JURISDICTIONAL CHALLENGES IN FIGHTING CYBERCRIMES: ANY PANACEA FROM INTERNATIONAL LAW?[1]

Abstract

Jurisdiction is pivotal and fundamental to administration of legal justice in general and of criminal justice in particular. It is trite in law that no matter how well conducted a proceeding was, lack of jurisdiction on the part of the trial court would bring to nullity the entire adjudicatory process. Jurisdiction itself is an issue of law. Yet, hardly are there uniform laws across jurisdictions. Even if the substantive laws are similar, the adjectival laws and enforcement procedures may differ. It is observed that situations are all the more complex when related to crimes in cyberspace which knows no boundaries. However, it may seem that the global nature of cyberspace and the Internet are coterminous with international geographical space, and thus may be subjected to the provisions of international law. This paper, after due consideration, discovers that this is not necessarily so. Rather than constituting a definitive panacea, some international law provisions and practice can only offer some help towards determining jurisdiction for combating cybercrimes. This study seeks only to identify the problem which the issue of jurisdiction does pose to the fight against cybercrimes, and advocates the need for a more global and universalist approach.

Key words: *Jurisdiction, Cybercrimes, International Law, Jurisprudence, Internet, Computer*

1. Preamble

The practice of conducting operations via cyberspace has become irresistible and unstoppable. Because activities on the Internet can have trans-boundary effect in every state in a nation and also every state on earth, there arises the issue of where exactly a person who has a cause of action based upon such activities may sue. Before a court or an agency can enforce a cybercrime case, it must be clothed with the necessary jurisdiction. Thus, a central and difficult legal issue in fighting cyber criminality is the problem of jurisdiction. This is particularly true as it is hard to territorially locate conduct in cyberspace because of the dispersed and amoeboid nature of the network that makes up the Internet.

No doubt, the electronic environment challenges the traditional methods for finding presence to assert jurisdiction. Questions of jurisdiction in cyberspace are essentially practical. First, does a person who posts information on the World Wide Web have to comply with the laws of every state or nation from which the website can be accessed? Second, do the courts of every state or nation from which information on the Web can be accessed have personal jurisdiction over the creator of the information and the operator of the site? Sorting out the answers to these two basic questions has in many foreign jurisdictions generated numerous court decisions and commentary over the years.

Therefore, jurisdiction can be based on a number of different issues such as determining the place where the cybercrime was committed, the country of origin of the cybercriminal, the property and owner of the property affected by the cybercrime. With the use of the internet, a cyber-criminal can perpetrate a cybercrime in country Z when in country Y while using facilities stationed in countries O, P or more as zombies in committing the act. A situation like this creates a problem of determining which country should assume jurisdiction. Under this scenario, it is possible that country Z does not have any law prohibiting cybercrime. Country Y may have cybercrime law but unwilling to enforce same against its subject who committed the cybercrime, simply because the effect is not felt within country Y. And even if Country Z has a cybercrime law, the next hurdle wound be how to move the offender from country Y to be tried in country Z. Again, the use of facilities stationed in countries O, P or more as zombies in committing the act means that the cybercrime would be traceable to countries O or P thereby making the tracing of the real suspect difficult.

[1]By **Ikenga K. E. ORAEGBUNAM, PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), MEd, BTh, BL,** Senior Lecturer and Ag Head, Department of International Law & Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria. E-mail: ik.oraegbunam@unizik.edu.ng. Phone Number: +2348034711211.

Computer offences and cybercrimes inevitably often have a transnational aspect to them, which can give rise to complex jurisdictional issues involving persons, things and acts being present or carried out in a number of different countries. Even where the perpetrator and the victim are located in the same jurisdiction, relevant evidence may reside on a server located in another jurisdiction. Again, an act may be initiated in one jurisdiction and completed or terminated, that is, the effect or harm felt, in another jurisdiction. In the course of a cybercrime investigation, law enforcement agencies will often need to obtain access to data held on systems located in foreign jurisdictions, or where the physical location of the data is unknown. As with most aspects of Internet-based activities, traditional legal concepts and principles are sometimes challenged by the nature of cyberspace environment. The enquiry will examine the legal principles of jurisdiction in international law with a view to ascertaining their relevance and propriety or otherwise in the prosecution against cyber criminality.

2. Jurisdiction under International Law

International law is founded on the concept of the state.[2] The state, in turn, is based on the foundation of sovereignty, which expresses internally, the supremacy of the governmental institutions and, externally, the supremacy of the state as a legal person.[3] Sovereignty is founded upon the fact of territory for without a territory, there can be no legal personality that can be called a state.[4] Legal concepts such as sovereignty and jurisdiction can only be comprehended in relation to territory. Contemporary international law assumes that the world is made up of states, each sovereign within its defined territory, and each with full jurisdiction and control over matters occurring within its borders. The Charter of the United Nations is also premised upon these fundamental principles, and recognizes that a state has to be supreme within its own borders.[5]

Jurisdiction concerns the power of the state to affect people, property and circumstances within its territory and reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs.[6] Jurisdiction is a vital and indeed central feature of state sovereignty; for, it is an exercise of authority which may alter or create or terminate legal relationships and obligations.[7]Jurisdiction equally refers to the power of each state under international law to prescribe and enforce its municipal laws with regard to persons and property within its territorial borders. This power can be exercised in three forms: legislative or prescriptive jurisdiction which relates to the competence to prescribe the ambit of municipal laws; judicial jurisdiction which signifies the competence of courts to apply national laws; and enforcement jurisdiction which refers to the ability of States to enforce the fruits of their legislative or judicial labour (for example, gathering of evidence and imposition of sanctions).[8] In other words, there are three types of jurisdiction generally recognized in international law, namely, jurisdiction to prescribe, jurisdiction to enforce; and jurisdiction to adjudicate[9]. The foregoing three types of jurisdiction are often interdependent and based on similar considerations.

It is essential to differentiate between the three forms of jurisdiction because while prescriptive and judicial may assume an extra-territorial character, enforcement jurisdiction generally cannot.[10]The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the

[2] M.N. Shaw, *International Law*, 5th ed., Cambridge, Cambridge University Press, Cambridge, 2003, p.409.
[3]*Ibid*.
[4] Article 1 of the *Montevideo Convention on Rights and Duties of States, 1933* lays down the most widely accepted formulation of the criteria of statehood in international law. It provides that the state as an international person should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with other states.
[5] The principle of respect for the territorial integrity of states is well founded as one of the linchpins of the international system, as is the norm prohibiting interference in the internal affairs of other states as provided in articles 2(4) and 2(7) of the United Nations Charter.
[6]Shaw, *op. cit.*, p.572.
[7]*Ibid.*
[8]Bantekas and Nash, *International Criminal*, *Law*, 2nd ed., Australia, Cavendish, 2003, p.143.
[9]Restatement (Third) of Foreign Relations Law of the United States, 1987, § 40.
[10]Bantekas and Nash, *Op.cit*., p.143.

status of persons, or the interests of persons in things[11]. Enforcement jurisdiction is restricted by territorial factors. For instance, if a man steals a vehicle in Nigeria and manages to escape to Cotonou in the Republic of Benin, the Nigerian courts have jurisdiction to try him, but they cannot enforce it by sending officers to Cotonou to arrest him. Nigeria has to apply to the authorities in the Republic of Benin for his arrest and extradition to Nigeria. To do otherwise, for instance, by abducting the criminal, would be a breach of the territorial sovereignty of the Republic of Benin.

International law limits a country's authority to exercise jurisdiction in cases that involve interests or activities of non-residents. First, there must exist 'jurisdiction to prescribe.' If jurisdiction to prescribe exists, 'jurisdiction to adjudicate' and, 'jurisdiction to enforce' will be examined. 'Jurisdiction to prescribe' means that the substantive laws of the forum country are applicable to the particular persons and circumstances. When a country has jurisdiction to prescribe, it can appropriately apply its legal norms to conduct. Simply stated, a country has jurisdiction to prescribe law with respect to: (1) conduct that, wholly or in substantial part, takes place within its territory; (2) the status of persons, or interests in things, present within its territory; (3) conduct outside its territory that has or is intended to have substantial effect within its territory; (4) the activities, interests, status, or relations of its nationals outside as well as within its territory; and (5) certain conduct outside its territory by persons who are not its nationals, that is, directed against the security of the country or against a limited class of other national interests. 'Jurisdiction to adjudicate' means that the tribunals of a given country may resolve a dispute in respect to a person or thing where the country has jurisdiction to prescribe the law that is sought to be enforced.

The exercise of jurisdiction by a country is subject also to the requirement of reasonability. States exercise jurisdiction to adjudicate on the basis of various links, including the defendant's presence, conduct, or, in some cases, ownership of property within the country, conduct outside the state having a 'substantial, direct and foreseeable effect' within the country or the defendant's nationality, domicile, or residence in the country. Exercise of judicial jurisdiction on the basis of such links is on the whole accepted as 'reasonable'; reliance on other bases, such as the nationality of the plaintiff or the presence of property unrelated to the claim, is generally considered 'exorbitant.' A country may employ judicial or non-judicial measures to induce or compel compliance or punish noncompliance with its laws or regulations, provided it has 'jurisdiction to prescribe.' Thus, a country may not exercise authority to enforce law that it had no jurisdiction to prescribe. A country may employ enforcement measures against a person located outside its territory if (a) the person is given notice of the claims or charges against him that is reasonable in the circumstances; (b) the person is given an opportunity to be heard, ordinarily in advance of enforcement; and (c) where enforcement is through the courts, if the country has jurisdiction to adjudicate. Cutting across the foregoing international law criteria is a general requirement of reasonableness. Thus, even when one of the foregoing bases of jurisdiction is present, a country may not exercise jurisdiction to prescribe law with respect to a person or activity having connection with another country if the exercise of jurisdiction is unreasonable. The net effect of the reasonableness standard is to require more close contact between a foreign defendant and the forum country than is required under constitutional due process.[12]

It is also necessary to differentiate between issues of jurisdiction as discussed under public international law and private international law. While public international law tries to set down rules dealing with the limits of a state's exercise of governmental functions, private international law attempts to regulate in a case involving a foreign element whether the particular country has jurisdiction to determine the question, and secondly, if it has, then the rules of which country will be applied in resolving the dispute.[13] The focus here will be on jurisdiction as it applies under public international law.

[11]*Ibid*., p.402.
[12]See J. A. Gladstone, *Determining Jurisdiction in Cyberspace: The "Zippo" Test or the "Effects" Test?* Available athttp://proceedings.informingscience.org/IS2003Proceedings/docs/029Glads.pdf. Last visited on 16-05-14
[13]Shaw, *Op. cit.*, p.573.

Jurisdiction may be civil or criminal. The focus will be on criminal jurisdiction, where a number of definite principles upon which to base jurisdiction have emerged, with varying degrees of support and of different historical legitimacy. These are the principles of territoriality, active nationality, passive nationality, protective, and the universality principle.

Under the territorial principle, all crimes committed within the territorial jurisdiction of a state may come before the municipal courts and this is so even where the offenders are foreigners. That a country should be able to prosecute for offences committed upon its soil is a logical manifestation of a world order of independent states and is entirely reasonable since the authorities of a state are responsible for the conduct of law and the maintenance of good order within that state.[14] Assumption of jurisdiction under this principle has the advantage of immediate accessibility to evidence and relevant witnesses and subsequent minimization of expenses and judicial time.[15] The territorial principle is further divided into two, i.e. the subjective territorial and objective territorial principles. Under the subjective territorial principle, if an activity takes place within the territory of the forum state, then the forum state has the jurisdiction to prescribe a rule for that activity. The vast majority of criminal legislation in the world is of this type. Under the subjective territorial principle, a state is entitled to try criminals for offences fully committed within its territory. Where an offence is commenced elsewhere but completed within the state such offence can be tried under the objective territorial principle. For instance, where a person fires a gun across a frontier killing somebody, both the state where the gun was fired and the state where the injury actually took place have jurisdiction to try the offender. The former is under the subjective territorial principle while the latter is under the objective territorial principle. Objective territoriality is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. The classic case is that of a rifleman in Niger shooting a Nigerian across the border in Katsina State. The shooting takes place in Niger; the murder, the effect, occurs in Nigeria. Nigeria would have the jurisdiction to prescribe under this principle. This is sometimes called 'effects jurisdiction' and has obvious implications for cyberspace which will be discussed anon.

In the *Lotus* case[16]the Permanent Court of International Justice examined the nature of territorial sovereignty in relation to criminal acts. The case concerned a French steamer, the *Lotus*, which was involved in a collision on the high seas with the *Boz-Kourt*, a Turkish collier. The Turkish vessel sank and eight sailors and passengers died as a result. When the French vessel arrived at a Turkish port, the Turkish authorities arrested the French officer at the watch (at the time of the incident) and charged him with manslaughter. France protested against this action, alleging that Turkey did not have the jurisdiction to try the offence. The Court, in its judgment, reasoned that because the basis of international law is the existence of sovereign states, restrictions upon the independence of states could not be presumed. It rejected the French claim that the flag state had exclusive jurisdiction over the ship on the high seas, and it stated that the damage to the Turkish vessel was equivalent to affecting Turkish territory so as to enable that country to exercise jurisdiction on the objective territorial principle. The approach of the Court in treating states as possessing very wide powers of jurisdiction which could only be restricted by proof of a rule of international law prohibiting the action has been criticized. It is widely accepted now that the emphasis lies the other way round.[17]

The active nationality principle of jurisdiction is based on the nationality of accused persons. Under this principle, states can prosecute their nationals who have committed crimes irrespective of where such crimes had been committed. This principle is based on the allegiance that is owed to one's country under municipal law.[18] Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. Under the law of the Netherlands, for

[14]Shaw, *Op. cit.*, p.579.
[15]Bantekas and Nash, *Op. cit.*, p.144.
[16] PCIJ, Series A, No.10, 1927, p.18.
[17] Shaw, *Op.cit.*, p.582. It is also noteworthy that the principle as regards collisions at sea has been overturned by article 11(1) of the High Seas Convention, 1958, which emphasized that only the flag state or the state of which the offender was a national has jurisdiction over sailors regarding incidents occurring on the high seas.
[18]Bantekas and Nash, *Op. cit.*, p.151.

example, a Dutch national 'is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed.'[19]Many other civil law countries have similar laws.

Passive nationality is a theory of jurisdiction based on the nationality of the victim. Passive and 'active' nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offence when both the offender *and* the victim are nationals of that state. Passive nationality is rarely used for two reasons. First, it is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. Second, the victim is not being prosecuted. A state needs to seize the actor in order to undertake a criminal prosecution. Under the passive nationality principle, a state may claim jurisdiction to try an individual for offences committed abroad which has affected or will affect nationals of the state.[20] Assumption of jurisdiction under this principle was initially criticized and opposed. In the *Cutting* case,[21] Mr. Cutting, a U.S. citizen was arrested in Mexico for a libel charge against a Mexican national. The action for which the libel was charged had been committed whilst its author was in the U.S., but he was arrested during a trip to Mexico upon the basis of the passive nationality principle. The US Government vigorously opposed Mexico's claim of jurisdiction and the case was finally discontinued. But with the upsurge of transnational terrorist activity, attitude towards this principle has changed; some states such as the United States, that were opposed to it now rely upon it. For instance, in *US v Yunis (No.2)*[22], the issue concerned the apprehension of a Lebanese citizen by US agents in international waters and his prosecution in the US for alleged involvement in the hijacking of a Jordanian airliner. The only connection between the hijacking and the US was the fact that several American nationals were on that flight. The court accepted that both the universality principle and the passive personality principle provided an appropriate basis for jurisdiction in the case. The court pointed out that although the US had historically opposed the passive personality principle, it had been accepted by the US and the international community in recent years in the sphere of terrorist and other internationally condemned crimes.

Yet another principle is the Protective principle which expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the 'victim' would be the government or sovereign itself. For example, in *United States v Rodriguez*[23], the defendants were charged with making false statements in immigration applications while they were outside the United States. This principle is disfavored for the obvious reason that it can easily offend the sovereignty of another nation. Under the protective principle, a state may exercise jurisdiction over aliens who committed an act abroad which is deemed prejudicial to the security of the particular state concerned.[24] Espionage and treason are classic examples of the application of the protective principle, since they have traditionally been viewed as acts endangering internal security. This doctrine appears to have been applied by the House of Lords in *Joyce v DPP*[25], Joyce was born in America, but in 1933 fraudulently acquired a British passport by declaring that he had been born in Ireland. In 1939 he left Britain and started working for the German radio and was broadcasting pro-Nazi propaganda during the Second World War. In 1940, he claimed to have acquired German nationality. The question was whether the British court had jurisdiction to try him after the war, on a charge of treason. The House of Lords held that jurisdiction did exist in the case since the fact that the treason occurred outside the territory of the U.K. was of no consequence because states were not obliged to ignore the crime of treason committed against them outside their territory. Relying on *Joyce*, the District Court of Jerusalem upheld, *inter alia*, the protective jurisdiction in the *Eichmann* case.[26] Eichmann was responsible for implementing Hitler's 'Final Solution' programme, the policy that led to

[19]Public Prosecutor/Y., HR May and September 1957, 24 Int'l L. Rep. 264, 265 (1957).
[20]Shaw, *op. cit.*, p.589.
[21]*Cutting* case (1887) U.S. For. Rel., p 751.
[22]*U.S. v Yunis (No.2)* (1988) 82 I.L.R. 344.
[23]*United States v Rodriguez*, 182 F. Supp. 479 (S.D. Cal. 1960).
[24] Shaw, *Op.cit.*, p.591.
[25]*Joyce v DPP* [1946] A.C. 347.
[26]*Eichmann* case (1961) 36 I.L.R. 5.

the extermination of over four million Jews. He was abducted by Israeli agents from Argentina to stand trial in Israel for war crimes and crimes against humanity. The judgment of the District Court, which was subsequently affirmed by the Israeli Supreme Court,[27]held that a country whose 'vital interests' and ultimately its existence are threatened, such as in the case of the extermination of the Jewish people, has a right to assume jurisdiction to try the offenders.

The final basis of jurisdiction is universal jurisdiction, sometimes referred to as 'universal interest' jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish pirates. This form of jurisdiction has been expanded to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy)[28]. Although universal jurisdiction may seem naturally extendable in the future to Internet piracy, such as computer hacking and viruses, such an extension is unlikely given the traditional tortoise-like development of universal jurisdiction. Just as important as it is, universal jurisdiction traditionally covers only very serious crimes[29]. As a result, all nations have due process type problems with convictions under this principle. Under the universality principle, each and every state has jurisdiction to try particular offences. The basis for this is that the crimes involved are regarded as offences to the international community as a whole.[30] Crimes against humanity must be distinguished from international crimes; the latter refers to crimes that are declared to be such by a treaty and state-parties are obliged to enact domestic laws criminalizing such acts if previously they were not deemed criminal.[31] This type of jurisdiction has been described as quasi-universal jurisdiction.[32] Examples of such treaties that provide for this type of quasi-universal jurisdiction include the UN Torture Convention 1984, and the Council of Europe Convention on Cybercrime.[33]

Apart from the principles of jurisdiction under international law as discussed above, it is also necessary to examine the concept of extradition which is a form of international cooperation against criminality. Extradition comes into the fore particularly in situations where the criminal is resident in one state and from there commits a crime in another without leaving his own state. This has become easier with advances in technology especially with the development of the Internet. Extradition can be defined as 'the surrender by one nation to another of an individual accused or convicted of an offence outside of its own territory, and within the territorial jurisdiction of the other, which, being competent to try and to punish him, demands the surrender.'[34] The practice of extradition enables one state to hand over to another state, suspected or convicted criminals who have fled abroad.[35] It is usually based upon treaties and it does not exist as an obligation on states. The law of extradition is based on the assumption that the requesting state is acting in good faith and that the fugitive will receive a fair trial in the courts of the requesting state.[36]

While requests for extradition are traditionally made through diplomatic channels, extradition proceedings usually involve inputs from both the executive and the judiciary. Most modern extradition treaties seek to balance the rights of the individual with the need to ensure the extradition process operates effectively and are based on principles which are designed not only to protect the integrity of the process itself, but also to guarantee the fugitive offender a degree of procedural fairness.[37] These

[27](1962) 36 I.L.R. 277.
[28]*Jus cogens* "compelling law" means a peremptory norm of general international law from which no derogation is permitted. J. M. Sweeney *et al*, *The International Legal System,* 1988, 1003-8.
[29]*See, e.g.,* US Constitution, art.I, para. 8, clause 10 (granting Congress the right "to define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations").
[30] A. Oyebode, *International Law and Politics: An African Perspective*, Bolabay Publications, Lagos, 2003, p.54.
[31]*Ibid.*
[32]Shaw, *op. cit.*, p.598. Also in *Congo v Belgium* [2002] ICJ Reports, p.3, Judge Guillaume referred to this form of jurisdiction as 'subsidiary universal jurisdiction.'
[33] Article 22 of the *Council of Europe Convention on Cybercrime* empowered parties to the convention to establish jurisdiction over any offence established in accordance with the convention.
[34]*Terlinden v Ames* (1902), 184 U.S. 270 at 289.
[35]Shaw, *op. cit.*, p.610.
[36]Bantekas and Nash, *op. cit.*, p.179.
[37]*Ibid.*, at p.181.

principles include that of double criminality, that is, that the crime involved should be a crime in both states that are concerned. There is also the principle of specialty, that is, a person surrendered may be tried and punished only for the offence for which extradition had been sought and granted. Also, political offences are usually excluded from the extradition proceedings although this would not cover terrorist activities.[38] In addition, many extradition treaties acknowledge the principle of double jeopardy and thus include exemptions for persons who have already been tried and discharged or convicted and punished for the same offence in another state.[39]

3. Evaluation

Until relatively recently, sovereign states, rather than individuals, were the main subjects of international law. An individual can be deemed to be in violation of international law regardless of whether punishment is rendered by the states, individually, or by international courts. But in order for an individual to be liable under international law, the person must commit an offence established under same. Cybercrime poses a problem in the international community because there is no international legal regime outlawing it at present, save regional instruments such as Budapest Convention 2001. Because cybercrime is relatively new, no international norm exists for punishment of offenders. Consequently, cybercrimes can be punished through a mechanism involving municipal law. Such mechanism may, however, involve obtaining cooperation among states to ensure that domestic cybercrime statutes are enforced.

The above difficulty, no doubt, touches on the concept of jurisdiction which describes the authority to affect legal interest. It pertains to which agency or court has the authority to administer justice in a particular matter, and to the scope of those agencies' and courts' authorities. A law enforcement agency or court has jurisdiction only over crimes that take place in the geographic location where that agency or court has authority. Determination of jurisdiction includes the location of the perpetrator, the location of the victim, or the location of the *locus criminis*, that is, where the crime actually occurred. As petered out from this study, the nature of cyberspace constitutes an affront to easy determination of jurisdiction in relation to the prosecution of Internet crimes.

According to Johnson and Post, 'cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location'.[40] They observe that 'the rise of the global computer network is destroying the link between geographical location and (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply'[41]. These scholars conclude that 'the Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules'.[42] How far can international law bridge the online-offline relationship gap?

It goes without saying that the international legal system's traditional rules for jurisdiction depend on localization of conduct or harm. The Internet, on the other hand, challenges all three kinds of jurisdiction, namely, prescriptive jurisdiction, adjudicative jurisdiction and enforcement jurisdiction, because it is difficult to localize legally relevant conduct occurring in the Internet. The first thing that must be determined is whether a cybercrime has taken place at all. In some cases, there is no law that covers the particular circumstance. In other cases, the wrongful action that took place is a civil matter, not a criminal one. This might be the case, for instance, if you entrusted your data to a company and

[38] Shaw, *op. cit.*, p.610
[39] Bantekas and Nash, *op. cit.*, p.189.
[40] RJ David and P David, 'Law and Borders -The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review,* 1367,1370.
[41] *Ibid*
[42] *Ibid*

that company lost it.[43]Jurisdictional questions pose a big problem because laws differ from state to state and nation to nation. An act that is illegal in one state may not be against the law in another state. This complicates things if the perpetrator is in a location where what he is doing is not even against any law, although it is a crime in the location where the victim is.

More still, under international law, the jurisdiction of a state depends on the interest that the state, in view of its nature and purposes, may reasonably have in exercising the particular jurisdiction asserted and on the need to reconcile that interest with the interest of other states in exercising jurisdiction. The nature and significance of the interest of the state in exercising jurisdiction depend on the relation of the transaction, occurrence, or event and of the person to be affected, to the state's proper concern. Thus, under international law, the interest involved is used as a criterion for determining the principle of a state's jurisdiction.

Thus, jurisdictional questions as shown above frequently slow down or completely mar the enforcement of cybercrime laws. Relevant treaties are therefore necessary to provide the legal arrangement between party states for bringing an alleged criminal within the jurisdiction of the court that renders the verdict as to his crime. Extradition treaties can provide for broad extradition powers or, in the alternative, they can specify limited circumstances and offences that are extraditable.[44]The traditional and most common form is where states limit extraditable offences to those punishable under the laws of both states by a specified minimum term of imprisonment.[45]The second form limits the offence, but also includes a particular list of non-extraditable offences. All this is based on the fact that under international law, a country has no obligation to hand over a criminal to the requesting entity, save and except by extradition treaties or by mutual agreement. Even in such cases, it is still a difficult process because extradition treaties often require 'double criminality', meaning that the conduct must be a crime in both the jurisdiction seeking to extradite the suspect and in the jurisdiction from which the extradition is sought. Double criminality is a basic principle under international extradition law. Double criminality means that an act is not extraditable unless it constitutes a crime under the laws of both the state requesting extradition and the state from which extradition is requested. Double criminality is vital in ensuring that a defendant's liberty is not restricted because of offences not recognized as criminal in the state receiving the extradition request. Double criminality appears in one of two forms in extradition treaties.

The principle of double criminality poses a problem to punishing cybercrime at the international level. This is because cybercrime is not treated the same in all countries, and some countries have no laws addressing cybercrimes.[46] Therefore, a loophole still exists. If a cybercriminal were to be a national and a resident of a country that does not have a cybercrime law, it is possible that a cybercriminal could operate across international borders and be spared from extradition to the country or countries that suffered the effects of the cybercrimes he committed.

Another mechanism is found in treaties on mutual assistance which would aid law enforcement and allow governments to go directly to other countries to seek assistance in gathering information.[47] Similar to extradition treaties, mutual assistance treaties may include limitations excluding the investigation of specified offences. Furthermore, some mutual assistance treaties apply the double criminality principle

[43]S Deb, 'What Makes Cybercrime Laws So Difficult to Enforce' (January 26, 20It).Available at<www.tecrepublic.com> accessed on July 24,2014.

[44]See article 24 (2) of the Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, 2001, which provides that offences provided under articles 2 - 11 of the Convention 'shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the parties'.

[45]See generally Nanda & Bassiouni (eds) 'International Criminal Law: A Guide to U.S. Practice and Procedure" (1987) pp. 336-63.

[46]See generally Organisation for Economic Co-operation and Development, 'Computer Related Crime: Analysis of Legal Policy'(1986) p. 10.

[47]Article 7 of the Council of Europe Convention on Cybercrime, CETS No, 185, Budapest, 2001, provides that 'The panics shall afford one another mutual assistance to the widest extent possible for the purpose of investigating or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.

in that only offences that are crimes in both countries can be mutually investigated. If applied to cybercrimes, mutual assistance treaties can be paramount in international cooperation in punishing the offenders. Since the cybercriminal may be in another country when he inflicts his damage, the victim country has no choice but to rely on the investigatory authorities of the cybercriminal's home country.

Yet, certain activities are so universally condemned that any state should have an interest in exercising jurisdiction to combat them. This is a demand before the universality theory[48]of state jurisdiction. Due to the ubiquitous nature of cybercrime and the serious danger it poses to the entire world, it is strongly suggested that universality principle of state jurisdiction under international law should serve as a spring board approach for state jurisdiction in cybercrime cases, pending a fine tuning of the law with the peculiarities of cyberspace. Accordingly, it seems that any state may assume jurisdiction to conduct inquiry and trial of cybercrimes committed anywhere in the world on the ground that the act should be universally condemned, especially given the fact that cybercrime has become a global menace.

[48]See LF Damrosch, *et al, International Law Cases and Materials* (4thedn, Minnesota: West Group, a Thomson Company, St. Paul, Minn., 2001) pp. 1090- 1091.