IMPLICATIONS OF THE APPLICATION OF THE "HOT PURSUIT" PRINCIPLE IN THE CYBERSPACE: AN ANALYSIS OF THE CASE "MICROSOFT V. UNITED STATES OF AMERICA"

PATRICIA A. VARGAS-LEON
PHD CANDIDATE
SYRACUSE UNIVERSITY

ABSTRACT

This paper analyzes the implications of applying one of the mechanisms for defense sovereignty contained in the "United Nations Convention on the Law of the Sea" (UNCLOS), known as "hot pursuit," into the cyberspace. For this purpose, this paper uses as a case study the analysis of the legal controversy, "Microsoft vs. United States of America," also known as the "Microsoft Ireland" case.

The Microsoft Ireland case occurred in a time when firms and companies store their data in different servers around the world and retrieve it at will. This is also a case that exemplifies the collision between different jurisdictions when nation-states try to exercise their legal powers into the cyberspace. Facing this scenario, and taking into account a long-time suggested academic proposal of comparing policies over the sea and the cyberspace, this paper presents a concrete opportunity of analyzing the possibility of applying some of the elements of the law of the sea into the cyberspace policy debate.

Taking the "Microsoft Ireland" case as a case study, this paper will: a) provide an overview of how the hot pursuit mechanism has been understood by the international court of justice (ICJ) and the International Tribunal of the Law of the Sea (ITLOS), b) analyze the arguments and allegations of the parties involved in the Microsoft case about why one nation-state's sovereignty should be applicable or not beyond the borders of its own territory, and c) analyze the possible repercussions of applying the hot pursuit, a mechanism used in the past by nation-states when they were trying to regulate a space beyond their national jurisdiction and apply their sovereignty into the cyberspace (an electronic medium that cannot be govern by any nation-state).

It is important to clarify that this paper does not advocate for a governance model for the cyberspace based in UNCLOS and the hot pursuit principle. Findings expect to clarify the diverse opinions this matter has generated and learn from previous experiences where governments were involved trying to regulate a space beyond their traditional territorial sovereignty.

1. CONTEXT

In today's world there is no treaty that regulates the Internet or the cyberspace. Although the multi-stakeholder model has been successful in keeping the Internet free of a unique point of control, there are still nation-states and individuals who advocate for a government-based-model. In the midst of the battle during the ICANN transition, some

governments (like Russia, India, Iran and Saudi Arabia) argued in favor of the regulation of the cyberspace in hands of an international organization like the ITU (Moyer, 2016; Schaller, 2014). Reasons for these opposing views are related to the different conceptions nation-states have over what should be the governance model for a resource beyond the traditional borders of their territories and, over which nobody has sovereign control. In this context, the question about the possibility of reaching a global and common governance regime for the cyberspace seems uncertain.

Taking these characteristics into account, and considering the cyberspace a global resource beyond the traditional nation-states' territorial borders, academics (Kalpokienė & Kalpokas, 2012; Sechrist, 2010) and non-academics (Barcomb, 2013; Steven, 2001) have called to apply similar policies to the ones contained in the United Nations Convention on the Law of the Sea (UNCLOS) to the cyberspace. Comparison for governments' regulatory practices in both spaces lies in the fact that, in the past, the sea was considered a space for communications, economic production, transportation and war, many of the characteristics attributed to cyber-space today (Steinberg, 2001). For other academics the relationship between the sea and the cyberspace is one related to concepts of war and state-practice: a) for the first ones, wars are traditionally fought over territory, but the concept of territory has evolved to incorporate five domains: land, air, sea, space, and, the cyberspace (Sheng, 2014), and b) for the latter ones, the existence of UNCLOS (and similar treaties) proofs the existence of a state practice of claiming any space beyond nation-states' territorial borders (von Heinegg, 2012).

For the purpose of making an analysis, this paper will include focus in one of the policies contained in UNCLOS: the hot pursuit principle. The following paragraphs will explain the main concepts to be used in this paper, such as "Nation-states," "Cyberspace," "Hot Pursuit" and a description of UNCLOS. More important we also will explain why these concepts built on the basis of the traditional sovereignty and basic for the survival of nation-states became so controversial.

2. Nations-states: No Longer the Only Ones in the International Realm

According to the classic rules of international law, a nation-state is an entity that possesses international rights and obligations and has the capacity to: a) maintain its rights by making international claims, b) negotiate and sign treaties and agreements valid at an international level and, c) enjoy privileges and immunities from national jurisdiction (Rosenne, 2007). In order to have the condition of "nation-state," some specific characteristics, known as "elements of statehood," are required. Those elements of statehood include the existence of a government, population, territory and sovereignty (Brownlie, 2012).

The enjoyment of a national jurisdiction is subordinated to the existence of territorial borders, as nation-states only can exercise jurisdiction within the borders of their own territory (Benadava, 1982). In the same way, legal competence is defined in terms of "sovereignty" and "jurisdiction" (Brownlie, 2003). In 1949, the International Court of Justice (ICJ) concluded that "between independent States, respect for territorial

sovereignty is an essential foundation of international relations"[1] (IDRC, p.6, 2001). Thirty years later, the ICJ would clarify its original statement by referring to "the fundamental principal of state sovereignty on which the whole of international law rests."[2] In this way, the general principle of international law reads that nation-states are entities with the capacity to exercise jurisdiction (the application of their own legal order) through the actions of their governments over the population within the borders of their own territory (J. Crawford, 2013). This will be the major point of conflict with the concept of cyberspace, because the latter is unrestricted to a particular geographic location and, at the same time, is available to anyone, anywhere (Johnson, 1999).

From a social sciences point of view, nation-states are the main suppliers of public governance and remain as very powerful institutions (Mueller, 2002, 2010). Nation-states main strength is the exercise of their control (their coercive capacity) by creating institutions, rules and regulations based in the traditional claim of guaranteeing their own survival. As it was in past centuries, nation-states still make decisions according their interests and the position of power they have in the international community (Bobbitt, 2002; Khan, 2007).

During the 15th century, nation-states consolidate as "solo" actors in the international realm and they became very powerful, being for centuries the only source of power, law and policy. Since the Peace of Westphalia in 1648 the current international system has been based upon the principle of territorial sovereignty (Fehlinger, 2014). However in 1949 things started to change. That year, in an advisory opinion, the ICJ[3] established, after the assassination of the Count Folke Bernadotte, that the United Nations (UN) had "international personality" like a nation-state would have. The ICJ then acknowledged the existence of other actors in the international realm besides the classic nation-states. The central question the ICJ analyzed was whether the "capacity to bring an international claim" is an attribute only from nation-states or it also can be attributed to international organizations. The court stressed that although the UN international legal personality is not identical to that of a nation-state since, the organization was "capable of possessing international rights and duties" and had "capacity to maintain its rights by bringing international claims" (ICJ, p.1, 1949).

Additionally, since early 1990s the dominant view in the international realm was the transformation of the world through non-state actors, a process known as "globalization." New technologies, in particular ICT and a non-territorial new medium, like the cyberspace, were supposed to supersede nation-states' old institutions and create new and more efficient ones. However, it is also true that these hopes may have underestimated the nation-states' role and its institutions, and the difficulty of replacing them. The current world financial crisis discredited the role of the market and called again for the restoration of the nation-state power; this situation has been well used by authoritarian regimes on behalf of the national sovereignty and democracy (Mazower, 2014).

[1] ICJ, the Corfu Channel Case (Merits), ICJ Rep., 1, at p. 35 (1949).
[2] ICJ, Military and Paramilitary Activities in and against Nicaragua (Merits), ICJ Rep., at p.14 (1986)
[3] ICJ Advisory Opinion, Reparation for Injuries Suffered in the Service of the United Nations, at p. 1 (1949).

3. CYBERSPACE: A CHALLENGE FOR THE TRADITIONAL INTERNATIONAL ORDER

As mentioned in the introduction, considering the cyberspace as a space beyond the traditional borders of nation-states, and also constantly subject to sovereignty claim, academics and non-academics have called to apply similar policies to the ones contained in UNCLOS to the cyberspace. In the U.S., military called to move from "sea power" to "cyber power" and, in June 2016, NATO announced that the 28- member alliance agreed to declare cyber an operational domain, like sea, air and land (Barcomb, 2013; Clark, 2016). So many policy decisions leads us to ask two important questions: what is the cyberspace and why is it so important for nation-states?

According to the American National Standard T1.523-2001 for Telecommunications, the cyberspace is the "impression of space and community formed by computer networks, and their users; the virtual 'world' that Internet users inhabit when they are online." (as citey by Rosenne, p.328-329, 2004). The cyberspace also has a "global connotation," as it was defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DoD, p.58, 2016).

Differently from a concept built on the basis of territorial borders, and opposed to the regulated traditional state relations, the cyberspace is "aterritorial,"[4] invisible, unidentifiable, irrefragable, cannot be felt or identified in any way and it does not have natural or physical characteristics. It is also characterized by anonymity and ubiquity (Johnson, 1999; Kulesza, 2012; Rosenne, 2004; von Heinegg, 2012). For some academics, the law cannot control the cyberspace, only can control the use that human beings put to it. For this particular characteristic, many legal scholars consider the cyberspace a "perplexity" for the classic theory of international law (Kulesza, 2012; Rosenne, 2004).

Governments on the other hand, have different expectations. Just to set an example, in 2011, when President Barak Obama declared the cyberspace as a "national asset," and also pointed out that the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace" (White House, p.9, 2011). Although the White House acknowledges that particular attributes of networked technology require additional work to clarify how these norms apply, it also calls to work internationally to reach consensus regarding how norms of behavior apply to cyberspace. This statement follows the premise that the first step to reach consensus is applying the broad expectations of peaceful interstate conduct within the cyberspace (White House, 2011).

[4] "Aterritoriality" refers to the lack of applicability of the territorial criteria for activities that occur in the cyberspace (Kulesza, 2012). According to Rosenne, differently from other spaces, the "cyberspace is invisible, unidentifiable, irrefragable, and cannot be felt or identified in any way: it has no known natural characteristics. It is simply there, and used by electromagnetic impulses made by human beings. The law can control the use that human beings put to it, and its use can be a subject of agreement." (Rosenne, p.349, 2004).

4. United Nations Convention on the Law of the Sea from 1982 (UNCLOS): "A Constitution for the Oceans"

UNCLOS is a multilateral treaty that covers multiple aspects of the regulation of the spaces and activities in the ocean, such as division of the sea into "fictional" spaces, environmental control, fishery protection, fight against piracy and marine scientific research, among others. UNCLOS was opened for signature in 1982, and entry into force on November 16, 1994. UNCLOS is known as a "constitution for the oceans,"[5] because it sets out the framework for legal governance within which all activities in the oceans must be conducted, and the institutions that must oversee those activities (WOR, 2010). Until September 2016, 168 governments ratified UNCLOS on behalf of their nation-states (DOALOS, 2016).

UNCLOS is also the result of more than 100 years of negotiations, three conferences on the law of the sea hosted by the United Nations, one by the League of Nations, and 2000 years of customary law and state practice (Messeguer Sanchez, 1999). The main characteristic of UNCLOS is the creation of "fictional spaces," legal zones where coastal nation-states sovereignty decreases with increasing distance of the coast. In these zones, UNCLOS defines nation-states' rights and obligations from coast to coast and from the surface to the deep sea" (Arias-Schreiber Pezet, 1984). This policy is known as "maritime jurisdiction" (See Figure 1 and table 1, in pages 9 and 10), and is a "virtual fragmentation" of the oceanic waters.

UNCLOS has two complementary agreements to regulate international fragments of the sea where no rights are assigned to any nation-state, but to the humankind itself:

a. Regarding the "Zone" (international seabed): Agreement relating to the Implementation of Part XI from 1994, in force since 1996
b. 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

The "hot pursuit" principle is one of the most controversial policies included in UNCLOS, and it will be the subject of analysis in this paper.

4.1. Hot Pursuit: a Policy Beyond the Territorial Sovereignty

Hot pursuit, also known as "fresh" or "immediate pursuit," refers to the urgent and direct pursuit of a criminal suspect by law enforcement officers under rules of international. Such a situation grants to the officers in command powers they would not have in normal

[5] The phrase "A Constitution for the Oceans" is attributed to Ambassador Tommy Koh in the statements made on 6 and 11 December 1982 at the final session of the III Conference on the Law of the Sea, in M. H. Nordquist (ed), United Nations Convention on the Law of the Sea 1982, A Commentary, vol. 1, (Center for Oceans Law and Policy UVA, P.11, 1985).

circumstances (Poúlantzas, 2002; Williams, 1939). In this way, the hot pursuit is a classic principle of the doctrine on the law of the sea, and has been recognized as part of the practices and opinions of modern nation-states. The doctrine of the hot pursuit principle evolved through history and developed as customary international law. Later on, the principle itself obtained legal international recognition by being included in UNCLOS in 1982 (Tasikas, 2004).

In terms of UNCLOS, the hot pursuit principle is defined as the right of a nation-state to pursue and seize a non-national vessel suspected of having committed a crime within the nation-state's internal waters and territorial sea (where the nation-state has sovereign rights) and arrest it, even if the vessel moves onto the high sea (where the coastal nation-state has no sovereign rights) (Churchill & Lowe, 1999). The territorial sea is the extension of seawaters adjacent to coastal states until the distance of 12 miles. According to the rules of UNCLOS, nation-states are sovereign in the territorial sea and the internal waters, as if they were in their own territory[6] (Messeguer Sanchez, 1999).

The hot pursuit principle of a foreign ship may be undertaken when there are reasons for competent authorities of the coastal nation-state to believe that a foreign ship violated its laws and regulations. The main characteristics of the pursuit are (Churchill & Lowe, 1999):

a. Pursuit must start when the foreign ship or one of its boats is within the internal waters, the territorial sea or the contiguous zone of the pursuing nation-state.
b. Pursuit must be continuous and only can continue outside the territorial sea if there were no interruptions and there was a warning, visual or auditory signal for the crew of the prosecuted ship.
c. Pursuit must end as soon as the chased ship enters into the territorial sea of its own nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory)

[6] UNITED NATIONS CONVENTION ON THE LAW OF THE SEA OF 1982
PART II.- TERRITORIAL SEA AND CONTIGUOUS ZONE
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.

As established by the International Tribunal for the Law of the Sea (ITLOS)[7] in the case of the merchant vessel M/V Saiga[8], conditions to exercise the hot pursuit are set out in the article 111 of UNCLOS[9]. Such conditions must be accumulative; i.e., each one has to be satisfied in order to claim the principle (Karim, 2011). In the Corfu Channel case[10], the ICJ recognized that the use of force is allowed when the pursued vessel subject to arrest refuses to stop. The idea of using necessary force is authorized despite of the fact that it is a serious infringement on the high seas freedom (Allen, 1989). On the other hand, as established in the article 110(3) of UNCLOS, if a nation-state engages in an unjustified hot pursuit, such nation-state will be required to compensate the vessel owner for any loss they suffered.

Main critiques again the hot pursuit claim that the principle allows a nation-state to enforce its laws and regulations against non-national ships that flee onto the high seas where nation-states lack jurisdiction (Reuland, 1993; Tasikas, 2004). Defenders of the principle claim that, if the hot pursuit empowers a coastal nation-state to pursue a vessel that has violated

---

[7] The International Tribunal for the Law of the Sea (ITLOS) is an independent judicial body created by UNCLOS to solve disputes related to the interpretation and application of the Convention. The Tribunal is composed of 21 independent members and, according the article 21 of its statute, ITLOS has has jurisdiction over any dispute concerning the interpretation or application of the Convention, and over all matters specifically provided for in any other agreement which confers jurisdiction on the Tribunal (International Tribunal for the Law of the Sea, 2016; United Nations, 2016). In practical terms, ITLOS is a parallel jurisdiction to the ICJ, and the final venue to solve a controversy is a matter of decision for the involved parties.

[8] ITLOS, The M/V "SAIGA" (No.2) CASE (SAINT AND VINCENT THE GRENADINES v. Guinea), Judgment, at p.146 (1997).

[9] UNITED NATIONS CONVENTION ON THE LAW OF THE SEA OF 1982
PART VII.- HIGH SEAS
Article 111: Right of hot pursuit
1. The hot pursuit of a foreign ship may be undertaken when the competent authorities of the coastal State have good reason to believe that the ship has violated the laws and regulations of that State. Such pursuit must be commenced when the foreign ship or one of its boats is within the internal waters, the archipelagic waters, the territorial sea or the contiguous zone of the pursuing State, and may only be continued outside the territorial sea or the contiguous zone if the pursuit has not been interrupted. It is not necessary that, at the time when the foreign ship within the territorial sea or the contiguous zone receives the order to stop, the ship giving the order should likewise be within the territorial sea or the contiguous zone. If the foreign ship is within a contiguous zone, as defined in article 33, the pursuit may only be undertaken if there has been a violation of the rights for the protection of which the zone was established.
2. The right of hot pursuit shall apply mutatis mutandis to violations in the exclusive economic zone or on the continental shelf, including safety zones around continental shelf installations, of the laws and regulations of the coastal State applicable in accordance with this Convention to the exclusive economic zone or the continental shelf, including such safety zones.
3. The right of hot pursuit ceases as soon as the ship pursued enters the territorial sea of its own State or of a third State.
4. Hot pursuit is not deemed to have begun unless the pursuing ship has satisfied itself by such practicable means as may be available that the ship pursued or one of its boats or other craft working as a team and using the ship pursued as a mother ship is within the limits of the territorial sea, or, as the case may be, within the contiguous zone or the exclusive economic zone or above the continental shelf. The pursuit may only be commenced after a visual or auditory signal to stop has been given at a distance which enables it to be seen or heard by the foreign ship.
5. The right of hot pursuit may be exercised only by warships or military aircraft, or other ships or aircraft clearly marked and identifiable as being on government service and authorized to that effect.
…

[10] ICJ, the Corfu Channel Case (Merits), ICJ Rep.4, at p. 77 (1949).

its laws onto the high seas, this occurs in order to deny to the offending vessel the opportunity of escape punishment by claiming the of free navigation designed to protect innocent vessels (Allen, 1989).

This is a very similar critique when talking about the cyberspace, where governments (acting on behalf of their nation-states) have acted in two different ways: a) by attempting to expand their sovereignty accessing data stored beyond the borders of their territory (Goldman, 2016) and b) by attempting to keep data within the borders of its own territory (RT, 2014; The Economist, 2015).

FIGURE 1.- THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA (UNCLOS) FROM 1982 MARITIME JURISDICTION AND THE HOT PURSUIT PRINCIPLE

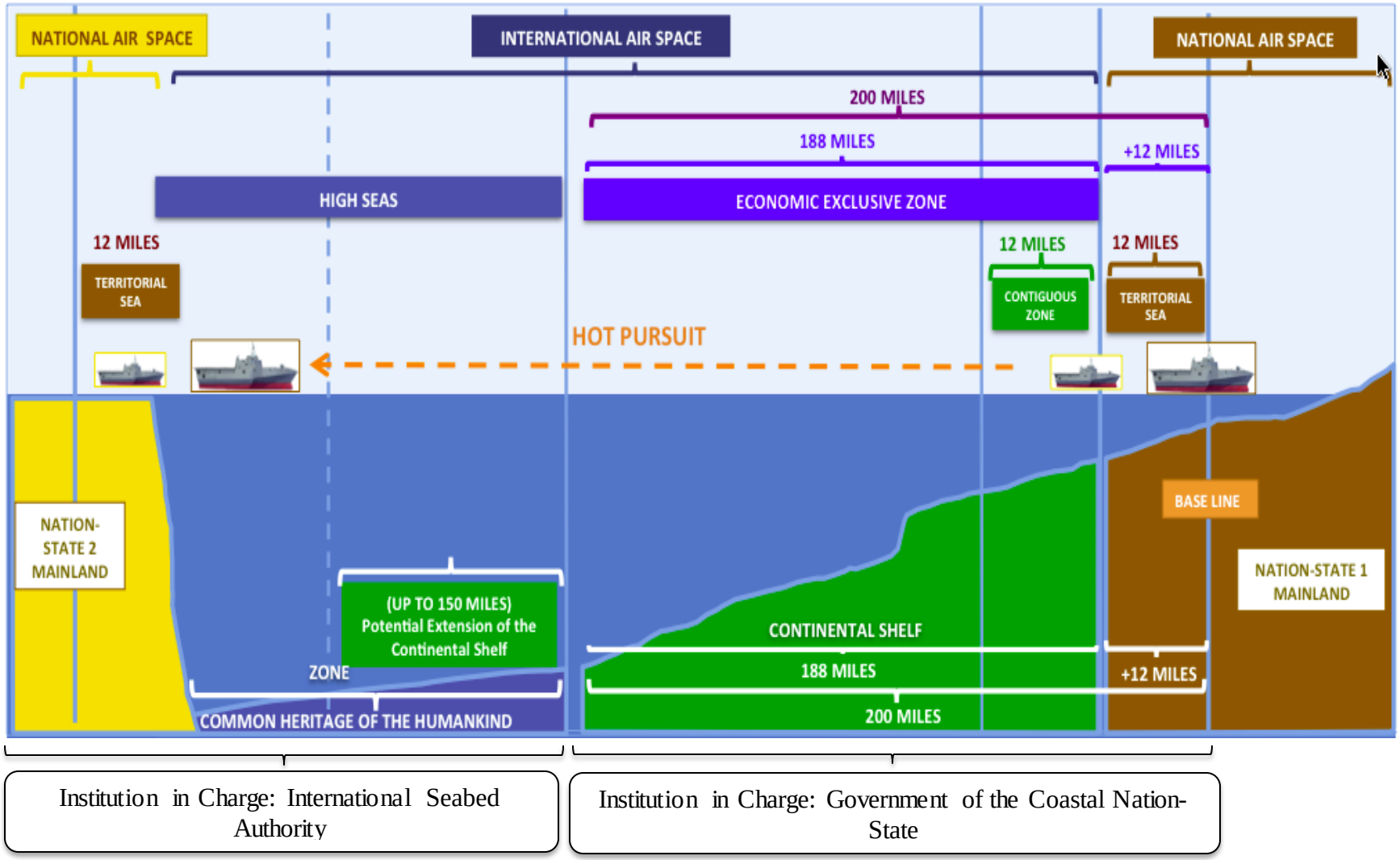

TABLE 1.- FICTIONAL SPACES CREATED BY THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA (UNCLOS) FROM 1982

SPACE	LENGTH/DISTANCE	SOVEREIGN RIGHTS
Territorial Sea	Base Line – Mile 12	Exclusive enforcement jurisdiction (like in the territory of the nation-state)
Contiguous Zone	Base Line – Mile 24 (juxtaposition with the territorial sea)	Jurisdiction for customs, immigration and sanitary
Economic Exclusive Zone	Base Line – Mile 200	Jurisdiction reserved to pollution, marine natural resources, fishing purposes and issues that affect national security
Continental Shelf	Base Line – Mile 200	Jurisdiction reserved to drilling and the protection of natural species (alive and non-alive) over and below the ocean surface
High Seas	Mile 200 - another nation-state's area of maritime domain	"International Waters" Freedom of navigation, over flight, to lay submarine cables and pipelines, to construct artificial islands, of fishing, of scientific research No rights reserved to any nation-state
The Zone	Mile 200 - another nation-state's area of maritime domain	"International Seabed" Declared "Common heritage of the humankind" No rights reserved to any nation-state Activities regulated according the agreement relating to the Implementation of the Part XI and the approval of the Seabed authority

5. MICROSOFT V. UNITED STATES OF AMERICA (U.S.): A HISTORY ABOUT THE CLASH OF JURISDICTIONS

This section will cover the main aspects of the legal case Microsoft v. U.S. describing the facts of the case and the arguments of the involved parties. As we will see, the controversy focuses in the extraterritorial application of the U.S. legislation in Irish territory. Although this became the main issue of the discussion between the involved parties, it is also a fact that in order to access the data, Microsoft did not have to send anyone to Ireland to collect it, since the data was under its control.

5.1. THE FACTS

In December 2013, a New York district Court judge issued a warrant requesting Microsoft to produce emails and private information associated to particular accounts hosted by Microsoft. The data was storage on a Hotmail server located in Dublin, Ireland and was related to a drug trafficking investigation (HLR, 2015; Scott, 2014).

In order to get the data, the U.S. government applied for a warrant according to section 2703(a)[11] of the Stored Communications Act (SCA), enacted as part of the 1986 Electronic Communications Privacy Act (ECPA) (Ely, 2015). According to the U.S. Department of Justice (DoJ), the U.S. government has the right to demand the emails of anyone in the world as long as the electronic email (e-mail) provider has headquarters within U.S. borders (Thielman, 2015).

Microsoft sued the U.S. government and refused to deliver the names and accounts of the server stored in Ireland arguing that a U.S. Court has no jurisdiction over information stored out of U.S. territory. Microsoft also argued that the U.S. government should pursue traditional bilateral law enforcement and diplomatic channels in order to work with the Irish government to get the data they required. Such channels referred to the "Mutual Legal Assistant Treaties" (MLATs), general agreements signed between two or more nation-states with the purpose of gathering and exchanging information to enforce public and criminal laws (DoS, 2012). Similarly, the Irish government supported the Microsoft opinion and claimed that U.S. Courts do not have sovereignty to issue search warrants to be executed abroad. The U.S. District Court for the Southern District of New York denied Microsoft's motion and the company appealed (Goldman, 2016).

Microsoft refused to turn over the e-mails and tried to quash the U.S. Warrant. Microsoft claimed that the U.S. government's warrant authority cannot extend extraterritorially and, therefore, the warrant was invalid. The government, along with the magistrate judge and district court, disagreed; they concluded that the relevant reference point for purposes of warrant jurisdiction was the location of the provider (in this case Microsoft), not the location of the data. In practical terms, the data located in Ireland can be accessed and retrieved by Microsoft employees within U.S. territory (Daskal, 2015).

---

[11] STORED COMMUNICATIONS ACT
18 U.S.C.
Title 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS
§2703. Required disclosure of customer communications or records
(a) Contents of Wire or Electronic Communications in Electronic Storage.—
A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

On July 7th, 2016, the 2nd U.S. Circuit Court of Appeals in Manhattan resolved that the U.S. government is not entitled to force Microsoft to turn over customer e-mails stored on servers outside of U.S. territory. According the appealing Court, U.S. service providers that own servers outside the U.S. are beyond the reach of domestic U.S. laws, and therefore, search warrants issued under SCA are not applicable (Stempel, 2016).

5.2. Arguments of the Involved Parties

The context of the Microsoft case refers to the rise of an electronic medium that cannot be governed by any current territorially based sovereign. In this regard, this case puts on the table an "international" problem: current national statutes (from the U.S. in this case) were written before the internet were privatized and open to the public. In this way, the U.S. Court has to guess or interpret what Congress would have written into legislation if the Internet was available at the time. In this scenario, law enforcement agencies find themselves trying to access data stored abroad, and sometimes facing multiple jurisdictions.

It is a fact that must be remembered that Microsoft, as well as other companies, invested billions to build data centers abroad, especially in Europe have invested billions in data centers abroad, particularly in Europe. If U.S. authorities and intelligence agencies can access that data, European firms may be reluctant to trust in U.S. companies On the other hand, depending upon the result, this case may encourage other governments to request Microsoft or other companies to hand data stored abroad. This situation could generate a forever conflict of jurisdictions (The Economist, 2015). Whatever the outcome of this case is, it is clear that the actions of the U.S. government will have important implications in terms of international law. Just to set an example, the former European Union Justice Commissioner warned that the final execution of the U.S. warrant may constitute a breach of international law (Reding, 2014). This was a clear call to respect the sovereignty of a member of the union.

.

In order to understand better the legal controversy, this section will describe the main arguments outlined by both parties, Microsoft and the U.S. government, during the case proceeding (AT&T, 2014; Bharara, 2014; EFE, 2014; Judge Francis, 2014; Microsoft, 2014; U.S. District Court, 2014; Verizon, 2014).

5.2.1. U.S. Government

For the U.S. government, the F.B.I. and the U.S. Courts are the authorities on charge of the criminal investigation, and upon its request, private companies (like Microsoft) must disclose customer information or records following the provisions of the Stored Communications Act (SCA). The exercise of authority is not an issue of international law, but one of the domestic laws that establish the duty of a citizen in relation to its government request. While the legislation of the Congress (unless the contrary intent appears) seems to be applicable only within U.S. territory, the question of its application requires construction and debate, not legislative change. According to the U.S. government, the nationality, as a

principle, supports the legal requirement that an entity subject to jurisdiction within U.S. territory (like Microsoft) may be required to get evidence stored abroad.

According of the provisions of the SCA, the government can request information through a subpoena, court order, or warrant. On this matter, the SCA was enacted in recognition that the fourth amendment protections that apply in the physical world might not apply to information communicated through the Internet. This is the reason why SCA authorizes the Court with jurisdiction over the investigation of a criminal act to issue a warrant directly, despite of the intervention of its counterpart in the district where the Internet service provider is located.

The warrant required in section 2703 of SCA demands the government to show probable cause, but it does not change the duty an entity has to produce information regardless of where the data is located. In this case, the U.S. Congress anticipated that an ISP located within U.S. territory would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control. Therefore, the warrant triggers the statutory obligation of a U.S. company to disclose records within its possession and control to law enforcement within U.S. territory. The purposes of the warrant are: (a) to require Microsoft to disclose the content of any electronic communication under Section 2703, and (b) to authorize a review of that data by law enforcement agents in the within U.S. territory after the data has been disclosed.

In terms of jurisdiction, Microsoft argues that it is not required to produce the records demanded by the warrant because those records were stored abroad. According to the U.S. government, that argument finds no support under the rules of SCA because any "court of competent jurisdiction" is authorized to issue a warrant. Those courts include those that have jurisdiction over (a) the offense under investigation, (b) the physical location of the service provider, or (c) the storage site of the relevant records.

5.2.2. MICROSOFT

In 1986, foreseeing the effect of modern technologies, such as e-mail, the U.S. Congress enacted ECPA, a statute intended to protect individuals' expectations of privacy in electronic communications. In order to protect these privacy interests, ECPA requires federal, state and local officers to use forms of process within their own powers and limitations. In terms of privacy, the Sixth Circuit's leading decision, ruled that the Fourth Amendment requires the Government to obtain a warrant in order to access the contents of e-mail communications. ECPA never meant to allow the government to obtain e-mails without warrant at all. This practice would be unconstitutional.

However, the extraterritorial application of warrants issued under ECPA represents a violation of international law and treaties, and reduces privacy expectations at a global level. No provision in the statute ever suggests that this was the intention of the U.S. Congress. If the Congress intended to give the warrant provision from ECPA extraterritorial effects, then the Congress should have been clear indications about it. The

legislative history of ECPA confirms that warrants executed according section 2703 (a) are limited to the U.S. territory.

About the competent jurisdiction, Microsoft also acknowledges that a court of competent jurisdiction is the only one who can issue a warrant, but for the company, this principle is vital. According to section 18, 2703(a), a state or federal entity may compel a provider of electronic communications services to disclose the content of a wire or electronic communication, but only when there is a warrant issued by a Court of competent jurisdiction. According to a related SCA provision contained in section 2703(b)[12] compels the disclosure of content information that is maintained by a provider of remote computing service as long as the government obtains a warrant issued by an appropriate state or federal court. To this end, and according to the Irish law, in order to obtain the content of electronic mails from an electronic service provider, it is required an authorization from an Irish District Court Judge.

In terms of jurisdiction, there is possibility of a constant conflict of jurisdictions. The use of "cloud" computing services makes more possible for U.S. companies to store data abroad. On this matter, each nation-state may have its own data protection law to protect data and may impose more strict protection standards than the U.S. law. When it about interpretation of the extension of the application of the U.S. legislation, Courts of justice are not free to re-write national statutes in order to achieve what they believe the Congress intended to say.

---

[12] STORED COMMUNICATIONS ACT
18 U.S.C.
Title 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS
§2703. Required disclosure of customer communications or records
(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—
(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii) obtains a court order for such disclosure under subsection (d) of this section;
except that delayed notice may be given pursuant to section 2705 of this title.
(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Microsoft does not refuse to provide the information requested by the U.S. Court, however the company argues that the U.S. authorities should request it through the regular MLAT procedures. MLATs convert a foreign law request for information into a request that conforms to the domestic law requirements. In this particular case, the U.S. government ratified a MLAT applicable to Ireland, the nation-state where the requested information is stored.

Finally Microsoft mentions an economic argument because the company has encountered concerns in consumers abroad about the U.S. Government extraterritorial pretensions to access their information. Potential customers have decided to hire the services of a provider based out of U.S. territory and therefore, out of U.S. jurisdiction.

6. Application of the Hot Pursuit Principle

From the arguments previously exposed the main legal issues can be summarized as: What legislation is applicable? What jurisdiction is the competent one? What nation-state's sovereignty prevails when there is a controversy about the cyberspace? We must remember that, on this matter, there is no international treaty or international agreement that solves the problem of the "right jurisdiction" when a data-access-issue occurs. So, how the rules of UNCLOS work in this case, more concretely, how the rules of the hot pursuit principle work in this case?

6.1. Are Bits Subject to the Sovereignty of a Nation-State?

A bit (b, short for "binary digit") is the smallest unit of storage used to quantify computer data. Bits are storage in a computer, so are bits subject to the sovereignty of a nation-state territorial sovereignty?

As mentioned before, the classic rules of international law established that nation-states' territorial sovereignty implies that, whether subject to applicable customary or conventional rules of international law, governments acting on behalf of their nation-states are entitled to exercise jurisdiction, by subjecting objects and persons within its territory. However, this principle has a two-side-application: territorial sovereignty protects a nation-state against any form of interference by other nation-states, but the principle also imposes obligations. Nation-states are obligated to protect the rights of other nation-states within their own territories too. This includes the right to integrity and inviolability, alongside with the rights each nation-state may claim for itself and its nationals in foreign territory[13].

[13] Corfu Channel Case, ICJ Rep., p. 43 (1949). As cited by von Heinegg (2012). In his Separate Opinion Judge Alvarez stated: "By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them" (Khan, 2007; von Heinegg, 2012).

Regarding the hot pursuit principle, the first condition for its application is the suspicion of criminal activity committed within territory under sovereignty of a nation-state, which seems to be the premise in the Microsoft case. Although the alleged criminal is located in U.S. territory, the required data to solve the investigation is not. In order to access the data, nobody has to travel (physically) to Ireland with that purpose, because the data is under control of Microsoft. However, also according to the theory of the hot pursuit principle, no matter what type of criminal activity is under investigation, once the sovereignty of a different nation-state (other than the one where the criminal act was committed) is involved, the pursuit must stop. The absolute end to any type of extraterritorial activity is the territory of another nation-state. Independently of the case, the pursuit must end as soon as the chased ship enters into the territorial sea of its own nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory).

In application of both principles, the classic rule of international law (that requires to one nation-state to protect other nation-state interests within its territory) and the hot pursuit, the U.S. government (or any other government) can request data storage beyond its own territorial borders, but cannot access directly. In order to get it, the government that requests the data must follow the traditional mechanisms of communication from government to government (traditional MLATs). The recognition of the sovereignty among nation-states (in theory at least) should be honored by the other nation-state involved. Following the rules of UNCLOS and the hot pursuit therefore, the U.S. government cannot access the data stored in foreign territories under the application of its own national statute. This is a constant reminder in Microsoft argumentation and, at the end, it would be backed up by the Second Circuit Court of Appeals. According to the Court, SCA does not authorize U.S. courts to issue and enforce warrants against U.S.-based service providers in order to get customer e-mail content that is stored exclusively on foreign servers (Stempel, 2016).

Ironically this conclusion is aligned with those who defend the "territorial sovereignty over the cyberspace" in benefit of their own governments. For these academics and non-academics, there is an absolute principle of territorial sovereignty when the cyberspace is involved and therefore, its infrastructure and activities are under the jurisdiction of the government where such infrastructure is located. For these defenders of the territorial sovereignty, nation-states are forbidden to interfere with the cyberinfrastructure located within another nation-state's territory (RT, 2012; von Heinegg, 2012; White House, 2011). Following this perspective it is interesting to ask the question changing the role of the participants in the Microsoft case: if the nation-state interested in accessing data abroad were Ireland, the U.S. government would accept it? Or, would the U.S. government require to Ireland to go to the long and bureaucratic MLAT process?

6.2.A "Virtual Fragmentation" with "Practical Consequences"

UNCLOS policy of creating fictional spaces with specific sovereign rights in favor of coastal nation-states in each space is no other thing than "fragmenting" the ocean until all of it gets "full" of "juridical meaning". The juridical meaning is the allocation of sovereign rights in favor of nation-states (Ferrero Rebagliati, 1962). Even international spaces ("High

Seas" and "The Zone"), where theoretically no nation-state has sovereign rights, have regulations that all nation-states are supposed to follow. Although according the rules of UNCLOS and the hot pursuit principle there are no absolute and exclusive rights in favor of nation-states, they are the main actors and constantly try to use their own sovereignty rights over others. Conflicts such as the South Sea in China, the Arctic and constant claims of sea boundary delimitation are a clear example of this government practice (BBC, 2016; Staalesen, 2015; The Economist, 2014). The hot pursuit was built on this policy of recognition of the absolute nation-states' sovereignty.

As defined, the cyberspace is aterritorial and invisible. However the Internet infrastructure, one of the most vital elements of the cyberspace, is not. When referring to specific policies applied by nation-states over the Internet infrastructure within their own territories, academics created the term "Internet fragmentation"[14]. It is possible to talk about Internet fragmentation when the conditions of the Internet infrastructure and government policies constrain or prevent certain uses of the Internet and do not allow to interoperate and exchange the Internet data packets consistently at all end points (Drake, Cerf, & Kleinwachter, 2016). Governments all over the world, acting on behalf of their sovereign nation-states, are constantly exercising jurisdiction and applying specific policies over the Internet infrastructure. These policies vary from censorship, filtering, data protection until more drastic policies, such as the most current Internet shut downs. These policies not only affect the Internet traffic, they are also significantly costly for the nation-states themselves (West, 2016).

Following the tradition of governments' practices, the application of the hot pursuit into the cyberspace carries the possibility of "re-align" or fragment the Internet infrastructure along the territorial boundaries of national jurisdictions. The ICANN transition can, at some extent, increase the resilience of the Internet; however, nation-states constantly try to construct borders around the Internet infrastructure in order to reaffirm the Westphalian conception of sovereignty. When the actions of one government have consequences on other nation-state's territory, a "collision" of jurisdictions is inevitable: what could happen if nation-states enforce national jurisdiction over global internet services that happen to be incorporated on their national territories? (Fehlinger, 2014). Consequences cannot be foreseen.

The hot pursuit and UNCLOS as well, are belong to a policy model over the sea of "filling" it with legal content in favor of nation-states. The application of this policy into the cyberspace has very similar implications: despite of the existence of different stakeholders that do not exist in the sea, the fragmentation policy of UNCLOS and the hot pursuit carries the risk of the Westphalian model, where the territorial sovereignty of nation-states is the rule and only source of law and practice.

7. CONCLUSION

[14] Some scholars prefer the use of the term "alignment" instead of fragmentation. This new concept is built on the idea that the Internet infrastructure is not fragmented into pieces, but that it is "aligned" with nation-states' territorial borders (Mueller M., panel "Is the Internet fragmenting, Microsoft, 2016).

Despite of any previous attempt, nation-states have not been able to achieve a common and global governance regime over the cyberspace. Claims to apply policies over other spaces beyond national jurisdictions, such as the ocean, can provide an overview about the practices and legal alternatives governments considered when trying to regulate spaces beyond their own territories. Situations like this create "conflicts" of jurisdiction, as portrayed in the Microsoft case, when more than one nation-state demand sovereignty right over a specific "thing" ("data" in this case). The hot pursuit principle is an example of the UNCLOS policies, as it set the rules when the legal claim of a nation-state ends because it encounters another nation-state sovereignty. In this regard, UNCLOS introduces the possibility of a virtual fragmentation of the cyberspace and, as a practical consequence, the fragmentation of the Internet infrastructure.

Fragmentation is a concept related to governments' policies and actions, in exercise of their own sovereignty within their own territorial borders. Opinions about this policy however, can be diverse depending on the vision nation-states have over the Internet infrastructure. In any case, fragmentation is the point of collision where sovereignty and cyberspace encounter each other.

UNCLOS policies of creating fictional spaces in the ocean and "filling" them with legal content is an example of the attempt of nation-states of applying the Westphalian model to every single space beyond their territorial borders. The hot pursuit was built on the bases of the spaces created by this fragmentation. Therefore, any possibility of applying the institutions and policies of UNCLOS also bring the possibility of including the concept of territorial sovereignty in the cyberspace policy debate. Finally, the possibility of the Internet fragmentation implies higher level of government control, in detriment of the multi-stakeholder model, the model that has allowed Internet users to enjoy a free and open Internet as we have become to know.

8. REFERENCES

Allen, C. H. (1989). Doctrine of Hot Pursuit: A Functional Interpretation Adaptable to Emerging Maritime Law Enforcement Technologies and Practices. *Ocean Development and International Law, 20*, 309–341. Retrieved from http://www.law.washington.edu/Directory/docs/Allen/Publications/Article_1989_DoctrineOfHotPursuitpp309-341.PDF

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

AT&T. AT&T District Court Amicus Brief in Support of Microsoft (2014). Retrieved from https://www.eff.org/document/att-amicus-brief-support-microsoft

Barcomb, K. E. (2013). From Sea Power to Cyber Power. *JFQ*, (69), 78–83. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_78-83_Barcomb.pdf

BBC. (2016). Why is the South China Sea contentious? Retrieved October 1, 2016, from http://www.bbc.com/news/world-asia-pacific-13748349

Benadava, S. (1982). *Derecho internacional público [Public International Law]*. Santiago: Editorial Jurídica de Chile.

Bharara, P. Government's Brief in Support of Magistrate's Decision (2014). Retrieved from https://www.eff.org/document/governments-brief-support-magistrates-decision

Bobbitt, P. (2002). *The Shield of Achilles: War, Peace, and the Course of History*. Knopf.

Brownlie, I. (2003). *Principles of public international law* (6th ed.). Oxford ;New York: Oxford University Press.

Brownlie, I. (2012). *Brownlie's Principles of Public International Law*. (S. P. Crawford, Ed.) (8th ed.). Oxford; New York.

Center for Oceans Law and Policy UVA. (1985). *United Nations Convention on the Law of the Sea 1982. A Commentary, Volume I*. (M. Nordquist, Ed.). Brill | Nijhoff. Retrieved from http://www.brill.com/united-nations-convention-law-sea-1982-volume-i

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 http://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/

Crawford, J. (2013). *Brownlie's Principles of Public International Law*. Oxford University Press.

Daskal, J. (2015). Case To Watch: Microsoft v. US on the Extraterritorial Reach of the Electronic Communications Privacy Act | Just Security. Retrieved April 1, 2016, from https://www.justsecurity.org/20780/case-watch-microsoft-v-united-states-extraterritorial-reach-electronic-communications-privacy-act/

DOALOS. (2016). Chronological lists of ratifications of, accessions and successions to the Convention and the related Agreements. Retrieved October 6, 2016, from http://www.un.org/depts/los/reference_files/chronological_lists_of_ratifications.htm

DoD. (2016). Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. Dictionary, Department of Defense. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

DoS. (2012). Treaties and Agreements. Retrieved September 30, 2016, from http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

Drake, W., Cerf, V., & Kleinwachter, W. (2016). Internet Fragmentation: An Overview. Retrieved April 15, 2016, from http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

EFE. EFF District Court Amicus Brief in Support of Microsoft (2014). Retrieved from https://www.eff.org/document/eff-amicus-brief-support-microsoft

Ely, A. (2015). Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview. Retrieved April 30, 2016, from https://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview

Fehlinger, P. (2014). Cyberspace fragmentation: an internet governance debate beyond infrastructure. Retrieved May 16, 2016, from http://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266

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

Goldman, D. (2016). Microsoft is fighting the DOJ too. Retrieved March 31, 2016, from http://money.cnn.com/2016/02/23/technology/microsoft-ireland-case/

HLR. (2015). In re warrant to search a certain email account controlled & maintained by Microsoft Corp. *Harvard Law Review*, *128*(3), 1019–1026.

ICJ. (1949). Reparation for Injuries Suffered in the Service of the United Nations. Advisory Opinion of 11 April 1949. Advisory Opinion, International Court of Justice. Retrieved from http://www.icj-cij.org/docket/files/4/1837.pdf

IDRC. (2001). *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa: International Development Research Centre.

International Tribunal for the Law of the Sea. (2016). The Tribunal. Retrieved October 7, 2016, from https://www.itlos.org/the-tribunal/

Johnson, L. (1999). Comment: Reno V. American Civil Liberties Union: The First Amendment Balance of a Child's Morality and an Adult's Naughty Net Play. *Rutgers Computer and Technology Law Journal*, (25). Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=25+Rutgers+Computer+%26+Tech.+L.J.+157&srctype=smi&srcid=3B15&key=c3f1368d5141848e8992bfc74405c7ba

Judge Francis. Magistrate's Opinion Denying Microsoft's Motion to Quash (2014). Retrieved from https://www.eff.org/document/magistrates-opinion-denying-microsofts-motion-quash

Kalpokienė, J., & Kalpokas, I. (2012). Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control. *Baltic Journal of Law & Politics*, *5*(2), 132–163. Retrieved from http://www.degruyter.com/view/j/bjlp.2012.5.issue-2/v10076-012-0014-y/v10076-012-0014-y.xml?format=INT

Karim, S. (2011). Conflicts over Protection of Marine Living Resources: The "Volga Case" Revisited. *Goettingen Journal of International Law*, *1*, 101–127. Retrieved from http://www.academia.edu/710622/Conflicts_over_Protection_of_Marine_Living_Resources_The_Volga_Case_Revisited

Khan, D.-E. (2007). Max Huber as Arbitrator: The Palmas (Miangas) Case and Other Arbitrations. *European Journal of International Law*, *18*(1), 145–170. http://doi.org/10.1093/ejil/chm011

Kulesza, J. (2012). *International Internet law*. Milton Park Abingdon Oxon ;;New York: Routledge. Retrieved from http://www.worldcat.org/title/international-internet-law/oclc/724640168&referer=brief_results

Mazower, M. (2014). After the crisis, nation-state strikes back. Retrieved December 2, 2014, from http://gulfnews.com/opinions/columnists/after-the-crisis-nation-state-strikes-back-1.1419157

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). Madrid. Retrieved from http://www.casadellibro.com/libro-los-espacios-maritimos-en-el-nuevo-derecho-del-mar/9788472486775/657385

Microsoft. Microsoft's Objection to the Magistrate's Opinion (2014). Retrieved from https://www.eff.org/document/microsofts-objection-magistrates-opinion

Microsoft. (2016). Event: Is the Internet Fragmenting? Part 2. Retrieved September 22, 2016, from https://internetpolicyforum.com/event-is-the-internet-fragmenting-part-2-the-technical-lens/

Moyer, E. (2016). US hands internet control to ICANN. Retrieved October 4, 2016, from https://www.cnet.com/news/us-internet-control-ted-cruz-free-speech-russia-china-internet-corporation-assigned-names-numbers/

Mueller, M. (2002). Ruling the root Internet governance and the taming of cyberspace. Cambridge, Mass. : MIT Press,.

Mueller, M. (2010). *Networks and states : the global politics of Internet governance*. BOOK, Cambridge, Mass.: MIT Press.

Poúlantzas, N. M. (2002). *The Right of Hot Pursuit in International Law*. Martinus Nijhoff Publishers. Retrieved from https://books.google.com/books?id=npdgzJEROswC&pgis=1

Reding, V. (2014). Viviane REDING letter European Commission. Letter. Retrieved from http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-.pdf

Reuland, R. C. (1993). The customary right of hot pursuit onto the high seas : annotations to article 111 of the Law of the Sea Convention. *Virginia Journal of International Law*. -.

Rosenne, S. (2004). *The perplexities of modern international law*. M. Nijhoff. Retrieved from http://books.google.com/books?id=aJ06AQAAIAAJ&pgis=1

Rosenne, S. (2007). Essays on international law and practice. Leiden ;;Boston : Martinus Nijhoff Publishers,. Retrieved from http://www.worldcat.org/title/essays-on-international-law-and-practice/oclc/307419308&referer=brief_results

RT. (2012). White House gives Homeland Security control of all communication systems. Retrieved January 31, 2016, from https://www.rt.com/usa/white-house-systems-order-142/

RT. (2014). MP urges "nationalization" of Google over security fears. Retrieved January 25, 2016, from https://www.rt.com/politics/186364-russian-google-nationalization-fyodorov/

Schaller, C. (2014). Internet Governance and the ITU: Maintaining the Multistakeholder Approach. Retrieved October 4, 2016, from http://www.cfr.org/internet-policy/internet-governance-itu-maintaining-multistakeholder-approach/p33654

Scott, M. (2014, December 24). Ireland Lends Support to Microsoft in Email Privacy Case. *The New York Times*. New York, New York, USA. Retrieved from http://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/?_r=0

Sechrist, M. (2010). Cyberspace in Deep Water: Protecting Undersea Communications Cables By Creating an International Public-Private Partnership. *Harvard - Belfer Center for Science and International Affairs*. Retrieved from http://belfercenter.ksg.harvard.edu/publication/20710/cyberspace_in_deep_water.html?breadcrumb=%2Fexperts%2F2223%2Fmichael_sechrist

Sheng, A. (2014). Andrew Sheng argues that cyberspace, land, air, sea, and space now define the basis of global conflict. Retrieved March 8, 2016, from http://www.project-syndicate.org/commentary/andrew-sheng-argues-that-cyberspace--land--air--sea--and-space-now-define-the-basis-of-global-conflict?barrier=true

Staalesen, A. (2015). "Conflict over Arctic shelf unlikely." Retrieved October 1, 2016, from http://barentsobserver.com/en/arctic/2015/08/conflict-over-arctic-shelf-unlikely-07-08

Steinberg, P. E. (2001). *The Social Construction of the Ocean*. Cambridge University Press. Retrieved from https://books.google.com/books/about/The_Social_Construction_of_the_Ocean.html?id=_sh9rBbPF6UC&pgis=1

Stempel, J. (2016). Microsoft wins landmark appeal over seizure of foreign emails | Reuters. Retrieved July 15, 2016, from http://www.reuters.com/article/us-microsoft-usa-warrant-idUSKCN0ZU1RJ

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

Tasikas, V. (2004). Unmanned Aerial Vehicles and the Doctrine of Hot Pursuit: A New Era of Coast Guard Maritime Law Enforcement Operations. *Tulane University Maritime Law JournalMaritime Law Journal*, *29*(1), 59–80.

The Economist. (2014). The Economist explains: Chile and Peru's Pacific dispute. Retrieved October 1, 2016, from http://www.economist.com/blogs/economist-explains/2014/01/economist-explains-21

The Economist. (2015). Should governments be able to look at your data when it is abroad? Retrieved May 1, 2016, from http://www.economist.com/news/business-and-finance/21663902-test-case-set-determine-whether-fbi-can-access-microsofts-foreign-data-should

Thielman, S. (2015). Microsoft case: DoJ says it can demand every email from any US-based provider. Retrieved March 31, 2016, from http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant

U.S. District Court. Microsoft's District Court Reply Brief (2014). Retrieved from https://www.eff.org/document/microsofts-district-court-reply-brief

United Nations. Statute of the International Tribunal for the Law of the Sea (2016). United Nations. Retrieved from https://www.itlos.org/fileadmin/itlos/documents/basic_texts/statute_en.pdf

Verizon. Verizon District Court Amicus Brief in Support of Microsoft (2014). Retrieved from https://www.eff.org/document/verizon-amicus-brief-support-microsoft

von Heinegg, W. H. (2012). *Legal Implications of Territorial Sovereignty in Cyberspace* (International Conference on Cyber Conflict No. 4). Retrieved from https://ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

West, D. M. (2016). Internet shutdowns cost countries $2.4 billion last year. Retrieved October 7, 2016, from https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/

White House. (2011). *International Strategy for Cyberspace*. Washington D.C. Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Williams, G. L. (1939). *The Juridical Basis of Hot Pursuit*. *British Year Book of International Law'*. Retrieved from http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/byrint20&div=&id=87&page=

WOR. (2010). A constitution for the seas. Retrieved April 17, 2015, from http://worldoceanreview.com/en/wor-1/law-of-the-sea/a-constitution-for-the-seas/