Common Grounds to Protect IXPs: The Key for the Internet Resilience in Times of COVID 19

Patricia A. Vargas-León[1]

Introduction

On December 31, 2019, China notified the World Health Organization (WHO) of a string of respiratory infections in Wuhan that infected around 11 million people. WHO baptized the virus responsible for those infections as "COVID-19." By early 2020, the number of COVID-19 cases tripled and compromised 114 nation-states in the world. Because of the high spread of the new virus, on March 11, 2020, WHO declared COVID-19 a global pandemic (Cucinotta & Vanelli, 2020).

Since those days, many governments closed their borders and declared strict or partial quarantines. Amid this challenging situation, the dependency on the so-called "essential workers" became apparent. In this group, the farmers are at the first step of the production chain. The situation is different in every part of the world, but in many nation-states of the Americas, these workers are usually neglected, not-considered, and lack labor-legal protections (Bottemiller & Crampton, 2020). In the virtual environment, something very similar occurred. When humans moved to a lockdown, the dependency on the Internet increased exponentially. Human activity moved to an online environment, including e-learning, messaging, health, video conferencing, among other activities. Network connectivity and online collaboration became the "new normal." Suddenly, the Internet became the only option for certain transactions and social interactions (Wooding, 2020).

Nevertheless, such an enterprise is possible, thanks to the Internet infrastructure that facilitates to work remotely. That infrastructure covers multiple elements that facilitate support international Internet traffic. This paper will refer to only one of those elements, the Internet Exchange Points (IXPs). IXPs are physical and neutral locations where different networks meet to exchange Internet traffic via a switch (ISOC, 2020b).

As a consequence of the lockdowns multiple governments imposed as part of their health policy to fight against COVID 19, the world witnessed an exponential increase in Internet traffic. Because of the critical role IXPs play supporting the local and international Internet traffic, the technical community has paid a great deal of attention. However, as it happened with the "essential workers" during the COVID 19 crisis, there is a lack of legal studies about this critical Internet infrastructure piece. From an international law perspective, it is unclear what legal provisions may protect the IXPs and the Internet traffic they backed. Previous studies of cybersecurity, like the Tallinn Manual 2.0 from 2017 (sponsored by the NATO Cooperative Cyber Defense Centre of Excellence) cited up to thirteen international treaties that have provisions related to the Internet and the cyberspace (Schmidt, 2017). This paper will conduct a legal analysis focusing on one of those treaties: The United Convention on the Law of the Sea, also known as UNCLOS.

Nation-states frequently claim sovereignty over the Internet. Some governments representatives have suggested applying similar policies to the ones contained in UNCLOS to the Internet (C. Clark, 2016; Steven, 2001). This paper proposes a different approach, this is, to use the rules of UNCLOS differently from the way the Tallin Manual 2.0 does. This paper aims to find, within UNCLOS provisions, international principles that could protect the Internet infrastructure and the Internet traffic from nation-state's claims. In other words, this paper's goal is identifying principles grounded within

[1] Postdoctoral Scholar, The Fletcher School, Tufts University; Visiting Fellow Information Society Project, Yale Law School, PhD (Syracuse University), Law Degree (Pontifical Catholica University from Peru)

The work described in this paper was partially supported by NSF grant CNS 1923528.

the traditional rules of international law to protect the infrastructure that supports the global Internet traffic.

It is also important to clarify that the purpose of this paper is not to analyze the application of the sovereignty rules of UNCLOS over the Internet, but as just mentioned, it is quite the opposite. A future and more comprehensive project will cover the analysis of additional international protocols. Therefore, within this context, this paper will:

1. To provide an overview of the current situation of the IXPs during the COVID-19 crisis with particular emphasis on Internet traffic. This paper will use the data provided by reliable public sources from the private sector and civil society about the fluctuation of the Internet traffic.
2. To identify what provisions of the law of the sea can protect the IXPs and the Internet traffic they support

I. The Internet: A Network of Networks and the Infrastructure Behind

The first task in analyzing how the law of the sea can provide some arguments to protect the Internet Exchange Points (IXPs) is to determine the scope of the problem. The first part of this paper will provide a definition of the Internet and the elements of the Internet infrastructure that we intent to address. This step is necessary to the legal analysis that follows.

A. Defining the Internet

The Internet is defined as a “network of networks,” the private sector is the owner and administrator of the Internet infrastructure. A network is a group of connected computers that send data to each other. In this regard, a computer network is very similar to a social circle, a group of people who all know each other and regularly exchange information. Since computers connect within networks, and these networks also connect with each other simultaneously, one computer can talk to another computer in a distant network thanks to the Internet. This facilitates the exchange of information among computers all over the world (Mueller, 2010).

As a distributed networking system, the Internet does not depend on any individual machine. Any computer or hardware capable of sending and receiving data through the correct networking protocols can be part of the Internet. The Internet also lacks a single “node” or central point of control; in fact, the Internet has a distributed nature that makes it resilient. Computers, servers, and other pieces of networking hardware may connect and disconnect from the Internet at any time without having an impact over the Internet functions (DeNardis, 2014). In terms of functioning, two concepts are critical to understanding how the Internet works: packets and protocols. A packet is defined as a small piece or segment of a larger message. Each packet contains both data and information about that data. When data travels through the Internet, it gets broken up into smaller packets. Then the packets get routed to their destination crossing by various networking devices such as routers and switches. When packets finally arrive at their destination, the receiving device reassembles them in the appropriate order to display the data. Packets travel through the Internet using a technique called “packet switching”(Clark, et all, 2014).

An additional challenge comes from interconnecting different hardware and software. The Internet must use communication techniques that all computers must understand. This problem was solved by creating standardized protocols, common ways of doing specific actions, and formatting data so that two or more devices can communicate and understand each other. The Internet packets are transmitted to their destination by routers and servers, using the “TCP/IP protocol” (Transmission Control Protocol/Internet Protocol). This last aspect of the Internet makes possible privatization and decentralization of networks operations and policies (Mueller, 2010).

In a few concrete points it can be said about w the Internet: (1) is a network of independent networks with common interconnection standards, open interfaces, common naming and addressing systems, (2) its basic goal of connectivity and, (3) to users, it appears to be one single network, where every user can access every connected device (Mclaughlin, 2002).

B. Internet Traffic

As mentioned in the previous section, the Internet is a network of networks, and autonomous systems (AS) are the networks that constitute the Internet. For proper and constant communication, AS have a standard routing policy. Every device that connects to the Internet is connected to an AS. Data packets across the Internet go from AS to AS until they reach the AS that contains their destination Internet Protocol (IP) address. Every AS controls a circumscribed set of IP addresses, and the range of IP addresses that an AS controls is called their "IP address space." AS connects and exchange Internet data packets through the "peering process" facilitated by the Internet Exchange Points (IXPs) (Cloudfare, 2020b, 2020a).

By 2014, the Internet had over 50000 interconnected Autonomous Systems (ASes). A business agreement between two ASes can exchange traffic under various policy constraints. One AS can be the provider of the other AS (the customer), offering the latter access to the entire Internet. Other AS allow-free peering relations, in which two ASes exchange their local and customer-originating traffic without charge. These business relations may have a heavy economic impact and/or affect the profitability of the ASes. In this context, peering agreements between Autonomous Systems affect not only the flow of interdomain traffic but also the economics of the entire Internet ecosystem (Lodhi, Dhamdhere, & Dovrolis, 2014). Private contract transactions define the Internet traffic as the traffic originated by an end-user subscriber served on one party's network, then transmitted to the other party's network (this means the other end-user or receiver). Next, the traffic is handed off by that party (the receiver) to an ISP served by that party, which has been assigned a local identification number to the originating end-user subscriber (Pac-West Telecomm & Cox Arizona Telcom, 2004).

At the end, the cost of interconnection depends upon privately negotiated peering and traffic agreements. Nevertheless, usually developing nation-states must sign traffic agreements (not peering), with backbone providers (or their customers), and pay 100% of the outbound and inbound packets' traffic. In this regard, backbone providers treat all ISPs equally, independently, whether they belong to a developing nation-state or not). In general, Internet traffic is defined as the service of allowing network traffic to cross from a device to the global Internet (Lodhi et al., 2014).

In the next paragraph, this paper will provide a definition of what IXPs and the peering process are.

C. Internet Exchange Points (IXPs)

IXPs are physical infrastructures that allow Internet service providers (ISPs), content delivery networks (CDNs), backbones to interconnect directly or exchange traffic among their networks. As mentioned before, this activity is known as the "peering process". Peering is a process by which two or more Internet networks connect and exchange traffic. Peering allows those networks to hand off traffic between each other's customers, without having to pay a third party to carry that traffic across the Internet for them. Peering is the more usual way of connecting to the Internet, in which an end user or network operator pays another network operator to carry all their traffic for them (Netnod, 2018, 2019). Peering is different from the "regular traffic," marked by business relationships where one ISP provides (mostly selling) connectivity to all destinations on the global Internet. The price is defined for access to the Internet according to the volume and is measured in Mbpb (megabits per second) (Mclaughlin, 2002).

By enabling a local network of networks, IXPs reduce the traffic ISPs must deliver via its upstream transit providers that may be located abroad (Nomikos, Sermpezis, & Dimitropoulos, 2017). Therefore, the more IXPs a nation-state has the quality and the speed of the Internet service increases.

For the most part IXPs are privately own and can be classified within five categories: non-profit organizations, associations of Internet Service Providers (ISPs), operator-neutral for-profit companies, university or government agencies, and informal associations of networks (ISOC, 2020b). IXPs conduct technical functions related to interoperability. In this regard, they also shape public policy related to information access, individual rights, and security. Internet interconnection agreements involve private contractual arrangements among network operators to connect directly or at shared Internet Exchange Points (IXPs), a transaction that raises governance questions about who can connect and under what economic terms (DeNardis, 2013).

In this condition, IXPs play a critical role in interconnecting national and international networks because of the multiple connections they handle (Medows, 2012). IXPs have the enormous task of transferring Internet packets and facilitate national and international Internet traffic. This function remains and is more vital in times of natural disasters and global pandemics.

IXPs reside mostly in nation-states of advanced economies with sophisticated Internet infrastructure. Because of this situation, Internet traffic makes a sort of 'roundabout' and travels to the more established IXPs globally (PCH, 2019; Sanchez, 2018). This activity is known as the 'boomeranging,' 'hair-pinning,' or 'trombone effect' and is peculiar from emerging markets, where local ISPs are less interconnected (Fanou et all, 2018).

Consequently, the Internet traffic routes through multiple territories and jurisdictions, a situation that brings up the question about governance and sovereignty. IXPs provide an alternative to the boomeranging effect's expenses that increases the costs of an expensive international link. On this particular subject, in 2005, during the World Summer Information Society (WSIS), this problem was highlighted by the developing nation-states that participated in the summit. Delegates of the developing nation-states were advocating for a better balance of the charges for international Internet connectivity, so that everyone could get Internet access. They also call to set up regional high-speed Internet backbone networks and the creation of national, sub-regional and regional Internet Exchange Points (IXPs) (WSIS, 2005). Moreover, IXPs help keep local traffic local and help with cheaper, better, faster, local Internet traffic exchange. The cost and quality of service that IXPs make can help ISPs, and content delivery networks see the benefit of supporting IXPs (ISOC, 2020a).

In the current pandemic context, the effects of COVID-19 can be foreseen and will affect developing nation-states most severely. Additionally, developing nation-states do not have a sufficient level of Internet infrastructure investments, and they are not prepared for the crisis. Moreover, some developing nation-states depend entirely on developed nation-states for Internet access. Consequently, if the supplier nation-state faces problems with the Internet or decides to act over the traffic, dependent developing nation-states will feel the impact (Geneva Internet Platform, 2020).

From a technical point of view, an IXP is an Ethernet switch, like connecting computers in an office network. Each network connecting to an IXP connects one or more of its routers to that IXP's Ethernet switch, and they send traffic across the Ethernet switch to routers belonging to other networks (Netnod, 2019; Norton, 2014). Interrupting the normal functioning of an IXP has a direct impact on the connection among ISPs and, therefore, it may slow down the Internet speed and eventually stop the Internet service (van Beijnum, 2011). Because of their importance in supporting Internet traffic, the technical community has paid a great deal of attention to the IXPs. However, as it happened with the "essential workers" during the COVID 19 crisis, there is a lack of legal studies about this critical Internet infrastructure piece. From an international law perspective, it is unclear what legal provisions may the IXPs and the so precious international traffic they support.

D. Internet Traffic during COVID 19: Impact of COVID-19 over the IXPs

The new Coronavirus, COVID 19, push thousands of people to work from home. During March 2020 the Internet traffic increased worldwide. As of April 2020, in the middle of the pandemic, there were around 4.57 billion active Internet users who relied on the Internet for performing different activities. People who conducted business activities relied on the Internet for communications, supply chain management, and business research, among other activities (US Signal, 2020).

According to Akamai, in March the Internet traffic increased to 30%, ten times more than in previous years. By definition, the Internet is a network of networks, and this year all networks are combining into a massive wave of traffic. In this context, video streaming and software download are the activities responsible for the majority of growth (McKeay, 2020b, 2020a). Similarly, private corporations report an increase in international Internet traffic. Nokia reports a 20-40% increase during March 2020, Verizon and Vodafone report 20%-50% week-on-week growth, and Orange reported the number of users connecting to its network increased by 700% (Geneva Internet Platform, 2020).

Regional concerns about COVID-19, alongside lockdowns and isolation protocols, had a crucial impact on traffic levels. Changes within nation-states health policies affected the local and regional traffic. Italy was the first European nation-state affected by COVID 19 and the first to go into isolation. The Italian isolation protocol got in place on March 8, 2020, and during the first week, Italy's daily traffic levels grew up to 75% above the levels in February. On April 3, 2020, the Internet traffic reduced to less than 10% above February's average (McKeay, 2020b, 2020a).

In Spain, the isolation order started on March 14, 2020. Almost immediately, telecom operators reported that that Internet networks had a 40% increase, and that voice and data usage in mobile networks went up 50% and 25% (Geneva Internet Platform, 2020). These dramatic demands are common factors at a regional level. As time passed and governments eased lockdowns the initial demand decreased. The tendency shows that there will be a demand of 15-30% higher than past years in Europe (McKeay, 2020b, 2020a). In general, major European IXPs (DE-CIX Frankfurt, AMS-IX Amsterdam, and LINX London) were able to handle higher traffic peaks. However, national IXPs (especially the ones located in developing countries) required additional capabilities to handle the increase in the Internet traffic (Geneva Internet Platform, 2020).

In the case of the U.S., where there was no uniform national lockdown, by March 27, 2020, there was an increase of 33% above February's average Internet traffic level. In April, the traffic decreased to 12-15% above the February level (McKeay, 2020b, 2020a).

At a worldwide level, the Internet Society (ISOC) reported an increase between 7- 40% in Internet traffic. In Asia, Hong Kong IXP (HKIX) traffic increased by 35%, from late January to mid-April. The increased came from the following platforms: video conferencing, online teaching, video streaming, online banking, Internet banking, and online shopping. The Asia Pacific IXP Asia Pacific Internet Exchange (APIX) located in Japan reported that the Internet traffic became 1.6 times higher during daytime because of work from home, remote study, video traffic (Netflix, Amazon Movie, and YouTube).

The Malaysian IXP (MyIX) described that the overall peak traffic increased from 20%-33% between March and May 2020. The traffic was constantly high between 10 am and 10 pm, and some networks' traffic increased at a 100% capacity, while some also decreased at a 100% capacity. In the case of Nepal, the IXP NPIX, informed of a peak traffic growth of 19% during the COVID-19 lockdown (ISOC, 2020a).

Finally, in Latin America, Cloudflare reported a rapid increase of 10-30% in Internet traffic since the beginning of March. In some cities, like Mexico City, São Paulo, Buenos Aires, and Santiago, there was an increase of 50% (Hernandez, 2020; Tribaldos & Silva, 2020).

Patterns during the pandemic show that there was no difference between peak and off-peak time. Nevertheless, the pandemic increased traffic, but it also changed the type of content in demand. Since March, there is an increase in the demand for content for kids, education, entertainment, arts & crafts, government resources, and online games (Hernandez, 2020). Regarding the IXPs functioning, there were no changes in peering policies, although some emergency measures were in place in Australia and Japan (Haq, 2020).

IXPs proved not only to be resilient, but also to quickly adapt to the new needs of the industry.

II.
An Overview of the Law of The Sea

The second task of this paper is providing an overview of the United Convention on the Law of the Sea (UNCLOS) and the principles that rule the freedom of navigation in the high seas. The conceptual basis to advocate for the existence of the high seas as a limitation to the sovereignty of the coastal nation-states will be the ones that provide some international law principles that protect the IXPs and the Internet traffic.

A. United Nations Convention on the Law of the Sea from 1982 (UNCLOS)

The United Nations Convention on the Law of the Sea or UNCLOS (UN, 1982) is an international agreement hosted by the United Nations (U.N.) that covers different aspects of the regulation over the spaces and activities in the ocean. This treaty divides the sea into “fictional” spaces and regulates policy issues such as environmental control, fishery protection, fight against piracy, and marine scientific research. UNCLOS ratification process opened for signature in 1982, and the treaty got into force on November 16, 1994, according to the provisions of its article 308 that established that the treaty would get in force twelve months after the date of deposit of the sixtieth instrument of ratification. To date, 168 nation-states, are members of UNCLOS (Arias-Schreiber Pezet, 1984; DOALOS, 2020; Johnston, 1988).

UNCLOS's extension and complexity follow the diversity of interests that coexist in an interrelated manner and the international attempt to find a global solution for the problems related to the law of the sea. In agreement with this international claim, UNCLOS was baptized as a ”constitution for the oceans,” because it sets out the rules for legal governance of the activities conducted in the sea and the institutions that must oversee those activities (WOR, 2010).

UNCLOS is also the result of more than 100 years of negotiations, three conferences on the law of the sea hosted by the U.N., one by the League of Nations, and 2000 years of customary law and state practice (Vargas-Leon, 2017). UNCLOS's main characteristic is the creation of ”fictional juridical spaces,” legal zones where coastal nation-states sovereignty decreases with increasing distance of the coast. In these zones, UNCLOS defines rights and obligations from nation-states and the ”international community,” from coast to coast and from the surface to the deep sea. This policy is known as ”maritime jurisdiction” (Arias-Schreiber Pezet, 1984) . The juridical spaces created by UNCLOS are (1) internal waters, (2) territorial seas, (3) the contiguous zone, (4) the exclusive economic zone (EEZ), (5) archipelagic waters, (6) the continental shelf, (7) the high seas and the (8) Zone (Rothwell, Oude Elferink, Scott, & Stephens, 2015; Tanaka, 2012). The maritime jurisdiction policy is defined as the allocation of sovereign rights in favor of nation-states in each sea space created by UNCLOS, even in international spaces (“High Seas” and “The Zone”), where theoretically, no nation-state has sovereign rights (Ferrero Rebagliati, 1962).

UNCLOS has two complementary agreements to regulate the international sea spaces where no rights are allocated to any nation-state, but to what UNCLOS calls the "humankind" (Brownlie, 2008; Churchill & Lowe, 1999):

1. Regarding the "Zone" (international seabed): Agreement relating to the Implementation of Part XI from 1994, in force since 1996
2. Regarding the "High Seas" (international waters): Straddling Fish Stocks Agreement (formally, the Agreement for the Implementation of the Provisions of UNCLOS relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks) from 1995, in force since 2001

This paper will focus on some of the provisions of the main treaty from 1982 and the agreement related to the high seas. The provisions of the original treaty from 1982 and the addendums will be used to compare how the nation-states created rules to protect the international traffic and its carriers, and how those rules can be used today to protect the Internet infrastructure.

B. A Look into the High Seas

Traditionally the international law defined the high seas as an international space common to all nation-states to conduct regular activities acknowledged by UNCLOS. However, nation-states cannot claim sovereignty rights in the high seas, except for UNCLOS cases. In this context, high seas are defined as all sections of the sea not included in the spaces where coastal nation-states retain some sovereignty rights (Churchill, 1983)[2].

[2] **United Nations Convention on the Law of the Sea**
PART VII.- High Seas
Section 1. General Provisions
Article 86.- Application of the provisions of this Part
The provisions of this Part apply to 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. This article does not entail any abridgment of the freedoms enjoyed by all States in the exclusive economic zone in accordance with article 58

All the mentioned concepts, the economic exclusive zone[3], the territorial sea[4], the internal waters[5] or the archipelagic waters are fictional spaces where the nearest coastal state retains some sovereignty rights. Nevertheless, UNCLOS acknowledges the right of freedom of navigation for all nation-states at least in the economic exclusive zone (Brownlie & Crawford, 2012; R. Churchill, 1983).

Despite UNCLOS provisions, there are constant sovereignty claims of nation-states over the sea. Governments, acting on behalf of their nation-states, frequently try to extend their sovereignty and reduce the high seas' surface. By 2014, the high seas represented 64% of the ocean (Katona, 2014). As mentioned before, UNCLOS got in force in 1994. Therefore, the coexistence between the high seas and other sea spaces where coastal states remain a highly controversial international problem even in the twenty-first century. This form of partial sovereignty "(...) is still in the process of being shaped thus forcing even a great power that tries to project power in these areas or deny them to others (...)" (Rubin & Eiran, 2017, p. 14).

The high seas' main characteristics include equality, exclusive use for peaceful purposes, and invalidity of sovereignty claims. On the other hand, nation-states also have rights in the high seas. These rights are exceptions to the invalidity of sovereignty claims in the high seas. Freedom of the high seas include: (1) freedom of navigation, (2) freedom of overflight, (3) freedom to lay submarine cables and pipelines, subject to Part VI, (4) freedom to construct artificial islands and other installations permitted under international law, subject to Part VI, (5) freedom of fishing, subject to the conditions laid down in section 2 and (6) freedom of scientific research, subject to Parts VI and

[3] **United Nations Convention on the Law of the Sea**
Part V.- Economic Exclusive Zones
Article 58.- Rights and duties of other States in the exclusive economic zone
1. In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention.
2.Articles 88 to 115 and other pertinent rules of international law apply to the exclusive economic zone in so far as they are not incompatible with this Part.
3.In exercising their rights and performing their duties under this Convention in the exclusive economic zone, States shall have due regard to the rights and duties of the coastal State and shall 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 in so far as they are not incompatible with this Part.

[4] **United Nations Convention on the Law of the Sea**
Section 1. General Provisions
Article 2.- Legal status of the territorial sea, of the air space over the territorial sea and of its bed and subsoil
1.The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.
2.This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.
3.The sovereignty over the territorial sea is exercised subject to this Convention and to other rules of international law.
Section 2.- Limits of the Territorial Sea
Article 3.- Breadth of the territorial sea
Every State has the right to establish the breadth of its territorial sea up to a limit not exceeding 12 nautical miles, measured from baselines determined in accordance with this Convention.

[5] **United Nations Convention on the Law of the Sea**
Section 2.- Limits of the Territorial Sea
Article 8.- Internal waters
1. Except as provided in Part IV, waters on the landward side of the baseline of the territorial sea form part of the internal waters of the State.
2. Where the establishment of a straight baseline in accordance with the method set forth in article 7 has the effect of enclosing as internal waters areas which had not previously been considered as such, a right of innocent passage as provided in this Convention shall exist in those waters.

XIII. All the freedoms may be exercised by all nation-states with due respect to the interests of other nation-states (Guilfoyle, 2015). For the purposes of this research we will focus in the freedom of navigation.

The bed of the high seas is known as the "International Seabed Area," also called the "Zone" or the "Area." The legal framework that governs the high seas depends on the principle known as the "freedom of the high seas," which is based at the same time in two core principles: (1) a ship of any nation-state may freely navigate in the high seas and (2) the nation-state of the ship's nationality has exclusive jurisdiction over the ship that sails in the high seas (Churchill, 1983; Sohn et al., 2010). The freedom of the high seas is included in article 87 of the rules of UNCLOS[6].

Moreover, UNCLOS also acknowledges in its article 90 that every nation-state of the world, coastal or land-locked, "has the right to sail ships flying its flag on the high seas." The rules of the high seas are the outcome of balancing the requirements of coastal state control under the regime of territorial seas (where nation-states can exercise jurisdiction as if they were in their territory, with only one exception, the innocent passage) and the requirements of freedom of navigation, international traffic, and trade. A concept opposed to the high seas is the "Blockade Zones," where ships are subject to the blockade. This is a zone created and imposed usually, but not exclusively, for times of war (Johnston, 1988).

C. The Freedom of navigation and the Flagship Rule

The freedom of navigation was negotiated to ensure international trade and commerce across the oceans. Defenders of the principle advocated the freedom of commerce on the basis of the freedom of the seas and free international traffic. Since early negotiations, the freedom of navigation in the high seas was characterized by the political and economic interests of nation-states (Rothwell et al., 2015).

As a consequence of the freedom in the high seas, all nation-states, despite being coastal or landlocked, have the right that their vessels use their flag in the high seas. Only ships that can claim a nationality can sail in the high seas. These ships are subject to the control of the nation-state under whose flag they sail. Each nation-state establishes a ship's requirements to be considered one of its own. The requirement of carrying a flagship is known as the "flagship rule" (Messeguer Sanchez, 1999).

Ships sailing under the flag of a nation-state have the right to navigate across the high seas without interference from any other nation-state. This right also prevails within the economic exclusive zone, where the nearest coastal state retains some sovereign powers for economic purposes. The protection also covers warships and ships owned and operated by nation-states with non-commercial purposes.

[6] **United Nations Convention on the Law of the Sea**
PART VII.- High Seas
Section 1. General Provisions
Article 87.- Freedom of the high seas
1.The high seas are open to all States, whether coastal or land locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and by other rules of international law. It comprises, inter alia, both for coastal and land-locked States:
(a) freedom of navigation;
(b) freedom of overflight;
(c) freedom to lay submarine cables and pipelines, subject to Part VI;
(d) freedom to construct artificial islands and other installations permitted under international law, subject to Part VI;
(e) freedom of fishing, subject to the conditions laid down in section 2;
(f) freedom of scientific research, subject to Parts VI and XIII.
2.These freedoms shall be exercised by all States with due regard for the interests of other States in their exercise of the freedom of the high seas, and also with due regard for the rights under this Convention with respect to activities in the Area.

In 1949, the International Court of Justice (ICJ) recognized in the Corfu Channel1 case that nation-states have a right to send their warships through straits used for international navigation even in times of peace without previous authorization of the nearest coastal state. This principle would remain even today.

These ships only may be stopped and boarded on the high seas by another warship or law enforcement vessel if there are reasonable grounds to suspect that such ship is engaged in acts of piracy or slave trade. In opposition to the principle of freedom of navigation, there is the principle of sovereignty that seeks to safeguard coastal nation-states' interests. This principle of sovereignty promotes the extension of national jurisdiction into offshore spaces and advocated for the "territorialisation" of the oceans (Tanaka, 2012) .

III.
The Rules of UNCLOS, the IXPs and the Internet

Rules about freedom of navigation provide elements of international law that may help protect the IXPs and the international Internet traffic they support. The next paragraphs will develop this idea.

A. Rules for International Connections: A Look into the Boomeranging Process

IXPs facilitate local and international traffic. In this context, although boomeranging may not deem as the most convenient thing for economic and security purposes, it is he way IXPs operate specially when there are developing nation-states involved. During the COVID 19 crisis, as the Internet traffic increased, so it was boomeranging process. Therefore, there was a higher volume of Internet packets traveling worldwide through multiple territories and jurisdictions.

According to the provisions of UNCLOS, the freedom of navigation is not only a rule within the high seas, where nation-states lack sovereignty rights, but also in: (1) the EZZ, where nation-states keep some sovereignty rights for economic purposes and (2) the contiguous zone, where nation-states keep some sovereignty rights for customs purposes. Finally, in the territorial sea, where nation-states exercise sovereignty rights as if they were in their territories, they have a restriction imposed by international law, the right of "innocent passage."[7] Although nation-states seek to limit foreign ships' access into their territorial seas (mostly because they are immediately adjacent to their territories), they cannot stop it completely.

These rules of international law in UNCLOS favored international traffic, even in spaces where nations keep partial or total sovereignty rights. The table below compares the different spaces UNCLOS recognizes, and the level of control over the traffic nation-states have in each one of those spaces.

Table 1. The state of the international traffic in UNCLOS

Space	Sovereignty of Nation-States	Treatment of the Traffic
Territorial Sea	Complete	Limited restrictions
Contiguous Zone	Partial	No restrictions
Economic Exclusive Zone	Partial	No restrictions
High-Seas	None	No restrictions

[7] **United Nations Convention on the Law of the sea of 1982**
Part II.- Territorial Sea and Contiguous Zone
Section 3. Innocent Passage in the Territorial Sea
Subsection A. Rules Applicable to all Ships
Article 17.- Right of innocent passage
Subject to this Convention, ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea.

There have been academic attempts to apply UNCLOS rules into the Internet and cyberspace to include a Westphalian approach to the Internet governance debate. This means to impose sovereignty rules over the Internet infrastructure and indirectly, favoring the Internet fragmentation. Nevertheless, even if that were the purpose, freedom of navigation is a restriction to nation-states' sovereignty rules and stands even in international treaties.

As stated at the beginning of this section, boomeranging may not be ideal for security purposes, but it is how the Internet traffic works, especially for nation-states that lack enough IXPs. Therefore, although boomeranging may not disappear, the international law rules related to the freedom of navigation provide some guidelines to protect the integrity of the Internet traffic independently of the location.

B. The IXPs and the Peering Process

As mentioned before, IXPs allow different networks to interconnect directly in a process known as "peering." Peering is the more usual way to exchange traffic on the Internet, and it is possible because of the IXPs. In this context, by protecting the traffic, the principle of freedom of navigation also protects the IXPs, because they exist only to facilitate the traffic. In consequence, it is not possible to protect the traffic, if the means that make possible the traffic are not protected as well.

Indirectly, it is possible to state that the principle of freedom of navigation also protects the IXPs because their presence is the only thing that guarantees the peering and preserves the way Internet networks connect. Although some claims may intent to assimilate IXPs to ports, such simile lacks legal foundations. UNCLOS considers ports as part of the internal waters of every nation-state where the nation-state of the coast has complete sovereignty to enforce domestic regulations even to stop the traffic of any ship. In this context, ports lack of international protection.

C. A Caveat in the Principle

Although this paper expects to prove why the freedom of navigation may serve as a principle to protect Internet traffic, it is also important to point out a negative side.

The main requirement to exercise the right of freedom of navigation is the "flagship rule," this means that ships sailing through the ocean must carry a flag, either the flag of the nation-state where they belong or a flag of convenience (used mostly for business purposes). The flagship rule is tied to the sovereignty of the nation-state the flag represents. Even if this principle does not affect the traffic itself but to the carriers (of cargo or Internet packets), it is a warning for the nation-states sovereignty's potential intrusion.

IV.
Conclusions

UNCLOS is the outcome of 2000 years of state practice and negotiations balancing the power among nation-states. UNCLOS rules address sovereignty issues that nation-states face beyond the borders of their traditional territorial borders. Nevertheless, principles like the freedom of navigation show that there are exceptions to the powerful rules nation-states imposed. The acknowledgment that the international traffic must be respected even in zones where nation-states keep limited or unrestricted sovereignty rights highlights the importance of keeping the integrity of the sender, receiver, and whatever is sent or received.

Similar concerns exist within the Internet domain where governments (for the most part) attempt to control or even block the Internet traffic at their convenience.

The COVID 19 crisis revealed the importance of the Internet in human lives and the Internet infrastructure dependence that supports all human activity during the lockdown. IXPs played a critical role as they are the ones that rout and support the high volumes of Internet traffic this crisis provoked. Since IXPs play such a critical role, it is imperative to find ways to protect them and the so precious Internet traffic they support.

V.
References

Arias-Schreiber Pezet, A. (1984). El Derecho del Mar [Law of the Sea]. *El Derecho Del Mar. Academia Diplomatica Del Peru.*

Bottemiller, H., & Crampton, L. (2020). Trump deems farmworkers “essential” but not safety rules for them. That could threaten the food supply. Retrieved May 22, 2020, from POLITICO website: https://www.politico.com/news/2020/05/12/trump-farmworkers-essential-coronavirus-safety-250142

Brownlie, I. (2008). *Principles of public international law* (7th ed.). Oxford ;;New York: Oxford University Press.

Brownlie, I., & Crawford, J. (2012). *Brownlie’s principles of public international law* (8th ed.). Retrieved from https://www.worldcat.org/title/brownlies-principles-of-public-international-law/oclc/1081152561&referer=brief_results

Churchill, R. (1983). *The law of the sea*. Manchester; Dover N.H.: Manchester University Press.

Churchill, R. R., & Lowe, A. V. (1999). *The Law of the Sea*. Manchester University Press.

Clark, C. (2016). NATO Declares Cyber A Domain. Retrieved October 4, 2016, from Breaking Defense website: http://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/

Clark, D., Berson, T., Lin, H. S., & National Research Council (U.S.). Committee on Developing a Cybersecurity Primer. (2014). *At the Nexus of Cybersecurity and Public Policy*. https://doi.org/10.17226/18749

Cloudfare. (2020a). What is an autonomous system? | What are ASNs? Retrieved September 14, 2020, from Cloudfare website: https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/

Cloudfare. (2020b). What is an Internet exchange point? How do IxPs work? Retrieved March 4, 2018, from Cloudfare website: https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/

Cucinotta, D., & Vanelli, M. (2020). WHO declares COVID-19 a pandemic. *Acta Biomedica*, Vol. 91, pp. 157–160. https://doi.org/10.23750/abm.v91i1.9397

DeNardis, L. (2013). *Internet Points of Control as Global Governance* (No. 2). Retrieved from https://www.cigionline.org/sites/default/files/no2_3.pdf

DeNardis, L. (2014). *The Global War for Internet Governance*. Retrieved from www.jstor.org/stable/j.ctt5vkz4n

DOALOS. (2020). Chronological lists of ratifications of, accessions and successions to the Convention and the related Agreements. Retrieved September 13, 2020, from Division of Ocean Affairs and Law of the Sea (DOALOS) website: https://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm

Fanou, R., Sanchez-Aguero, V., Valera, F., Mwangi, M., & Coffin, J. (2018). *A System for Profiling the IXPs in a Region and Monitoring theirGrowth: Spotlight at the Internet Frontier*. https://doi.org/https://doi.org/10.1002/nem.2056

Ferrero Rebagliati, R. (1962). *Derecho internacional público [Public International Law]*. Lima: Pontificia Universidad Católica del Perú Facultad de Derecho y Ciencias Políticas.

Geneva Internet Platform. (2020). *Editorial Covid-19 & Digital Policy Data Analysis Online*

Meetings. Retrieved from https://dig.watch/sites/default/files/2020-04/DWnewsletter48.pdf

Guilfoyle, D. (2015). The High Seas. In D. Rothwell, A. O. Elferink, K. Scott, & T. Stephens (Eds.), *The Oxford Handbook of the Law of the Sea*. https://doi.org/10.1093/law/9780198715481.001.0001

Haq, N. (2020). IXPs: Keeping Local Infrastructure Resilient during COVID-19. Retrieved September 13, 2020, from Internet Society website: https://www.internetsociety.org/blog/2020/07/ixps-keeping-local-infrastructure-resilient-during-covid-19/

Hernandez, R. (2020). COVID-19's impact on internet traffic in Latin America. Retrieved September 13, 2020, from MDC Data Centers website: https://www.mdcdatacenters.com/company/blog/covid-19s-impact-on-internet-traffic-throughout-latin-america/

ISOC. (2020a). How IXPs are supporting the Internet during COVID-19 | Internet Society. Retrieved September 13, 2020, from Internet Society website: https://www.internetsociety.org/events/how-ixps-are-supporting-during-the-internet-covid-19/

ISOC. (2020b). Internet Exchange Points (IXPs) | Internet Society. Retrieved September 13, 2020, from Internet Society website: https://www.internetsociety.org/issues/ixps/

Johnston, D. M. (1988). *The Theory and History of Ocean Boundary-Making*. Retrieved from https://www.amazon.com/Theory-History-Ocean-Boundary-Making/dp/0773506241

Katona, S. (2014). 2014 Antarctica Regional Assessment : Ocean Health Index.

Lodhi, A., Dhamdhere, A., & Dovrolis, C. (2014). Open Peering by Internet Service Providers: Peer Preference or Peer Pressure? Retrieved October 4, 2020, from IEEE Confeence on Computer Communications website: https://ieeexplore-ieee-org.ezproxy.library.tufts.edu/stamp/stamp.jsp?tp=&arnumber=6848203

McKeay, M. (2020a). Parts of a Whole: Effect of COVID-19 on US Internet Traffic. Retrieved September 12, 2020, from Akamai Security Intelligence and Threat Research Blog website: https://blogs.akamai.com/sitr/2020/04/parts-of-a-whole-effect-of-covid-19-on-us-internet-traffic.html

McKeay, M. (2020b). The Building Wave of Internet Traffic. Retrieved September 12, 2020, from Akamai Security Intelligence and Threat Research Blog website: https://blogs.akamai.com/sitr/2020/04/the-building-wave-of-internet-traffic.html

Mclaughlin, A. (2002). *The Law, Politics, and Economics of Interconnection*. Retrieved from https://cyber.harvard.edu/mclaughlin/presentations/mclaughlin-eaif-04aug02.pdf

Medows, D. B. (2012). The Sound of Silence: The Legality of the American Kill Switch Bill. *Journal of Law, Technology & the Internet*, *4*(1), 59–79.

Messeguer Sanchez, J. L. (1999). *Los Espacios Maritimos en el Nuevo Derecho del Mar [Sea Spaces in the New Law of the Sea]* (Marcial Po). Retrieved from http://www.casadellibro.com/libro-los-espacios-maritimos-en-el-nuevo-derecho-del-mar/9788472486775/657385

Mueller, M. (2010). *Networks and States: the Global Politics of Internet Governance*. Cambridge Mass.: MIT Press.

Netnod. (2018). What is peering. Retrieved February 27, 2018, from NETNOD website: https://www.netnod.se/ix/what-is-peering

Netnod. (2019). What is an IXP? Retrieved September 23, 2019, from Netnod website: https://www.netnod.se/ix/what-is-an-ixp

Nomikos, G., Sermpezis, P., & Dimitropoulos, X. (2017). Re-mapping the internet: Bring the IXPs into play: www.inspire.edu.gr/ixp-map. *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 910–915.

https://doi.org/10.1109/INFCOMW.2017.8116497

Norton, W. B. (2014). *What is an Internet Exchange Point?* Retrieved from http://drpeering.net/FAQ/What-is-an-Internet-Exchange-Point.php

PCH. (2019). Internet Exchange Directory. Retrieved June 17, 2019, from Packet Clearing House website: https://www.pch.net/ixp/dir

Rothwell, D., Oude Elferink, A. G., Scott, K. N. (Karen N., & Stephens, T. (Law teacher). (2015). *The Oxford handbook of the law of the sea*. Retrieved from https://www.google.com/books/edition/The_Oxford_Handbook_of_the_Law_of_the_Se/gbS6BwAAQBAJ?hl=en&gbpv=0

Rubin, A., & Eiran, E. (2017). Legal Sea Feuds: The Shrinking of the Command and the Legalization of the Commons. *58th Annual Convention of the International Studies Association*. Baltimore, MD.

Sanchez, C. (2018). Does Establishing More IXPs Keep Data Local? Brazil and Mexico Might Offer Answers. Retrieved June 19, 2019, from ORACLE Dyn website: https://dyn.com/blog/does-establishing-more-ixps-keep-data-local-brazil-and-mexico-might-offer-answers/

Schmidt, M. (2017). Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't.

Sohn, L. B., Sohn, L. B., Juras, K. G., Noyes, J. E., Franckx, E., & West (Firm). (2010). *The law of the sea in a nutshell*.

Steven, B. (2001). Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of the cyberspace. *Naval Law Review*, *48*, 56–83. Retrieved from http://unclosdebate.org/evidence/1115/unclos-provisions-transit-passage-provide-good-model-international-agreements

Tanaka, Y. (2012). *The international law of the sea*. Cambridge University Press.

Tribaldos, F., & Silva, C. (2020). LATAM Spanish Webinar: Ciberseguridad en Latinoamérica durante COVID-19. Retrieved September 14, 2020, from Cloudflare website: https://www.cloudflare.com/en-ca/webinars/ciberseguridad-en-latinoamerica-durante-covid-19/

US Signal. (2020). Know Your Options: Peering, IP Transit and Direct Internet. Retrieved October 4, 2020, from US Signal website: https://ussignal.com/blog/know-your-options-peering-ip-transit-direct-internet-access

van Beijnum, I. (2011). How Egypt did (and your government could) shut down the Internet | Ars Technica. *Ars Technica LAW & DISORDER / CIVILIZATION & DISCONTENTS*. Retrieved from http://www.bgp4.as/internet-exchanges

Vargas-Leon, P. A. (2017). Implications of the application of the "hot pursuit" principle in the cyberspace: an analysis of the case "Microsoft v. United States of America." *Understanding Change in World Politics ISA's 58th Annual Convention*. Baltimore, MD.

Wooding, B. (2020). Wanted: More Local Bandwidth for COVID-19 Internet Usage Spike. Retrieved October 4, 2020, from Team ARIN website: https://teamarin.net/2020/05/14/wanted-more-local-bandwidth-for-covid-19-internet-usage-spike/

WSIS. (2005). WSIS: Tunis Agenda for the Information Society. Document: WSIS-05/TUNIS/DOC/6(Rev. 1)-E. Retrieved August 19, 2017, from World Summit on the Information Society. Geneva 2003-Tunis 2005 website: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html