreign states on the high seas. While UNCLOS only protects against “damage” to cables,\(^\text{170}\) states can reasonably argue the UNCLOS protections are an outgrowth of a history of protecting general use and operation of cables. Because the 1884 Convention protected against interference of cable operation, which was subsequently codified in the intervening conventions, states can reasonably claim UNCLOS’s more general cable freedoms extend to freedom from arbitrary interference by foreign states. Because hacking interferes with a cable’s signal and likely requires repair by the operator, states can then argue hacking falls under this sphere of prohibited activities.

ITLOS would likely be receptive to this argument. ITLOS has a history of extending greater protections to states than is precisely articulated in the language of UNCLOS. In *MV/Saiga*, ITLOS held Guinea violated the prohibition against the excessive use of force in detaining ships, although prohibitions against the

\(^{168}\) Matis, supra note 113.

\(^{169}\) *The Economic Impact of Submarine Cable Outages Can Still Be Enormous*, supra note 114.

\(^{170}\) UNCLOS, *supra* note 65, art. CXIII.
excessive use of force are not expressly articulated by UNCLOS.\textsuperscript{171} And in \textit{Guyana v. Suriname}, ITLOS held Suriname used unlawful force against a Canadian vessel licensed by Guyana even without a prohibition on the use of force against foreign vessels under UNCLOS.\textsuperscript{172} These cases indicate ITLOS’s willingness to extend more general international law protections beyond UNCLOS. These cases further demonstrate ITLOS is willing to extend protections to states beyond the text of UNCLOS using the history and subtext of the treaty. Accordingly, ITLOS may be receptive to the argument that freedom from damage or interference has long been historically recognized.

This solution is novel as it resolves the lack of enforcement mechanism scholars criticized by scholars with respect to domestic cable regimes. Because ITLOS can require states to abide by their treaty obligations, ITLOS can then mandate states create domestic regulations to protect cables. Further, this solution allows ITLOS to hear arguments about more general freedoms related to submarine cable use. Because ITLOS can hear arguments related to other binding treaties and agreements,\textsuperscript{173} states can argue the 1884 Convention or intervening law of the sea conventions established the freedom to lay and operate cables includes freedom from unnecessary cable interference.

This solution carries with it a handful of potential caveats. First, ITLOS will most likely require the offending country to hold violators domestically liable. This follows because Articles 112 and 113 of UNCLOS only require a domestic cable protection scheme. The offending country is likely to impose minimal penalties or elect not to impose penalties. This strategy may then not raise costs associated with hacking to lower overall activity levels. This outcome, however, does not fully undermine the solution described above. If countries’ domestic regimes continue to be weak or weakly enforced, ITLOS is more likely to extend greater protections to cables than are required under UNCLOS. This would be similar to the extension of greater rights than necessary in \textit{Guyana v. Suriname}.\textsuperscript{174} Further, continued refusal to hold violators domestically liable will cause ITLOS to hold contravening states accountable for failing to uphold their UNCLOS responsibilities. This may in turn increase the costs associated with hacking and lower activity levels.

Second, arguments about more general rights to cable protections, such as the freedom of cable operation, may be weak because not many states signed onto the 1884 Convention or the intervening conventions of the laws of the sea. Without a convention to point to, ITLOS would then be relying on general norms


\textsuperscript{172} Guyana v. Suriname, 47 I.L.M. 166, ¶ 405 (Perm. Ct. Arb. 2007).

\textsuperscript{173} UNCLOS, \textit{supra} note 65, art. CCLXXXXIII.

\textsuperscript{174} Suriname, 47 I.L.M. 166.
Submarine Cable Hacking and Law of the Sea

Jason Petty

Summer 2021

of international law in creating a liability regime for cable damage. ITLOS may be reticent to do that for fear of overstepping its bounds and of countries not participating in dispute resolution. Once such refusal occurred in 

Arctic Sunrise

during Russia refused to appear in front of ITLOS.\textsuperscript{175}

Third, not all hacking attempts end in damage to submarine cables. If a cable was not damaged during a hacking attempt, this regime may not apply. Accordingly, states must turn to other norms or rights to protect against submarine hacking. The following Section presents a solution to submarine cable hacking that centers on the right to privacy and does not rely on damage to the underlying cable to provide liability.

C. Using ITLOS to Protect Against Violations of the Right to Privacy

States can also use ITLOS to pursue violations to the international right to privacy committed by hacking. ITLOS is able to apply UNCLOS law and “other rules of international law not incompatible with” UNCLOS including the Universal Declaration of Human Rights and the ICCPR.\textsuperscript{176} States subject to hacking can use these conventions and other international human rights to argue against hacking once they have jurisdiction under ITLOS.

States can argue hacking contravenes the right to privacy embedded in numerous human rights treaties. As discussed in Section V, citizens enjoy a right to privacy under many international conventions. ITLOS can enforce violations of the ICCPR and other treaties as they relate to the right to privacy. While submarine cable hackers may be attempting to access sensitive government information, the hacking of underwater cables almost inevitably includes access to private citizens’ internet traffic because states cannot pick and choose what information they obtain.\textsuperscript{177} Such a broad sweeping may therefore be considered “arbitrary” and in contravention of the international right to privacy.

While litigation around the right to privacy is relatively new, there is a trend among international bodies toward recognizing a universal right to privacy. As discussed in Section V, the ECtHR previously held the U.K.’s bulk surveillance program through fiber optic cables violated the right to privacy but subsequently dismissed the case on appeal for failure to pursue all domestic remedies.\textsuperscript{178} In October 2020, the CJEU held indiscriminate mass surveillance violated E.U.

\textsuperscript{175} Chao Zhang, Russian Absence at the Arctic Sunrise Case: A Comparison with the Chinese Position in the South China Sea Arbitration, 8 J. E. ASIA & INT’L L. 413, 414 (2015).

\textsuperscript{176} UNCLOS, supra note 65, art. CCLXXXIII; Noyes, supra note 159, at 124.

\textsuperscript{177} Mark Harris, How US National Security Agencies Hold the Internet Hostage, TECHCRUNCH (July 18, 2019), https://perma.cc/J4UV-HNNM.

\textsuperscript{178} 10 Human Rights Organisations v. United Kingdom, supra note 132.
privacy and data protections.\textsuperscript{179} And the German Constitutional Court held Germany’s constitutional protections against indiscriminate surveillance and data collection extended to foreigners living abroad.\textsuperscript{180} Beyond these court rulings, the International Court of Justice (ICJ) has affirmed the rights under the Universal Declaration of Human Rights and the ICCPR apply globally.\textsuperscript{181} And while the ICJ has not affirmed a right to privacy against all indiscriminate surveillance, the Court did not denounce such an argument in two prior cases involving surveillance on private communications.\textsuperscript{182} This matches a trend in international bodies toward greater recognition of the right to privacy in recent years.\textsuperscript{183}

Rights under the ICCPR and the Universal Declaration of Human Rights have previously been protected by ITLOS.\textsuperscript{184} While ITLOS has not taken on cases involving privacy, ITLOS precedent indicates a keen and demonstrated interest in protecting other human rights outside of those codified by UNCLOS. For example, ITLOS in its 1999 \textit{MV Saiga Nr. 2} judgment,\textsuperscript{185} for a case involving seized vessels, referred to “considerations of humanity” that “must apply to the Law of the Sea as they do in other areas of international law.”\textsuperscript{186} The ITLOS decisions in \textit{Arctic Sunrise} and \textit{Enrica Lexie} further indicate an increasing willingness by ITLOS to consider human rights concerns, either implicitly in the case of \textit{Enrica Lexie} or explicitly as in \textit{Arctic Sunrise}.\textsuperscript{187}

These cases demonstrate “a pattern of increased willingness on the part of States to invoke (universal) human rights instruments (i.e., the ICCPR)—and, in this case, even the views of human rights bodies (i.e., the Human Rights Committee) — in provisional measures proceedings before ITLOS.”\textsuperscript{188} Scholars have observed ITLOS increasingly incorporates “considerations of humanity” in

\begin{footnotesize}
\begin{enumerate}
\item Lomas, \textit{supra} note 136.
\item Melissa Eddy, \textit{Right to Privacy Extends to Foreign Internet Users, German Court Rules}, \textit{N.Y. Times} (May 19, 2020), https://perma.cc/GVU4-X7L5.
\item Frederic Gilles Sourgens, \textit{The Privacy Principle}, 42 \textit{Yale J. Int’l L.} 345, 354 (2017); \textit{see also} Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).
\item United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, 35 (May 24) (finding expulsion of the spying diplomat was the proper remedy); Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8, Decision on Preliminary Issues, 1 43 (June 23, 2008) (finding states can intercept communications as part of lawful criminal investigations).
\item Van Schaack, \textit{supra} note 130, at 32.
\item \textit{See generally} Petrig & Bo, \textit{supra} note 160.
\item M/V Saiga (No.2) (St. Vincent v. Guinea), Judgment of July 1, 1999, ITLOS Rep., 10.
\item \textit{Id.} ¶ 15; \textit{see also} Treves, \textit{supra} note 90, at 5.
\item Petrig & Bo, \textit{supra} note 160, at 382–85, 386–91.
\item \textit{Id.} at 391.
\end{enumerate}
\end{footnotesize}
its decision-making.\textsuperscript{189} And, as discussed in Section V, the international right to privacy would fall into such considerations.

ITLOS is further likely to invoke the right to privacy under the ICCPR or the Universal Declaration of Human Rights because privacy is so closely linked to the subject of the proceeding on the merits. ITLOS requires “the relief sought (and the rights to be protected by the relief) must be closely related to the rights subject to the proceedings on the merits.”\textsuperscript{190} The freedom to lay cables under UNCLOS impugns some respect for those cables, their use, and their content. Because hacking violates the use and content of these cables, the right to privacy seems closely associated with hacking and capable of being invoked in proceedings.

This solution is novel for a handful of reasons. First, this solution uses a supposed weakness in international protections for submarine cables—lack of domestic protections—as the jurisdictional hook for liability. Although scholars have critiqued the weakness of these regimes,\textsuperscript{191} the lack of an effective or a largely weak framework is actually a strength in creating a secondary method to pursue violators. Further, if domestic protections were stronger, ITLOS complaints may be superseded by domestic and local remedies. Because domestic remedies are limited in application and minimal at best, the dispute resolution system offered by ITLOS has broader application and ability to impose necessary penalties.

Second, this solution avoids questions of the peacetime legitimacy of state intelligence gathering more generally. As discussed in the Tallinn Manual, cyber operations may not be conducted in an unlawful manner.\textsuperscript{192} If submarine cable hacking is considered a violation of the international right to privacy, this particular method of collecting surveillance would be deemed unlawful. States still preserve the ability to gather intelligence or surveillance through other, less arbitrary, means. This solution is therefore more tailored than other debates around peacetime intelligence gathering writ large.

While a novel method of solution, the use of ITLOS to make claims against the international right to privacy is not without caveats. While the caveats discussed below are not fatal to the solution described, they do present questions about the potential scope of the solution asserted and how controversies around the international right to privacy and international legal obligations generally bleed into the conversation around submarine cables.

\textsuperscript{189} See generally Francesca Delfino, ‘Considerations of Humanity’ in the Jurisprudence of ITLOS and UNCLOS Arbitral Tribunals, in INTERPRETATIONS OF THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA BY INTERNATIONAL COURTS AND TRIBUNALS 421 (Angela Del Vecchio & Roberto Virzo eds., 2019).

\textsuperscript{190} Petrig & Bo, supra note 160, at 380.

\textsuperscript{191} See Davenport, supra note 29, at 84; Scanlon, supra note 149, at 299–301.

\textsuperscript{192} TALLINN MANUAL, supra note 99, at 170.
First, not all states are signatories to UNCLOS or the human rights conventions that describe the international right to privacy. Prominently, for example, the U.S. has not ratified its participation in UNCLOS, although it is a signatory. While making some claims against other states under UNCLOS, it is not clear the U.S. can invoke UNCLOS or be subject to liability under UNCLOS for claims made by other states. Non-signatory parties could voluntarily agree to arbitration under ITLOS but doing so does not seem to be in their rational self-interest. Because not all states are then bound to ITLOS as a dispute resolution mechanism, the solution offered above may not be universal in application.

Second, even if a decision is binding, it is not clear how ITLOS would enforce its arbitration decisions if parties do not comply. For example, in the Arctic Sunrise arbitration, Russia refused to appear before ITLOS or abide by the tribunal’s ruling. ITLOS does not have a security force to implement rulings and does not have the ability to levy sanctions or restrict access to seaways if states do not comply with their rulings. States would therefore still need to consent to whatever ruling ITLOS makes, even if their rulings are technically “binding.” This critique, however, could likely be levied with any international legal enforcement mechanism as truly bad actors can continue to evade judgments.

Third, if the injured state and the hacking state have reasonably robust domestic cable protection schemes, ITLOS may not have jurisdiction. As discussed above, ITLOS requires states to exercise local remedies before appealing to ITLOS for dispute resolution. If the offending state has domestic protections, the injured state can appeal to that state to subject the offenders to domestic protections. This would result in the offending state being responsible for enforcing a regime which its citizens, and quite probably state agents, have violated. The incentives for the offending state to do so are minimal.

This possibility, however, is not fatal to the above solution mechanism. States can still appeal to UNCLOS for greater clarity for states’ responsibilities for cable protections on the high seas under Articles 112 and 113 of UNCLOS. States can further dispute the domestic proceedings as insufficient to compensate the injured party for potential cable damage or the stolen information. And states can likely still make claims related to the international right to privacy not addressed by domestic protections. While this last claim may raise issues around whether ITLOS is the proper body to hear these complaints, because the conduct occurs at sea, ITLOS still has a viable claim to jurisdiction.

194 Id.
195 Noyes, supra note 159, at 154.
Fourth, relatedly, the most probable avenue to obtain jurisdiction under ITLOS involves damage to submarine cables as a result of hacking. If hacking technologies are sufficiently sophisticated, they may cause no harm to submarine cables. Accordingly, states would need to develop alternative reasons to obtain ITLOS jurisdiction. As discussed above, states can argue for dispute resolution for interfering with cable operation under Articles 112 or 113. More generally, states can argue ITLOS’s broad jurisdiction gives them standing, but this also seems weak.

Alternatively, states can make claims using the more general wording of the 1884 Convention. The 1884 Convention prevents “interference” with telegraph cables. Because hacking necessarily involves some degree of signal interference of fiber optic cables, hacking would likely fall into this broader “interference” category. And because the 1884 Convention does not have a body for dispute resolution related to obligations under the Convention, states can reasonably argue ITLOS is the most proper forum to hear disputes.

This argument does not guarantee jurisdiction either. Foremost, the 1884 Convention addresses telegraph cables. While it seems reasonable to extend these protections to fiber optic or internet cables given the spirit of the Convention, the 1884 Convention is then limited in scope. Further, “interference” is harder to prove as compared to external damage to cables in hacking attempts. It is more difficult for signal operators to observe momentary gaps in service as compared to external cable damage, and maintaining a record showing this interference is both costly and difficult. Additionally, not many states are parties to the 1884 Convention as compared to UNCLOS. While many of the power players likely to engage in hacking are parties to both, including Russia and the U.K., some states are parties only to UNCLOS, like China, or party only to the 1884 Convention, like the U.S. Finally, the 1884 Convention, like UNCLOS, only presents obligations for states to create domestic protective schemes for submarine cables. The 1884 Convention does not have any enforcement mechanisms against this bad behavior which makes ITLOS’s jurisdiction more spurious. And claims related to U.N. human rights obligations using the 1884 Convention to confer jurisdiction seem weak.

Fifth, claims of the right to privacy are relatively novel for international courts and the limits of this right have not been clearly defined. ITLOS, in turn, may not make sweeping decisions related to hacking for these types of cases without further clarity on the scope of the right to privacy. ITLOS may instead resolve the dispute by requiring greater compensatory damages or greater domestic protections for damage to cables without resolving the issue of hacking. This result may incidentally reduce hacking by raising the possible costs associated with hacking attempts, but states may still find the possible damages as reasonable to the perceived intelligence gains from hacking. Accordingly, privacy suits may
need to wait for greater international consensus on the limits of the right to privacy.

This solution, however, can build on changing norms around the right to privacy. As discussed in Section V, the international right to privacy is increasingly recognized on the global stage. This solution presents novel questions within this ongoing debate. The recognition of the right to privacy depends largely on “effective control” of the persons or territory involved in the surveillance. Submarine cables present novel questions around this effective control as it is nearly certain that at least some of a state’s citizens’ communications will be obtained through a submarine cable hack. Is this incidental acquisition enough to violate standards against countries surveilling their own citizens arbitrarily?

Further, submarine cables are simultaneously a protected and necessary state resource and located on the high seas. Cables may then be a useful framing to consider how much control and sovereignty states have over their cyber space. Are cables more like physical territory or more like ephemeral cyber space in considering sovereignty and does the distinction ultimately matter with respect to privacy rights? This Comment is unable to answer these questions fully, but the Comment’s solution opens novel avenues for argument around these themes and may help advance the dialogue with respect to privacy rights.

Sixth, some states may not want to pursue creating a regime against submarine cable hacking. As discussed in Section II, many global powers, including the U.S., China, the U.K., and Russia, engage in submarine cable hacking. States, particularly those with robust submarine military presences, may want to preserve the ability to surveil other states using submarine cable hacking. These states would therefore not invoke ITLOS or the right to privacy against submarine cable hacking. This may be a particularly onerous challenge because these powerful states often develop and enforce global norms.

As discussed in Section III, however, this criticism may not necessarily be fatal to the solution offered above. Norms with respect to submarine cables and hacking in general appear to be shifting. Smaller states or landlocked states that do not engage in submarine cable hacking have incentives to further develop these norms to protect their citizens’ privacy and governmental data without the counterincentive of preserving the right to hack other states. While this shift may take time to play out, the momentum is in favor of increased recognition of privacy rights as discussed in Section V. Regardless, as hacking increases and as the associated damage from hacking rises, international legal solutions may be more cost effective than patrolling the seas against hacking attempts. Accordingly, states may decide international norms are a more cost-effective way of reducing hacking activity levels.

---

197 Bignami, supra note 119, at 5.
Seventh, if states elect not to pursue a hacking complaint against another state for geopolitical reasons, the injured cable operator may not be able to use ITLOS to seek a suitable remedy. In most cases, the injured party is likely a corporation. Due to the terrific costs in laying submarine cables, the majority of modern-day cables are owned and laid by private companies and collectives. For example, Google has backed at least 14 cables globally and other tech firms have similarly pursued their own submarine cable systems. Accordingly, corporations often foot the bill for cable damage or privacy concerns.

ITLOS jurisdiction over corporations is somewhat ambiguous but appears limited. Article 20 of the ITLOS charter provides non-state entities can access to the Tribunal for cases where other agreements accepted by all parties in the case confer jurisdiction to ITLOS. It is highly unlikely the corporation and the hacking party will have agreed to dispute resolution by ITLOS in the case of hacking. Accordingly, when the corporation’s home country elects not to pursue dispute resolution, ITLOS may not be a viable solution.

This, however, does not entirely eliminate the possibility of enforcing an anti-hacking regime through corporate action. Depending on the jurisdictional limits of the corporation’s home country, corporations can pursue private civil suits against foreign states. These actions are generally not taken due to geopolitical concerns, concerns about comity, and questions about where the alleged tort occurred. The possibility of these suits, however, raises the specter of private action against hacking malfeasors, which may be worth considering in subsequent analyses beyond the scope of this Comment.

VIII. Conclusion

This Comment examined whether states had any recourse under public international law when foreign states hacked into submarine cables. In so doing, this Comment explored public international law around submarine cables (Section IV) and public international law with respect to hacking (Section V) to conclude states can use the International Tribunal of the Law of the Sea (ITLOS) invoke liability (Section VI). This Comment argued ITLOS would have proper

---

198 Winston Qiu, Complete List of Google’s Subsea Cable Investments, SUBMARINE CABLE NETWORKS (July 9, 2019), https://perma.cc/3KL8-T4PK.

199 Many corporations form cable cooperatives to share repair and installation costs. See, for example, the Atlantic Cable Maintenance & Repair Agreement. About, ACMA, https://perma.cc/DXF6-NPFM.

200 Noyes, supra note 159, at 132.


202 See generally Samantha N. Sergent, Extinguishing the Firewall: Addressing the Jurisdictional Challenges to Bringing the Cyber Tort Suits Against Foreign Sovereigns, 72 VAND. L. REV. 391 (2019).
jurisdiction over submarine hacking claims and would be a suitable body to address these complaints due to the weakness of domestic cable protections. This Comment argued states have two avenues for establishing liability through ITLOS: damage to cables or violations of the international right to privacy. This Comment thus invokes broader discussion of how states can seek legal recourse against submarine cable hacking while norms and conventions addressing hacking and submarine cables continue to develop.