CHAPTER – II
PROBLEM OF JURISDICTION IN CYBERSPACE
AND ITS IMPACT ON INTERNATIONAL AND
DOMESTIC LAWS

2.1  INTRODUCTION

The jurisdiction is the most crucial question posed in any court of law. If the court does not have jurisdiction, the matter would not be proceeded in the court. The court (Domestic or International) without jurisdiction does not have any authority to entertain the matter, to decide rights and duties or impose penalty or punishment. The cyber space has raised the basic problems of jurisdiction in international laws and domestic laws because of its de-territorial nature. As discussed earlier, internet allows parties to execute transactions without disclosing their identity; and the parties may not even know each other’s location.\(^{32}\) The party may sit at any corner of the world and violate the rights of the other party or person. The paradigm of the jurisdiction in the International law and national law is required to be shifted because of the peculiar nature, increasing use and need of the cyber space.

The customary international law does not allow evasion in a sovereign state by any other (foreign) entity. In the celebrated *Lotus case*,\(^{33}\) the permanent court of justice held that, “now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – *it may not exercise its power in any form in the territory of another State*. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory… except by virtue of a permissive rule derived from international custom or from a convention”.\(^{33}\) (emphasis added)

In other words, the state cannot exercise the jurisdiction on the persons, events and things physically located in the territory of another state. The result of nature of

---


cyberspace in many cases is that the parties to an Internet transaction are faced with overlapping and often contradictory claims that national law applies to some part of their activities.\textsuperscript{34} The problem of multiple and overlapping jurisdiction is more prominent either because the national courts have applied the favorable principles out of available principles of International law or evolved new principle(s) to assume jurisdiction.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state or country where the Website is located or by the laws of the state or country where the Internet service provider is located, or perhaps all of these laws.\textsuperscript{35} A number of commentators and jurist have voiced the notion that cyberspace should be treated as a separate jurisdiction or territory. In practice, this view has not been supported by courts and also not addressed by law-makers.\textsuperscript{36}

As per the mandate of the International Law, no sovereign country can interfere in the sovereignty of others. The control over physical space, people and things located in that space, is a defining attribute of sovereignty and statehood.\textsuperscript{37} Law making requires some mechanism for law enforcement, which in turn depends on the ability to exercise physical control over and impose coercive sanctions on law violation.\textsuperscript{38} Even if a domestic court in a state passes a judgment in a case, the state cannot take a measure that violates another state’s sovereignty.\textsuperscript{39} The advancement of the technology and technological inter-dependence also has an adverse impact on the established principles of the International Law (such as the principle of Sovereign Jurisdiction; Non-Interference; Sovereign Equality, etc.).

\textsuperscript{34} CHRIS REED, INTERNET LAW: TEX AND MATERIAL 217 (2d ed., 2004).
\textsuperscript{35} C.F. R.K. SURI AND T.N. CHHABRA, IT ENCYCLOPAEDIA.COM 72, Vol-11 (1\textsuperscript{st} ed., 2002).
\textsuperscript{36} Ibid.
\textsuperscript{37} PATRICIA L. BELLIA AND PAUL SCHIFF BERMAN, CYBER LAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 75 (1\textsuperscript{st} ed., 2007).
\textsuperscript{38} Ibid.
The objectives of this chapter are as follows:

a) To analyse the various types of jurisdictions and its application by the domestic and international courts.

b) To analyse as to how far traditional doctrines and principles on jurisdiction can be flexibly interpreted and made applicable to the extraterritorial offences in cyberspace.

c) To critically analyse the validity of the application of Domestic Laws to the non-nationals doing offences from another sovereign territory or in future even from Outer Space, High Seas, etc..

d) To analyse the impact of the cyberspace on the established principles of International Law on one hand and application of these principles by the domestic courts of various countries on the other.

e) To comment upon various judgments of the courts to resolve the problem of jurisdiction.

f) To recommend appropriate changes in domestic and international laws.

2.2 CONCEPT OF JURISDICTION UNDER INTERNATIONAL LAW AND ITS APPLICATION TO THE CYBER SPACE

The traditional principles and doctrines of jurisdiction are developed and applied to resolve the problems of the physical world that exist in the pre-cyberspace era. Therefore, there is a need to discuss the concept of jurisdiction and its application to cyberspace.

2.2.1 Concept of jurisdiction under International law

Jurisdiction concerns the power of the state under international law to regulate or otherwise impact upon people, property and circumstances and reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs. It is an aspect of sovereignty and refers to judicial, legislative, and administrative competency. Normally the International law sets little or no limit on the jurisdiction which a particular State may arrogate to itself. Even though the

---

international law sets minimum limitation, the sovereign state shall not control things, events, and persons, etc., which are either totally out of its concern or are completely controlled by other sovereign States. As Mr. Justice H. V. Evatt (in 49 CLR (1993) AT 239), rightly opined, “no state attempts to exercise a jurisdiction over matters, persons or things with which it has absolutely no concern.”

2.2.1.1 Classification of jurisdiction under International law:-

The jurisdiction in the International law is divided broadly as:

a) Civil jurisdiction
b) Criminal jurisdiction

The civil jurisdiction is applied in civil matters and criminal jurisdiction is applied to the criminal matters. In order to apply the above jurisdictions, traditional International law has adopted the following basic principles or doctrines:

i) The territorial principle:
   a) Subjective territoriality
   b) Objective territoriality/ The ‘effects’ doctrine

ii) The nationality principle:
   a) Passive nationality principle
   b) Active nationality principle

iii) Protective or security jurisdiction

iii) Universality jurisdiction

i) The territorial principle

The territorial principle protects the authority of the state over its territory with respect to property, persons and acts occurring in the territory. According to the third, and as a corollary to the first of the *Lotus* principles, it is a fundamental rule of international law that the jurisdiction of a State within its own territory is complete and absolute. It is a basic attribute of sovereignty and flows from the very existence of the state as an international legal person.

The principle has been well explained by Lord Mcmillan. According to him,

“It is an essential attribute of the sovereignty of this realm, as of all sovereign independent states, that it should possess jurisdiction over all persons and things within its territorial limits in all causes, civil and criminal, arising within these limits.”45

The territorial principle is an attribute of control over physical space; but, in reality, persons, things and actions may move across physical boundaries. It functions as a constraint on the strict application of territorial principles that attempts to reconcile “the principle of absolute territorial sovereignty [with] the fact that intercourse between nations often demand[s] the recognition of one sovereign's lawmaking acts in the forum of another”.46

The territorial principle is further divided in the following categories:

a) **Subjective territoriality**47

The subjective international principle allows the exercise of jurisdiction in the state where a crime is commenced.48 Subject to certain immunities under the International Law, this principle is applied when the offence is committed within the sovereign territory of a state irrespective of the nationality of the doer. The crime may be committed against the territorial state or against any other state. Whenever it is punishable according to the laws of the territorial state, the state has jurisdiction to punish the person. The principle of the subjective jurisdiction flows from the principle of territorial sovereignty.

---

47 The subjective and objective principles of jurisdiction were introduced in Article 9 of the Convention for the Suppression of Counterfeited Currency, 112 LNTS 2624, 20 April 1929, and Article 2 & 3 of the Convention for Suppression of the Illicit Traffick in Dangerous Drug, 198 LNTS 4648, 26 June 1936. These principles are also used and distinguished by JB Moore in his ‘Report on Extraterritorial Crime and the Cutting case’, US For Rel 575, 770 (1887).
b) Objective territoriality/ The ‘effects’ doctrine

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.\(^{49}\) The effects principle is based upon the territorial sovereignty of the state. The premise is that a state has jurisdiction over extraterritorial conduct when that conduct has an effect within its territory.\(^{50}\) The above principle is applied by the International court of Justice in the *Lotus*\(^ {51}\) case.

The effect doctrine was developed by USA court while dealing with antitrust law.\(^ {52}\) The significance of decision was that it did not depend upon the commission of the physical acts within US territory, the intentional production of economic ‘effects’ within the United State was sufficient.\(^ {53}\) The doctrine is further followed in the case of *Rio Tinto Zinc Corp v. Westinghouse Electric Corp.*,\(^ {54}\) wherein there was no intra-territorial act. The only basis for jurisdiction was ‘effect’ or economic repercussions of cartel on US.

The objective territorial principle requires intra-territorial action, whereas according to the effects doctrine, a jurisdictional link between the act and the state that claims jurisdiction is constituted by the effects.\(^ {55}\) In short, the ‘effects’ doctrine does not require any intra-territorial conduct, whereas the objective territorial jurisdiction does require at least some intra-territorial conduct to assume the jurisdiction. There are mixed reactions of the European Court of Justice towards ‘effect doctrine’. In *Wood Pulp*\(^ {56}\) case, the court preferred objective territorial principle over the effect doctrine, and basis of jurisdiction in the *Wood Pulp* case was “significantly narrower than the


\(^{50}\) MARK W. JANIS, *AN INTRODUCTION TO INTERNATIONAL LAW* 326 (3rd ed., 1999).


\(^{52}\) See, US v. Aluminium Co. of America, 148 F. 2d 416 (1945).


\(^{54}\) Rio Tinto Zinc Corp v. Westinghouse Electric Corp. [1978] 1 All ER 434 (HL).


\(^{56}\) Ahlstrom and Others v. Commission of European Communities [1988] ECR 5193 [hereinafter referred to as the *Wood Pulp* case).
‘effects’ doctrine in its most extreme form.” 57 Further, in Gencor Ltd. v. Commission of the European Communities, 58 the court held that, “[A]pplication of the Regulation is justified under public international law when it is foreseeable that a proposed concentration will have an immediate and substantial effect in the community.”

The application of this (territorial jurisdiction) principle to the physical world activities is comparatively straightforward; the geographical location of an actor or an object at the relevant time is objectively determinable, and on the basis of the application of the local law appropriate jurisdiction can be decided. 59

The territorial principle cannot completely resolve the problem of the jurisdiction in cyberspace. As discussed earlier, the cyberspace is de-territorial or borderless space, the offence in cyberspace can be committed by any person from anywhere and at any time. The most difficult challenge in resolving the problem of jurisdiction by applying traditional principles of jurisdiction is that the offence in cyberspace can be easily committed against multiple countries. The territorial principle of the jurisdiction does not provide solution to the multiple countries either by establishing common tribunal or otherwise.

There are a number of problems which may arise while applying the effect doctrine to cyber crimes. As discussed earlier, the crime or act in cyberspace may have multiple effects (direct and indirect) on multiple territories; but an actor may not have any intention or Mens Rea to cause the effect on some of the territories. Another problem is that if the accused is caught by one sovereign territory, he/she will not be available to others. Further, the person may be prosecuted and punished in multiple jurisdictions simultaneously; it may cause great inconvenience and lead to injustice. It will also lead to violation of the principle of ‘double criminality’.

The ‘effect doctrine’ can be used as a tool to resolve the problem of the jurisdiction in cyberspace only in instances of offences against one country only. In instances of

impact upon multiple countries, it cannot be an effective solution to the problem of jurisdiction.

i) The Nationality Principle
The principle of Nationality plays a vital role in International law. According to the nationality principle, the State can exercise a direct control over its nationals. The State gets the right to protect and the right to punish its own nationals. The state can legislate to regulate activities of its nationals abroad, whether living there or merely visiting. The nationals of a country are considered to be under the observation of the state, but the state legislations cannot be enforced in another state. In a number of instances, it has been observed that sovereign states are not ready to extradite their own nationals because they assume that they only have authority to punish them. The nationality principle is divided into Passive Nationality Principle and Active Nationality Principle.

a) Passive Nationality Principle
A state may assert jurisdiction over activities which, although committed abroad by foreign nationals, have affected or will affect nationals of the state. This (passive personality) principle authorizes states to assert jurisdiction over offences committed against their nationals abroad. It recognizes that each state has a legitimate interest in protecting the safety of its citizens, when they travel outside national boundaries. In other words, the passive personality principle recognizes that a sovereign can adopt laws that apply to the conduct of foreign nationals who commit crimes against the sovereign’s nationals while the sovereign’s nationals are outside the sovereign’s territory. Though the court can assume jurisdiction under passive nationality principle, the problem with the custody of offender, problem of investigation and extradition will remain unanswered.

---

60 ANTHONY AUST, HANDBOOK OF INTERNATIONAL LAW 44 (1st ed., 2005).
Article 113-7 of the French Penal Code is a unique example of application of the passive personality principle. According to Article 113-7 of the French Penal Code, “French criminal law is applicable to any felony, as well as to any misdemeanor punishable by imprisonment, committed by French or foreign national outside the territory of the French Republic, where the victim is a French national at the time of the offense.” (emphasis added) According to some of the authors, the reach of the French statute intrudes on the sovereignty of other nations and subjects foreign nationals to an indeterminate threat of criminal responsibility in dealings with French nationals.

b) Active nationality principle

A sovereign state can claim jurisdiction on the basis of nationality of the defendant. Individuals are subject to the jurisdiction of their state of nationality because they owe allegiance to that state. The right of a state to regulate the conduct of its nationals everywhere and thus assert nationality as a basis for jurisdiction is widely accepted. International law requires that a state must have a genuine link with the person to assert jurisdiction based on nationality. On the whole, civil law countries (many of which do not extradite their nationals) tend to exercise jurisdiction on the basis of active nationality more frequently than common law countries. Active nationality principle is recognized in many Conventions, which define international crimes and national jurisdiction (such as Article 5(1)(b), Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 1984, UN Counter-Terrorism Convention; UK International Criminal Court Act, 2001 etc.).

---

65 According to ARTICLE 113-9 of French Penal Code, “In the cases set out under articles 13-6 and 113-7 no prosecution may be initiated against a person who establishes that he was subject to a final decision abroad for the same offence and, in the event of conviction, that the sentence has been served or extinguished by limitation.” This Article aimed at avoiding problem of double criminality.
In accordance with the nationality principle, a country has jurisdiction to punish its own nationals who commit offences outside the national territory. These principles cannot be effective solutions when the offence is committed against the nationals of multiple countries.

ii) Protective or security jurisdiction

The protective principle allows a state to prosecute foreigners who have committed acts outside the State’s territory that are directed against the sovereignty or security of the state or endanger its functions. Jurisdiction under the protective or security principle can be resorted to in relation to acts aimed at States themselves committed by anyone, and anywhere. The protective principle applies to treason, espionage and other crimes directly affecting the state’s security, but not to ‘ordinary’ crimes, such as murder and assault. A distinction has to be made between the ‘effects doctrine’ and ‘protective or security jurisdiction’. While jurisdiction based on the ‘effect doctrine’ requires that the effect or result of the offence occurs in the territory of the state claiming jurisdiction, the protective principle applies if the conduct abroad threatens the security, integrity or the proper functioning of the prosecuting state’s government, though there is no effect in the state’s territory.

Protective or security jurisdiction may be useful in exceptional cases. As discussed above, the protective or security jurisdiction cannot be claimed in every ordinary offence. It may be claimed when conduct abroad threatens the security, integrity or proper functioning. In instances of attack on the critical infrastructure or websites of the sovereign state (it may include attack upon the websites of the military or armed forces), the protective principles can be applied. In instances of ordinary crime or copyright infringement, the protective principle does not allow a sovereign state to assume jurisdiction.

---

iii) Universality jurisdiction

The Final Report on the Exercise of Universal Jurisdiction in Respect of Gross Human Rights Offences presented to the International Law Association describes the concept of universal jurisdiction as follows: “Under the principle of universal jurisdiction, a state is entitled, or even required to bring proceedings in respect of certain serious crimes, irrespective of the location of the crime, and irrespective of the nationality of the perpetrator or the victim.”

It means unlike other principles of jurisdiction, the exercise of universal jurisdiction does not require any nexus to the locus delicti, nationality of the offender, nationality of victims, or the interest of the state. Jurisdiction on the basis of the universality principle can be invoked in relation to activities directed against the international community as a whole. According to the First report of International Law Association the State is not only entitled to but also requires to bring action against offences forming part of universal jurisdiction.

The controversy arises from the fact that the International Criminal Court (ICC) can theoretically assert jurisdiction over nationals of states that have not adhered to its statute, provided the state where the crime occurred (the territorial state) has accepted the court’s jurisdiction and other preconditions have been satisfied. The U.S. government has taken serious objection to this particular feature of the Rome Statute. While it has pressed political objections, the United States has also argued that ICC jurisdiction over nationals of non-consenting States is legally impermissible. This type of objections undermines the validity of the universal jurisdiction. There are

---

77 ‘Locus Delicti’ means, the place where the tort, offence, or injury has been committed., See, http://legal-dictionary.thefreedictionary.com/Locus+delicti (last updated on Dec., 16, 2013).
further problems about the perception and interpretation of universal jurisdiction. In
general, universal jurisdiction is associated with the presence of a suspect in the
executing State, whereas some interpret universal jurisdiction as allowing all States to
exercise jurisdiction.\(^8^2\) In other words, according to the first School of Thought the
State can exercise universal jurisdiction only if the accused is present in their
territorial jurisdiction. The second school of thought approves the action of an
individual State even without the presence of the accused in the territory. The
principle approved by the second school of thought is also known as ‘universal
jurisdiction \textit{in absentia}'. The term ‘universal jurisdiction \textit{in absentia}' is also used by
International Court of Justice in \textit{Democratic Republic of the Congo v. Belgium}\(^8^3\)
(Case concerning the Arrest Warrant of 11 April 2000). In practice, both the schools
of thought are followed by the sovereign states.

\section*{Requirement of the presence of the accused in the territory}

The legislations of some of the countries requires the presence of the accused in the
territory, whereas the legislations of other countries do not require any physical
presence of the accused. For example, according to The United Kingdom War Crimes
Act of 1991, the presence of an accused is a must. The above Act allows proceedings
to be brought against a person in the UK irrespective of his nationality at the time of
the alleged offence. Similar provisions are made in Australia and Netherlands.
Requirement of the presence of the accused does not find a place in the legislations of
Spain, Belgium and Germany.\(^8^4\)

Application of ‘universal jurisdiction \textit{in absentia}' to cybercrime or copyright
infringement would pose problem of multiple prosecution in different jurisdictions.
Recognition of the ‘universal jurisdiction \textit{in absentia}' would entitle the sovereign
state to take cognizance of the case, \textit{su o moto} or otherwise, though property of the
accused may or may not be situated in the territory of the state. In a globalised world,

\(^8^2\) \textit{Cf.} Mitsue Inazumi, \textit{Universal Jurisdiction in Modern International Law:}
\textit{Expansion of National} 26 (1\textsuperscript{st} ed., 2005).

\(^8^3\) Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium), Judgment, I.C.J.
Aug., 18, 2013).

\(^8^4\) For further clarification see, Mohamed El Zeidy, \textit{Universal Jurisdiction In Absentia: Is It A Legally
Valid Option for Repressing Heinous Crimes?}, http://ouclf.iuscomp.org/articles/zeidy.shtml#fn58anc
(last updated Nov., 13, 2013).
the property of a person may be situated in multiple countries. In such instances, it is
difficult for the accused to defend himself in multiple countries against criminal
allegations. The multiplicity of the prosecution is against the basic principle of
criminal law i.e. ‘double jeopardy’, which is protected as a fundamental right in many
jurisdictions. It furthermore raises another question: is taking cognizance with respect
to universal jurisdiction a right or an obligation? If it is a right, then the State has
discretion to exercise such jurisdiction, but if it is treated as an obligation, then the
State is bound to exercise universal jurisdiction. Article 90 of the Rome Statute of the
International Criminal Court, 1998, makes extradition as an obligation with respect to
offences punishable under the said statute. The universal justice demands that the
affected sovereign state shall get the first privilege to punish the accused, though the
offence forms part of the universal jurisdiction. The universal jurisdiction does not
ensure the protection of the right to be punished by the affected sovereign state.

As discussed above, the universal jurisdiction is based on the nature and the gravity of
the offence. The above basis is observed in international treaties, customary
international law and also demonstrated by State practices and opinions of jurists. 85
The exercise of the jurisdiction under treaty requires signatures or consent of the
States, whereas customary international law provides jurisdiction to States over the
crimes considered to be of common concern to all States, i.e. erga omnes obligations
owed to the international community or violation of peremptory norms of
international law (i.e. jus cogens). The concept of the universal jurisdiction is codified

In order to resolve some of the issues and develop consensus with respect to universal
jurisdiction, in 2001, a famous Princeton Project was conducted. In this project,
scholars and jurists from around the world participated in their personal capacities.
They laid down 14 famous principles with respect to universal jurisdiction. 86 Principle
1(1) of the Princeton Principles expects state to observe international Due Process;
and according to the Principle 9, in the exercise of universal jurisdiction, state shall

---

85 See, Noora Arajärvi, Looking Back from Nowhere: Is There a Future for Universal Jurisdiction over
86 See also, CHARLOTTE KU AND PAUL F. DIEHL, INTERNATIONAL LAW: CLASSIC AND CONTEMPORARY READINGS 202-216 (2nd ed., 2004).
ensure that a person shall not be exposed to multiple prosecution or punishment for the same criminal conduct. The serious crimes are stated under Principle 2 of the Princeton Principles. It includes Piracy,\textsuperscript{87} Slavery,\textsuperscript{88} War crimes,\textsuperscript{89} Crime against peace,\textsuperscript{90} Crime against humanity,\textsuperscript{91} Genocide\textsuperscript{92} and Torture.

The customary principle of the universal jurisdiction cannot be an effective remedy for the cyber crimes. As analyzed above, universal jurisdiction can be claimed over the crimes considered to be a matter of concern to all states, i.e. \textit{erga omnes} obligations owed to the international community or violation of peremptory norms of international law (i.e. \textit{jus cogens}). The cyber crimes including infringement of copyright are not considered as \textit{erga omnes} or violation of peremptory norms of international law (i.e. \textit{jus cogens}). Therefore, according to customary international law, state practices, \textit{opinion juris} or existing Conventions, the State cannot claim universal jurisdiction for ordinary cyber crimes or copyright infringements.

\textbf{2.3 PROBLEM OF MULTIPLE JURISDICTIONS}

Since cyberspace is a borderless space and the established rules are established by keeping in mind the principles of territorial sovereignty, the established principles need to be either modified, or there is a need to establish new principles of jurisdiction for cyberspace. At present, a number of national courts are using and interpreting established principles, while keeping in mind the interest of their own territory or nationals.\textsuperscript{93} The multiple nations are claiming the jurisdiction on the same subject matter or against the same culprit. All nations are not able to take actual action because of lack of physical presence or property of the accused in a sovereign

\textsuperscript{88} See also, Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others, 1950, Article11; Convention Relative to the Slave Trade and Importation into Africa of Firearms, Ammunition, and Spiritous Liquors, 1980, Article 5 etc..
\textsuperscript{89} See also, Geneva Convention for Amelioration of the Condition of the wounded and Sick in Armed Forces in the Field, 1949, Article 50; Geneva Convention for Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces, 1949, Article 51; Geneva Convention Relative to the Treatment of Prisoners of War, 1949, Article 130; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 1949, Article 147; Protocol I Additional to the Geneva Conventions, 1949, Article 85.
\textsuperscript{90} See also, Charter of the International Military Tribunal 1945, Article 6(a).
\textsuperscript{91} See also, Article 7 of the Rome Statute of the International Criminal Court, 1998.
\textsuperscript{92} See also, Article 6 of the Rome Statute of the International Criminal Court, 1998.
\textsuperscript{93} \textit{Infra}, Chapter no. II. Pp.27-37.
territory. At present, there is no international treaty to compensate loss in proportion, if the action of the person (individual or corporation) is affecting the nationals of multiple countries.

The most basic cause of multiple jurisdictions is the capacity of the individual actor to commit crime against many nations. There are thousands of examples of multi-jurisdictional crimes. Recent news published in The New York Times addresses the gravity of the problem. According to The New York Times, published on May 9, 2013, the hackers distributed the information to individuals in 20 countries who then encoded the information on magnetic-stripe cards. On Dec. 21, 2013, the cashing crews made 4,500 A.T.M. transactions worldwide, stealing $5 million.  

According to USA today, after penetrating the processor's computer network, the hackers fraudulently manipulated the balances and withdrawal limits on Rakbank prepaid debit card accounts. Then, teams of so-called cashers allegedly launched carefully timed attacks that caused more than $5 million in criminal losses from more than 4,500 ATMs in about 20 countries. In this ATM attack people from at least 20 countries are involved. The victims may be from 20 countries or more than that. Similarly, in scenario of linking and copyright infringement links to copyrighted material from different jurisdictions can be provided. In instances of online copyright infringement, multiple jurisdictions can be targeted.

The problem of multiple jurisdictions would be multifold in the near future. This problem would be a cause of concern and it would have a serious impact on the liberty, property and other rights of nationals and economy of states. As discussed earlier, the present principles and doctrines on jurisdiction are not coping with the problem of multiple jurisdictions in cyberspace.

---


2.4 DISORDER THROUGH JUDICIAL ORDERS IN THE AREA OF JURISDICTION IN CYBERSPACE

As discussed earlier, there is a fundamental gap between the notions of personal jurisdiction that is basically territorial in nature and the internet that defies all territorial constraints. This makes the application of territory based doctrines complicated. It has been argued that complexities of internet do not allow the application of traditional legal paradigms and instead requires a separate governing body and a new legal regime. In order to analyze the application of customary principles of international law and new principles developed by various courts, the researcher has considered the following fundamental cases for analysis.

It has been observed that the judicial pronouncements have created chaos in the arena of the jurisdiction in order to preserve the interest of nationals by providing case based and self-centric solutions. In *International Shoe Co. v. Washington*, the court held that plaintiff has to show that the defendant has sufficient minimum contacts with the forum state. According to the court, the personal jurisdiction cannot be assumed without minimum contacts with the forum state. In *Asahi Metal Indus. Co. v. Superior Court*, the US court held that, the website’s effect may be felt nationally or even internationally, but this, without more, was not enough to establish an act that was ‘purposefully directed’ towards the forum state. Based on this judgment, the Court further held that an exercise of personal jurisdiction would violate the protections of the ‘Due Process Clause’ under the US Constitution. In order to meet the Due Process requirements, the court had to satisfy the twin test formula. Firstly, that a non-resident corporate defendant has minimum contacts with the forum state such that it would reasonably anticipate being dragged into court. Secondly,

---

that maintenance of the suit in the forum state would not offend traditional notions of fair play and substantial justice.\textsuperscript{102}

In another case known as a \textit{Dow Jones Case},\textsuperscript{103} a company (Dow Jones & Company) published a Wall Street and Barrons Magazine. This magazine was uploaded on servers maintained at New Jersey, US. It was carrying material allegedly defamatory to the defendant (Joseph Gutnick), resident of Victoria, Australia. In this case, the most basic question posed was the question of jurisdiction of the court. The court held that the material is downloaded in Victoria. Thus, the court in Victoria has jurisdiction and Victorian law would govern the rights and duties of the parties.

Two other courts of the US had taken contrary view on the issue of jurisdiction. In \textit{Young Case},\textsuperscript{104} the court has taken a completely opposite view. In this case, two newspapers had published material with defamatory comments about Mr. Young (a Jail Warden). The District Court held that the Virginia (US state) court has jurisdiction, but the US Court 4\textsuperscript{th} circuit reversed the judgment. The Appellate Court held that the newspaper neither targeted their websites for Virginia audience nor had they posted articles from them and merely because any one could download the articles from the website did not give jurisdiction to the courts in Virginia.

The view taken by court in \textit{Young case} is further supported by \textit{Zippo Mfg. v. Zippo Dot Com, Inc.}\textsuperscript{105} The court, in this case, has applied jurisdiction based on nature of website i.e. active or passive.\textsuperscript{106} Again in \textit{GTE New Media Services, Inc., v. BellSouth Corp.},\textsuperscript{107} the Appellate Court rejected the finding of \textit{Zippo case} and employed the standards of ‘purposeful direction’ and ‘intended effects’\textsuperscript{108} rather than standards based on the ‘interactive’ nature of the website. In some other cases, rather than

\begin{itemize}
\item \textsuperscript{103} Dow Jones and Company Inc. v. Gutnick, (2002) HCA 56.
\item \textsuperscript{104} Young v. New Haven 315 F. 3d 256 U.S. Appl. [2002].
\item \textsuperscript{105} Zippo Mfg. v. Zippo Dot Com, Inc.152 F. Supp. 1119. The court has pronounced sliding scale test in this case.
\item \textsuperscript{106} If a site allows browsers to enter into binding contracts, the court would consider that site as an ‘active’, and if the website is only providing certain information to the web browser, the site would be considered ‘passive’ website.
\item \textsuperscript{107} GTE New Media Services, Inc., v. BellSouth Corp. 199 F.3d (D.C. Cir. 2000).
\item \textsuperscript{108} ‘Purposeful Direction’ and ‘Intended Effects’ doctrines were well established doctrines of traditional International Law.
\end{itemize}
applying the principle of ‘intended effect’, the courts have applied the ‘minimum contact principle’. Minimum contacts with a jurisdiction would be established based on domicile, consent or committing actions in the State, such as doing business or committing a tort. Even though the court has the power to apply jurisdiction, the State has still to decide the reasonableness of the application of the jurisdiction. The US court has used five factors while determining the reasonableness of the contact. The five principles concluded by the court are: 109

1. The burden on defendant;
2. The forum state’s interest in adjudicating the disputes;
3. The plaintiff’s interest in obtaining convenient and effective relief;
4. The interstate judicial system’s interest in obtaining the most efficient resolution of controversies;
5. The shared interest of several states in furthering substantive social policies.

The court further in Telco Comm. v. An Apple A Day held that posting of a defamatory press release on an internet site was sufficient to confer jurisdiction over and out-of-state (US) party who should have reasonably known that their press release would be disseminated outside the state of origin.

In Sarl Louis Feraud International v. Viewfinder, Inc. case, the plaintiff, a French company, had organized a fashion show in France. The defendant Viewfinder had posted photographs of the fashion show on its website. Sarl Louis Feraud International (Plaintiff) filed a suit in French court for unauthorized use of intellectual property and unfair competition. The suit was decreed ex parte by French court (the Tribunal de grande instance de Paris). The plaintiff sought to enforce the decree. The United States District Court for the Southern District of New York dismissed the suit holding that: “The French Default judgment is incompatible with the First

---

109 Burger King Corp. v. Rudzewicz, 471 USA 462[1985]
111 In traditional International Law, courts used to apply the principle of, ‘Forum Non Convenience.’ According to this principle, the court should try to find out the ‘natural forum’, that is the forum (court), ‘with which the action has the most real and substantial connection’. See also, Spiliada Maritime Corporation v. Cansulex Ltd. (1987) 1 AC 460.
Amendment and with Article 1, Section 8 of the New York State Constitution. Its enforcement would, therefore, be repugnant to the public policy\textsuperscript{114} of this State, in violation of C.P.L.R. 5304(b)(4)” (emphasis added). The appellate court held that, it seems that the decision of the District court is based upon the assumption that the Viewfinder is a news magazine supposed to report public events and has an absolute First Amendment defense. The appellate court further pointed out that, “Intellectual Property Laws co-exist with the First Amendment in this country.” The appellate court tried to balance the author’s rights with First Amendment to the Constitution of US. The judgment was remanded for further proceedings consistent with the opinion of appellate court. The apparent conflict in this case was that the French court had considered the act of the defendant as an infringement of IPR, whereas the US court had considered the judgment of French court against ‘public policy’ and ‘First Amendment’ to the US Constitution.

Another important case of the jurisdiction is Yahoo Inc v. La Ligue Contre Le Racisme Et Antisemitisme.\textsuperscript{115} The Yahoo! is a US-based service provider. The Yahoo was providing services in twenty other nations. Every national service had a two-letter code in its URL. The services operated in France were operated at http://www.yahoo.fr. The above page was providing services in local languages. The Yahoo! was also providing Yahoo!’s auction site. The Yahoo! auction site was allowing anyone to post an item for sale and solicit bids from computer users around the globe. Yahoo! was providing the site but was never a party to a transaction. According to Yahoo! Policies, the auction sellers were prohibited from offering items to buyers in jurisdictions in which the sale of such items violates the jurisdiction’s applicable laws. Display of Nazi material or sale of Nazi-insignia is made illegal in France.\textsuperscript{116} Since it is made an offence in France, there was no Nazi material or insignia at http://www.yahoo.fr., website created for France. The discussion about Nazism had occurred in chat room of American website. The American website was also carrying the information about the prohibited auction material. The US Yahoo!

\textsuperscript{114} See also, New York Law- "A foreign country judgment need not be recognized if . . . the cause of action on which the judgment is based is repugnant to the public policy of this state." N.Y.C.P.L.R. § 5304(b) (4) (emphasis added).


\textsuperscript{116} See, Section R 645-1 of the French Criminal Code.
website was accessible to French nationals and had the opportunity (accesses) to purchase auction items including Nazi paraphernalia.

Two civil liberty groups brought an action in French court. According to the finding of the French Court nearly 1,000 Nazi and Third Reich related objects, including Adolf Hitler's *Mein Kampf*, *The Protocol of the Elders of Zion* (an infamous anti-Semitic report produced by the Czarist secret police in the early 1900's) were being offered for sale on Yahoo.com's auction site.

Yahoo! challenged the jurisdiction of the court, but its plea was denied. After a hearing on May 15, 2000, the French court issued an interim order on May 22 requiring Yahoo! to “take all necessary measures to dissuade and render impossible any access [from French territory] via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes”.

Yahoo! objected to the order and contended, among other things, that “there was no technical solution which would enable it to comply fully with the terms of the court order”. The court gave three months time to comply with its order. The Yahoo! brought an action in US District court for declaration of invalidity of the French court’s order in US. The District court held that enforcement of the French order in US would violate First Amendment of the Constitution. Therefore according to court they were unenforceable in the US.

The French liberty groups filed an appeal against the above finding of the court. Yahoo! Sought a declaration from the Court that the First Amendment precludes the enforcement within the United States of a French order intended to regulate the content of its speech over the Internet.

### 2.4.1 Analysis of judgments of courts

The test laid down in *International Shoe Co. v. Washington*[^118] *i.e.* ‘the minimum contacts’ test has its own limitations. In instances of passive websites directed towards global community at large, there cannot be ‘minimum contacts’ more than


mere accessibility with particular nation. The object of these types of websites may be to make material available or accessible to the globe at large. For example, pornographic websites are not intentionally directed towards a particular State. They are made accessible to the world community at large. In such cases, it is difficult to prove ‘minimum contacts’ more than mere accessibility with a particular country; and it is also difficult to prove ‘purposeful direction’ towards a particular country only. Similarly, in online copyright infringement, copyrighted material may be accessible to whole of the world. The ‘minimum contact’ with a particular nation may not be established or it may not be ‘purposefully directed’ towards that nation. Therefore, minimum contacts, if any, established in such instances is against the world at large. Therefore, application of these doctrines to the copyright infringement would make authors helpless. They may not be able to prove establishment of ‘minimum contact’ or ‘purposeful direction’ towards a particular country.

The ‘minimum contacts’ and ‘purposeful availment’ doctrines would have multiple advantages. Firstly, it gives reasonable idea to the defendant about the probable action i.e. suit or litigation. As Michael Geist pointed out that: “...a foreseeability metric lies at the heart of the reasonableness standard. This metric dictates that a party should only be hauled into a foreign court where it was foreseeable that such an eventuality might occur.” Secondly, in maximum cases it avoids multiplicity of jurisdiction because it is difficult to prove purposeful direction towards a particular State, though the website is accessible in that state. In World-Wide Volkswagen Corp. v. Woodson, the court held that, what was relevant was the foreseeability, “that the defendant's conduct and connection with the forum state are such that he should reasonably anticipate being hauled into court there.” The principle of foreseeability can be further supported on the ground of traditional notions of fair play and substantial justice recognized by US court in International Shoe Co. v. Washington.

Thirdly, the ‘purposeful availment’ doctrine further supports territorial sovereignty principle of international law and the traditional understanding of the law. As discussed earlier (in Introduction), according to the traditional notion of the law, a

\]

\[\text{120} \quad \text{World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980).}
\]

\[\text{121} \quad \text{International Shoe Co. v. Washington, 326 U.S. 310, 316 [66 S.Ct. 154, 158, 90 L.Ed., 95] (1945).}
\]
person cannot be held responsible under laws of another sovereign state unless he/she either enters into the territory or the other sovereign territory is directly or indirectly affected. The adoption of the ‘purposeful availment’ doctrine saves the individual actor from the application of the laws of all countries though material is accessed or downloaded in almost all the sovereign states. Therefore, problem of multiple jurisdictions and multiple prosecutions can be minimized by applying the above principles.

The *Sarl Louis Feraud International v. Viewfinder, Inc.*\(^\text{122}\) can be criticized on various grounds. According to several authors, the first implication of the District court judgment is that it has adhered to the customary rule of the territorial jurisdiction. According to them the District court has assumed that the laws of the territory are only binding on the territory and other territories’ law cannot be enforced on the said territory. As per Thomas Schultz “If this approach was followed globally, then websites would be subject only to the law of the state from which the flow of information stems. It would make forum shopping very easy, as it would be sufficient to find a country with the appropriate legal regime and publish any content there such content remaining, in principle, accessible from the place where the publisher actually wanted it to be so accessible, even if it was in violation of the laws of the country from which it was accessed.”\(^\text{123}\) As Horatia Muir-Watt puts it, “there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it”.\(^\text{124}\) These authors expect different treatment to cyberspace. The above criticism points out that the court would have considered the laws protecting French nationals. The United States District Court for Southern District of New York dismissed the suit holding that enforcement of judgment by French court is against ‘public policy’. The basic question about the ‘public policy’ is: whose ‘public policy’


should govern the internet activities? Should it be US or particular nation’s policy or policy of the world community? The obvious answer to this question would be the policy of the world community at large. Therefore, there is a need to establish supranational forum to decide and implement the ‘public policy’ applicable to the internet. The above notion of the application of every state’s law to the borderless medium would give rise to other multiple problems.125

As discussed above, Yahoo Inc v. La Ligue Contre Le Racisme Et Antisemitisme126 is another important case in the arena of jurisdiction. The basic difference between the Sarl Louis Feraud International v. Viewfinder, Inc.127 and Yahoo! case was that in the first case the copyrighted material was protected both in France and US. Therefore, the US court restricted claim of IPR violation in the light of First Amendment to US Constitution. In Yahoo! case the act was not made an offence in US but was punishable in France.

The number of authors raised the objections against judgment in Yahoo Inc v. La Ligue Contre Le Racisme Et Antisemitisme.128 According to Rinat Hadas the instant court did not attempt to discuss moral acceptability of Nazi propaganda.129 One difficulty in this decision, arising from First Amendment application is, whose law applies to the Internet.130 Professor Jack Goldsmith proposed that it was proper for France to exercise jurisdiction over Yahoo! because “Yahoo has something on its

125 For detailed explanation on other problems posed by cyberspace see, Chapter no. IV, Pp. 92-126.
website that is being accessed by French citizens that violates the French law”.\footnote{Cf. Carls Kaplan, \textit{French Nazi Memorabilia Case Presents Jurisdiction Dilemma}, CYBER LAW JOURNAL August 11, 2000, http://partners.nytimes.com/library/tech/00/08/cyber/cyberlaw/11law.html (last updated Dec., 24, 2013).} He further noted that the United States could likewise enforce its own laws against content posted in France, and concluded that “the harmful effects are running in both directions.”\footnote{Cf. Marc H. Greenberg, \textit{A Return to Lilliput: The Licra v. Yahoo! Case and the Regulation of Online Content in the World Market}, BERKELEY TECHNOLOGY LAW JOURNAL [Vol. 18:1191. P. 1212], http://www.btlj.org/data/articles/18_04_05.pdf (last updated Aug., 20, 2014).} Rabbi Cooper rejected the First Amendment defense and urged that (as Judge Gomez did) there is a need to value the moral values. Rabbi Cooper further pointed out that, “It’s good to try to wrap yourself around free speech . . . but in this case it doesn’t wash. Television stations, newspapers and magazines refuse to accept some advertisements in an effort to marginalize viewpoints and products that the vast majority of Americans think are disrespectful or even potentially dangerous. Internet companies . . . should just do what American companies have been doing for half a century: reserve the right not to peddle bigotry.”\footnote{Cf. Marc H. Greenberg, \textit{A Return to Lilliput: The Licra v. Yahoo! Case and the Regulation of Online Content in the World Market}, BERKELEY TECHNOLOGY LAW JOURNAL [Vol. 18:1191. P. 1212], http://www.btlj.org/data/articles/18_04_05.pdf (last updated Aug., 20, 2014).}

The problem of conflict of law and conflict of jurisdiction in this case reminds the world community about requirement of uniform standards or rules for cyberspace. The problem of the jurisdiction raised in the French case shall be analyzed from both angles. From the angle of the sovereign state, the state could not effectively exercise its sovereign right to enact and implement the laws, though the website is accessible in its territory. Further, France, a sovereign state, cannot ask for extradition of the culprit. Since the act is not punishable in the US, the extradition by the US would be against the principle of ‘double criminality’. It is important to note that ‘double criminality’ principle is a well established principle of international law. The said principle invalidates the extradition. From the user’s point of view if every country like France starts imposing restrictions on speech and expression on internet, the cyberspace would be a subject matter of immense restrictions; practically it may not even be possible to utilize this most effective medium of communication. The user would be in constant fear of prosecution in some or the other sovereign state.
In instant case, each country feels its own laws are important and although the instant court's decision sends a message that the United States will not enforce foreign orders that violate the First Amendment and other countries do not agree that the Internet should be regulated by the US right to free speech. The US court would have applied the principle of comity by responding to the international obligation against racism activities. Ironically, military tribunal led by America known as Nuremberg Trial punished the accused on the ground of violation of crime against humanity and other crimes. Crimes against humanity include “murder, extermination, enslavement, deportation and other inhuman acts committed against any civilian population, before or during the war; or persecutions on political, racial or religious grounds in the execution of or in connection with any crime within the jurisdiction of the Tribunal, whether or not in violation of the domestic law of the country where perpetrated.”

It simply means US is observing double standard while dealing with the “Crime against humanity”.

The above verdict of the tribunal can be used to counter the argument based on the principle of ‘double criminality’. As discussed earlier, the offence against humanity (including offence involved in this case) can be punished irrespective domestic law. Therefore, in present case there extradition by US would not have violated the principle of ‘double criminality’. Furthermore, as discussed in *Sarl Louis Feraud International v. Viewfinder, Inc.*, the Supreme Court itself in a number of cases held that First Amendment of United States is not an absolute right. It has been subject to exceptions. In other words, the right granted in the First Amendment of US shall be balanced with the rights of others. The racism can be an obvious exception to any Constitutional guarantee. It needs to be further noted that interpretation of the US court is against prevailing rules of interpretation adopted by modern civilized countries. Now modern states including India have started interpreting domestic laws in the light of international obligation. The American court had prime

---

reasonability to impose reasonable restrictions in the light of the international law, including crimes against humanity in the present case.

The above analysis shows that European and US courts are providing self-centric solutions rather than co-operating and aligning with other states at international level. Such conflicting judgments of various courts show that the judicial orders have created disorder in the arena of cyberspace.

**Cyber jurisdiction and other practical problems**

Acceptance of the principle based on accessibility or effect theory would also cause multiple problems. At present conducts on internet is governed by the territorial laws of every sovereign country. The act may be conducted in a particular sovereign country but in principle it would have access to almost every country. In instances of common offence recognized by almost every country, there would be the problem of multicity of prosecution.

In addition to these the other major challenges analyzed are given below:

First of all, if it is punishable in a forum country (i.e. State having presence of an accused and property of the accused) then that country would claim jurisdiction. The property may be seized by that country. The said country would only be able to impose fine and imprisonment. The actual victim country or other sufferer countries would not get opportunity to punish the culprit. It simply means that victims of other sovereign states would not be compensated or no justice would be provided to them. Secondly, in instances of drastic difference in punishment, lenient approach of the court towards offence, possibility of delay or acquittal or act being not punishable in some of the countries, the offenders would take shelter or would prefer prosecution in the country, where they get maximum benefits. If the court providing minimum punishment takes cognizance, the other countries may not be able to take cognizance because of protection against ‘double criminality’. In instance of the offence punishable in one country and not punishable in other country, the accessibility principle would not work. According to established principle of international law (i.e. double criminality) it would be wrong to prosecute the person in forum state, where act is not punishable or extradite him to the requesting state. In cases the court of the sovereign state claims jurisdiction or passes **ex parte** judgment or decree, the question
of implementation could not be resolved. Prescriptive jurisdiction cannot, in any way, ensure power of enforcement or power to bring culprit to justice in accordance with local laws. Further extradition in every cyber offence is virtually impossible due to multiplicity of the parties and the offences involved.

Therefore, the apparent solution in the above mentioned instances is to establish international tribunal with benches at regional levels. These courts or tribunals shall be at par with the International Court of Justice. The sovereign state should have responsibility to co-operate as it is provided under Rome Statute of the International Criminal Court, 1998. Further there shall be mechanism to implement the judgments and orders of such court. 138

2.5 INDIAN POSITION OF THE JURISDICTION IN CYBERSPACE

Now the question arises as to what is the position of jurisdiction of cyber space in India? In majority of instances the Indian Penal Code, 1860139 (IPC) and Information Technology Act, 2000 (IT, Act) in India deal with the above mentioned problem. Section 2 to 4(2)140 of the IPC deals with territorial and extra territorial offences. The

---

138 See, Infra. Chapter no. V, “Conclusion and Recommendations”, Pp. 146-148. In this chapter the researcher has given various suggestions to implement the orders of the supra-national tribunal.
139 It is pertinent to note that the author of the copyrighted work may file a case for mis-appropriation of property under section 403 of IPC. The mis-appropriation of property may also be claimed for providing links to the copyrighted material. The only problem in India for charging person for mis-appropriation of the property is the definition of the ‘movable property’ provided under section 22 of the IPC. According to Section 22 of IPC, “The words ‘movable property’ are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.” The copyright is not a ‘corporeal property’ as required for charging person under section 403 of IPC. But section 22 is an inclusive section, therefore, the intellectual property can be interpreted under term ‘movable property’ for the purpose of section 403 of IPC.
140 Section 2-4 of IPC are as follows:

**Section 2 of IPC: Punishment of offences committed within India:**
Every person shall be liable punishment under this Code and not otherwise for every act of omission contrary to the provisions thereof, of which, he shall be guilty within [India]

**Section 3: Punishment of offences committed beyond, but which by law may be tried within, India:** Any person liable, by any (Indian law) to be tried for an offence committed beyond (India) shall be dealt with according to the provisions of this Code for any act committed beyond (India) in the same manner as if such act had been committed within (India).

**Section 4: Extension of Code to extra-territorial offences:** The provisions of this Code apply also to any offence committed by

1. Any citizen of India in any place without and beyond India;
2. Any person on any ship of aircraft registered in India wherever it may be. Explanation: -In this section the word “offence” includes every act committed outside [India] which, if committed in [India], would be punishable under this code.
IPC is made applicable to the any offence committed by the Indian citizen in the whole of the globe. In the instances of a person (non citizen) doing offence outside the Indian territory, the offence does not fit in the scope and ambit of the Indian Penal Code, 1860. Therefore offence conducted by the person from other sovereign nation in cyberspace is not punishable under Indian Penal Code, 1860. Another important legislation, IT Act, 2000 is enacted to resolve the problem of jurisdiction in India.\textsuperscript{141} The Information Technology Act, 2000 is applicable to the citizen and non citizens committing crimes outside the India territory (Section 1(2) and 75\textsuperscript{142} of the IT Act, 2000).

It is submitted that even section 75 of the Information Technology Act, 2000 and section 3 and 4 of The Indian Penal Code provides extraterritorial jurisdiction. The provisions of both the Acts have only partially resolved the problem of the jurisdiction. According to sub-section 1 of the section 75 of the Information Technology Act, 2000 the jurisdiction with respect to the offence or contravention committed outside India by any person irrespective of his nationality the IT Act, 2000 would be applicable. The sub-section 1 of the section 75 is subject to qualification provided under sub-section 2 of the section 75. Sub-section 2 of the section 75 of the Information Technology Act, 2000 applies to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention ‘involves’ a computer, computer system or computer network located in the territory of India. The word ‘involve’ is very broad word. It may include the offence committed by the foreigner against another foreigner of different country involving computer network located in the territory of India. In such cases the offence may be conducted on internet from one sovereign state to another sovereign state via network located in India. In above example though internet network is located in India neither interest of Indian territory nor citizen of India is involved in any manner.

\textsuperscript{141} For understanding the relation of IT Act, 2000 and copyright protection see, Praveen Dalal, \textit{Long Arm Jurisdiction of Courts Regarding Copyright Law in India}, JIPR, http://nopr.niscair.res.in/bitstream/123456789/4890/1/JIPR%209%286%29%20557-567.pdf (last updated Sep., 22, 2014).

\textsuperscript{142} Section 75 of IT, Act, 2000 is as follows:

\textbf{Act to apply for offence or contravention committed outside India}: - (1) Subject to the provision of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub- section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.
Therefore, these types of broad wording of the legislation are in conflict with the territorial principle of the international law.

In addition to above sections, section 13 of Information Technology Act, 2000 is also relevant to analyze the problem of jurisdiction in cyber space. Section 13 deals with time and place of dispatch and receipt of electronic record. Sub-Section 3 of the section 13 is worded as follows: “Save as otherwise agreed\textsuperscript{143} between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.” Section 13 of the IT Act, 2000 assumed the place of dispatch and place of receiver of electronic record at the place of business, irrespective of actual place of dispatch or receipts of the electronic record. This assumption is important because it provides jurisdiction to the Indian courts if the place of business of originator or addressee is in India. According section 13 the court will have jurisdiction though the electronic record in fact may or may not be received in or dispatched from the computer, computer systems or computer mechanism situated in India. Normally, the court gets jurisdiction at the place of business, place of dispatching of electronic record and place of receiving the electronic record. Section 13 of the IT, Act, 2000 will have overriding effect on CPC and Cr.P.C.\textsuperscript{144} As discussed above, according to statutory assumptions created under section 13 of IT Act, 2000 though the person is residing and dispatching an electronic message from the territory of India and if his place of business is outside the territory of India, the Indian court cannot exercise the jurisdiction. Similarly, according to said assumption created under section 13 the court can assumed jurisdiction though electronic message is dispatched or received outside the territory of India if the person receiving or dispatching an electronic message has place of business in India.

It needs to be noted that because of section 13 of the IT Act, 2000 the Indian court would not be able to take cognizance of the matter though act of dispatching electronic message is partially or fully conducted from the territory of India. Further,

\textsuperscript{143} It is pertinent to note that word ‘Agreed’ is used in sub. 3 of Section 13, it means by agreement parties can decide the place of receiving and dispatching the electronic record. It is needed to be noted that parties cannot decide jurisdiction of criminal law. Therefore, jurisdiction according to section 13 of IT, Act, 2000 cannot be applied to the criminal offences, including copyright infringements. Thus, sub. 3 of Section 13 of IT Act, 2000 would be applicable to civil wrongs only.

\textsuperscript{144} See, Section no. 81 of IT Act, 2000
because of this statutory assumption the court would be unable to take cognizance of
the matter even if the electronic message has an adverse impact on rights or interests
of the citizen(s) of India. The assumption created under section 13 of IT Act, 2000
does not have any advantage as such because otherwise also according to general
principles of jurisdiction and CPC and Cr. P.C the court was empowered to take
cognizance of the matter at the place of the business of the person. Section 13 of the
IT Act, is apparently inconsistency with territorial and passive nationality principles
of International law on jurisdiction.

Section 4 of the Indian Penal Code, 1860 has been amended by amendment Act,
2008. According to new sub-section (3) of section 4 of Indian Penal Code, the code
would apply to “any person in any place without and beyond India committing
offence targeting a computer resource located in India”. According to explanation (b)
the expression “computer resource” shall have the same meaning assigned to it in
clause (k) of sub-section (1) of section (2) of the Information Technology Act, 2000
(21 of 2000). According to the new provision of the Indian Penal Code, 1860 for
applying the India Penal Code “targeted computer resource” shall be located in India.

It is pertinent to note that the word ‘targeting’ is used in sub-section 3 of section of 4
IPC, 1860. The word ‘targeting’ is not further defined or clarified by the legislature.
The literal or dictionary meaning of ‘targeting’ is ‘aiming at’. The literal or
dictionary meaning of words used in criminal law is needed to stress out because the
rule of strict interpretation is applicable to the criminal law. The rule of strict
interpretation implies the strict or literal interpretation of the criminal law. It is
submitted that, after applying the rule of strict interpretation, there is a doubt whether
IPC would be applied when: a) aim or target is not a computer resources but a person.
It means the intention is not to cause wrongful loss to the computer resources
including computer or data per se but to the person via or with help of computer
resources (for example by publishing the defamatory comments). In this example
‘means’ and ‘target’ are different. ‘means’ is computer resource and ‘target’ is a
person. Therefore, in the above example offence is committed with the help of

145 According to Section 2(1) (K) “computer resource” means computer, computer system, computer
network, data, computer database or software. The word “computer system” is further defined in
computer resource and not by targeting it. b) the offences are committed via network located in India; c) wrongful loss is caused to the person by making data accessible to the entire world including India but date is copied from the computer located outside the territory of India d) In the examples of passive websites registered and created outside India (for example photographic websites) but accessible in India. Similarly, a website with unauthorized copyrighted material may have access in India without targeting computer resources located in India. In these examples the target is not computer resources located in India per se. The intention is to make it accessible to the entire world. Incidentally, it would be accessible in India also. The above explanation shows that the jurisdiction clause is resource (object) centric rather than victim centric.

Apart from above both these legislations would not be applicable to the recent development that is services of cloud computing. The services of cloud computing may be provided by the person, company or corporation. In cloud computing the computer resources may not be physically located in the territory in India. The relation between the cloud computing company and the person staying or residing in India would be governed by the cloud computing agreement. The cloud computing agreement is a contractual liability. It is a civil liability subject to term and conditions of the agreement. Further the jurisdiction of the court depends upon the ‘choice of the law clause’ agreed by both the parties to contract. In instances of lack of choice of law agreement, general rules of jurisdiction would be applied.

It is further submitted that in the instances of the agreement between the parties, the body corporate may be responsible under Section 43A of the Information Technology Act, 2000. According to Section 43A of the Information Technology Act, 2000:
“where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, in negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”
It is submitted that according to Section 75 of IT, Act, 2000 or Section 4 of the IPC, the above mentioned body corporate should be located in the territory of India or shall use the computer resources located in India. In other words, Section 43A would not work in isolation. It is not an exception to the Section 75 of the Information Technology Act, 2000. It shall be interpreted along with Section 75 of the IT Act, 2000. It is submitted that reading Section 43A of IT, Act, 2000 in isolation would be inconsistent with basic rule of interpretation of statutes (i.e. statute shall be read as a whole). It is pertinent to note that Section 43A does not provide any liability of the actual offender (i.e. a third person committing offence from foreign jurisdiction with the help of computer etc. situated outside India). In an example of cloud computing or liability under section 43A of the Information Technology Act, 2000, if the body corporate was not negligent in implementing and maintaining reasonable security practices and procedures, then no liability can be imposed against the said body corporate.

Furthermore, section 75 of the IT Act, 2000 or sections 4 of Indian Penal Code, 1860 do not provide jurisdiction in scenario when an offence is committed by foreigner from other country against citizen of India by using computer resource located outside India. For example, in instances of Indian nationals carrying the computer resources with them outside the Indian territory, no express jurisdiction is provided to Indian courts under IPC, 1860 or Information Technology Act, 2000. In examples of social websites also the computer resources located in the territory of India may not be used.

Apart from above, section 1 (2) and section 62 of Indian Copyright Act, 1957 are relevant to analyze the problem of jurisdiction in cyberspace. According to section 1 (2) of the Indian Copyright Act, 1957, the Indian Copyright Act extends to the whole of India. According to section 62 (1) of the Indian Copyright Act, 1957, “Every suit or other civil proceeding arising under this chapter in respect of the infringement of copyright in any work or the infringement of any other right conferred by this Act shall be instituted in the district court having jurisdiction”. Further, according to section 62(2) of the Indian Copyright Act, 1957 for the purpose of sub-section 1 district court include a district court within the local limits of whose jurisdiction, at the time of the institution of the suit or other proceeding, the person instituting the suit or other proceeding actually and voluntarily resides or carries on business or
personally works for gain. The explanation on above sections shows that the Indian Copyright Act, 1957 is made applicable to the Indian territories only. It does not provide any express provision for extra-territorial application of the Indian Copyright Act, 1957.

It means Indian laws on jurisdiction are location (territory) centric rather than victim or offender centric. In other words, the IT Act and IPC are the glaring examples of non application of the passive nationality principle recognized by International Law. It is respectfully submitted that the Indian Parliament lacks visualization of nature and probable offences committed with help of cyberspace. The Indian laws on jurisdiction need to shift offence centric paradigm to offender and victim centric.

The amendment to IPC is partially providing relief or remedy from possible misuse of computer resources. It may be noted that the Amendment Act fails to provide relief or remedies against the offences committed by the person, when the computer resources are not located in the territory of India, though the rights of Indian citizens are infringed.

Though the IPC and IT, Act, 2000 provides partial jurisdiction to courts implementation of the Acts depends upon the extradition treaty of India with the territorial states or friendly diplomatic relations with the respective countries.

Apart from above sections 178, 179, 182 and 188 of the Criminal Procedure Code, 1973 deals with the issue of jurisdiction. Section 178 of Criminal Procedure Code deals with place of inquiry or trial. The section 178 provides jurisdiction to the court when the act, fully or in part, arises in the said territory. Section 179 of Criminal Procedure Code provides jurisdiction to the court on the basis of the act done or its impact. According to section 179 of Cr.P.C, 1973, “when an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued”. The Criminal Procedure Code has adopted territorial principles and impact theory of jurisdiction. Section 182 of Cr. P. Code deals with offences committed by letters or telecommunication messages. It provides jurisdiction where letters or messages were sent or received. Section 188
deals with offence committed outside India. It provides the same jurisdiction as provided in the original Indian Penal Code.

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra,\textsuperscript{147} is a first case from India about the cyber defamation. In this case High Court of Delhi assumed jurisdiction over a matter of defamation of reputation of corporate through e-mails. The court passed an \textit{ex-parte} injunction. The Supreme Court of India, in SIL Import v. Exim Aides Silk Importers\textsuperscript{148} pointed out that judiciary needs to interpret a statute in the light of technological change that has occurred. Until there is specific legislation in regard to the jurisdiction of the Indian Courts with respect to Internet disputes, or unless India is a signatory to an International Treaty under which the jurisdiction of the national courts and circumstances under which they can be exercised are spelt out, the Indian courts will have to give a wide interpretation to the existing statutes, for exercising Internet disputes.\textsuperscript{149}

\subsection*{2.6 JURISDICTION IN CYBERSPACE: EUROPEAN UNION APPROACH}

The jurisdictional matter of civil and commercial disputes of the European Union is governed by the Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial matters.\textsuperscript{150} The Regulation is issued by the Council of European Union and in operation from March, 2002. Article 2 of the Regulation provides jurisdiction based upon domicile of the person irrespective of his nationality. In instances of performance of the contractual obligation a person can be sued at the place of performance of the obligation in question (Article 5.1.). According to the Article 13, the consumer can sue in his own courts against trader if “in the state of consumer’s domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising”. The consumer may further sue a trader at home court in accordance with Article 15. For suing trader in home court, the trader should pursue commercial activities in the state of consumer’s domicile or by any means direct such activities towards the said member state. In instances of

\textsuperscript{149} See also- http://lexwisdom.wordpress.com/author/lexwisdom/ (last updated Dec., 11, 2013).
question related to whether trader directed activities towards a particular member state or not, the European Court of Justice is appropriate authority to decide the matter.

The EU member states are also signatories to the Rome Convention, 1980. The Rome Convention, 1980 provide jurisdiction based upon ‘choice of law’, but it must demonstrate reasonable certainty (Article 3.1.). Apart from ‘choice of law clause’ ‘mandatory rule’ of consumers’ habitual residence will be applied (Article 5). In case of absence of ‘choice of law clause’ the contractual relations of the parties will be governed by the law of the country with which it is ‘most closely connected’ (Article 4.1.).

Further the Council of Europe helps in protecting societies worldwide from the threat of cybercrime through the Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and the technical cooperation Programme on Cybercrime.\textsuperscript{151} According to Article 11 of the Cyber Crime Convention, 2001\textsuperscript{152} the ratifying states to “adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences”. Article 11 of the above Convention imposes the liability upon the signatory states to enact relevant laws with respect to the above subject matter. Article 11 of the Cyber Convention does not provide direct jurisdiction to the domestic courts. It imposes liability upon the sovereign states. There is possibility that sovereign state would enact either favourable laws or there can be problem of conflict of laws.

The Article 22 of the Cyber Convention, 2001\textsuperscript{153} provides jurisdiction based on territorial principles. It also includes ship flying the flag of that party, aircraft registered in accordance with respective parties’ laws. The sub-clause (d) (1) of the

\begin{footnotesize}\textsuperscript{151} http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (last updated Nov., 19, 2013).


\textsuperscript{153} Cyber Convention, 2001 is applicable to the member States of the Council of Europe and the other States signatory hereto.\end{footnotesize}
Article 22 incorporated the nationality principle. According to clause (d) (1) party shall adopt such legislative and other measures to establish the jurisdiction if offence is committed by “by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State”. Clause 2 of Article 22 provides privileges of the parties to lay down certain conditions. The clause 4 of the Article 22 of the Cyber Convention gives privilege to the parties to establish jurisdiction in accordance with their own national laws. Further, according to clause 5 of the Article “When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.”

The privilege given in clause 4 of the Article provides party to establish jurisdiction based on their own domestic laws. Claiming jurisdiction in accordance with their own national laws would continue the problem of conflict of laws and case laws. Further consultation provided under Clause 5 of the Article may not be effective because; a) there is no intervention by third party or international community. The egoist nations may not compromise on certain points; b) the consultation process is followed by the executives. It would not have any direct impact unless there is an amendment to domestic laws. In instances of the amendment to the domestic law also no retrospective effect can be given to the criminal law. In other words, no justice can be provided to the existing victims by amending criminal law.

In many high-technology crimes the physical presence of the offender is not a defining factor.154 Crimes can therefore be committed from jurisdictions that have the

weakest legal framework and law enforcement infrastructure to counter them. Further, the “consent of the governed” implies that those subject to a set of laws must have a role in their formulation.

2.7 JURISDICTIONAL ISSUES IN CYBERSPACE AND ITS IMPLICATIONS ON VARIOUS ESTABLISHED TRADITIONAL PRINCIPLES OF INTERNATIONAL LAW

Jurisdictional issues in Cyberspace and Its Implications
The information age has significant effect on the doctrine of territorial sovereignty, international law and relations between and amongst the states on the one hand and non-state entities and states on the other hand. The foundation of the doctrine of sovereignty, non-interference, sovereign equality are affected and the horizon of the national and international law is continuously widening because of de-territorial nature of the cyberspace. Due to development of cyberspace and technology the concept of territorial sovereignty is being liberalized, and the states and nationals are exposed to whole of the world. The information technology has not only increased inter-dependence between Domestic Laws and International Law but also has changed the power structure, including power to decide matter affecting nationals of a sovereign state. The technological advancement is also empowering the non-state actors, such as inter-governmental organizations (IGOs) and non-governmental organization to assume decision-making role, previously reserved primarily to

---

157 For further explanation on above doctrine see, Westphalian model of sovereignty. According to Westphalian model of sovereignty three fundamental principles of international law are: Exclusive control over the nation’s territory, non-interference, and equality between States. The above principles are also recognized under Article 2 of UN Chapter, 1949.
sovereign states. For example the ICANN, a body established by US law has assumed the jurisdictional power with respect to the domain name disputes, though it is not an international body established by UNO. Thus technological advancement has an impact on traditional concept of sovereign jurisdiction and statehood.

2.7.1 Legalization of the International and Domestic Laws vis-à-vis Technological Advancement

Consent and bargaining power of states are some of the assumptions behind the legitimization of International Law. According to a rationalist-institutionalist (such as Hurrell) the bargaining outcomes determining the degree of legalization of a regime depend on the capabilities and resources of the individual actors involved in its formation. According to Hurrell, the institutionalist interpretation gives incomplete picture of complex linkages between power and law that shape the role of law in international politics. In other words, according to this school of thought though the implied or express consent is given by the state, it would not legalize international law in true sense.

Some critics claimed that there is a systematic tension between norm-oriented and interest-based politics. They pointed out that under the veil of ‘legalization’, long standing principles of International Law have been abandoned to make the structures on international conflicts and co-operation more responsive to the interest of the powerful, ‘multilateral’ agreements that are accused of advancing a hegemonic order (Trachtman 1997; Wiener 1999).

159 It is needed to be noted that consent is not a sole source of international law there are other sources also such as general principles recognized by civilized nations, writing of jurist, judgments of International Court of Justice etc. (See. Art. 38 of the Statute of International Court of Justice, 1945)
160 Moreover it is one of the requirements of the legitimization of the private International Law.
162 Ibid., P.10.
163 CHARISTIAN BRUTSCH AND DIRK LEHMKUHL, COMPLEX LEGALIZATION AND THE MANY MOVES TO LAW, LAW AND LEGALIZATION IN TRANSNATIONAL RELATIONS 10 (1st ed., 2007).
Many other jurists of the International Law believe that internet undermines the feasibility –and legitimacy –of laws based on geographical boundaries.\textsuperscript{164} The technologically powerful states are able to establish corporations\textsuperscript{165} to control sovereign\textsuperscript{166} power of other states. According to the representational concept, an individual is the most important unit of analysis in the international system; and a truly sovereign state represents the general will of its populace.\textsuperscript{167} Which means that the legitimacy of applying a state’s laws to conduct that occurs in another State’s territory depends on whether such laws would prevent (that) state from functioning as a sovereign.\textsuperscript{168} The above process of legalization of international law is not followed while establishing the so called international body like ICANN.

The present laws of governing internet are territorial in nature. There is no effective mechanism at international level to protect rights of individuals.\textsuperscript{169} In this situation, the nationals of other state are left with no choice but to accept the policy of ICANN to avail (at least partial) worldwide protection to their domain names.

Therefore, applying the laws to multiple states without giving it bargaining power has impact upon the process of legalizing in the International Law. In present instance, US was able to establish and declare ICANN as international body because of emergence of cyberspace.

### 2.7.2 Impact of cyberspace on the Doctrine of Sovereignty

The doctrine of territorial sovereignty assumes the control of the state over the territory including the living and non-living things. Thus legal competency of the states and the rules for their protection depends upon and assumes the existence of a


\textsuperscript{165} The USA has established ICANN Corporation, which has the authority to take decisions, affecting nationals of other States, with respect to Domain Names.

\textsuperscript{166} The word ‘sovereignty’ is used in the broader sense include privilege to decide the matter related or affecting to nationals in the territory.


\textsuperscript{169} Trips and WIPO imposes obligation on the state and no remedy is provided for the infringement of copyright infringement by individuals from other country.
stable, physically delimited homeland. Law making sovereignty itself – internationally recognized “statehood”-is defined, at bottom, by control over a physical territory, over which it has control. This means that the sovereign has the suprema potestas in local matters and as such has superior authority over its powers of command. In traditional sense it also means that when a person is in a territory, the other territorial laws would not be applied. The International Law also allows the state to react, in case of interference by other state or non-state entities. The relation of the cause and effect underlines the parallel principle that a state may be held responsible under International Law for damage which it causes in the territory of another state. In these cases, under the International Law the state gets extraterritorial jurisdiction. General principle has now emerged that a state may exercise jurisdiction if there is a sufficiently close connection between the subject matter and the state to override the interests of a competing state. The principle of territorial sovereignty is not applied in strict sense in the era of cyberspace. However, there are many cases in which multiple sovereign states are claiming jurisdiction at a time. As discussed earlier, the logic of claiming jurisdiction is that their nationals have access to material on internet.

The jurisdiction and the prerogative of enactment of the laws and enforcement of the laws in relation to territory are important facets of the doctrine of sovereignty. The technological advancements have adverse impact on traditional sovereign privilege to take decisions in relation to citizens and non-citizens vis-à-vis cyberspace.

173 If a citizen of the country is in another country then, he/she would be governed by both countries laws. According to personal jurisdiction nation’s law would be always applicable to nationals. And as soon as a person would enters in another country’s territory that country’s law would be applicable but third country’s law would not be applied.
174 Alfred P. Rubin, Pollution by Analogy: The Trail Smelter Arbitration (Abridged), in TRANSBOUNDARY HARM IN INTERNATIONAL LAW 46 (Rebecca M. Bratspies and Russell A. Miller ed., 2006).
175 The principles followed in the extraterritorial jurisdiction (i.e. Territorial Principle, Nationality Principle, Protective Principle, Passive and Active Personality Principle, Universality Principles etc.) are analyzed in Chapter no. II. Pp. 15-25.
As discussed above, the technologically advanced states are in position to control sovereign power of the other states. ICANN\textsuperscript{178} is one such type of corporation. ICANN is established by US government.\textsuperscript{179} The corporation is organized, and will be operated, exclusively for charitable, educational, and scientific purposes according to § 501 (C) (3) of the Internal Revenue Code of 1986 of US. ICANN is in a position to take decisions in relation to the nationals of other countries.\textsuperscript{180} As discussed earlier, International Law is legitimized if it is consented by the parties or it is a decision of the international community in its interest. The ICANN policy is a contract between a domain name holder and the ICANN. It is not a contract between two or more nations. Though policy is consented by an individual, it still does not legitimatize the action by ICANN because the other party (individual) does not have any bargaining power. The individuals and the nations are helpless because of the need of domain name facility and protection. The US, under the garb of ICANN controls the activities of the non-national in relation to the domain name such as registration, cancellation, transfer and change of domain name. This has an adverse impact on the well-established principles of sovereignty, sovereign equality and non-interference.

\section*{2.8 CONCLUSION}

The virtual world is a set back to the traditional principles; but sovereignty and other principles discussed above would not completely disappear. The jurisdictional and choice-of-law dilemmas posed by cyberspace activity cannot be adequately resolved by applying the “settled principles” and “traditional legal tools” developed for

\textsuperscript{178} Internet Corporation for Assigned Names and Numbers, Headquartered in Marina Del Rey, California, United States.
\textsuperscript{179} On September 29, 2006, ICANN signed a new agreement with the United States Department of Commerce (DOC), that was a step towards the full management of the Internet's system through ICANN.
\textsuperscript{180} According to Paragraph 3. of the policy the ICANN may cancel, transfer or change domain name. The ICANN is authorized to take the above action in following circumstances:

\begin{itemize}
  \item a. Subject to the provisions of Paragraph 8, on receipt of written or appropriate electronic instructions from domain name holder or his/her authorized agent to take such action;
  \item b. If ICCAN receives an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
  \item c. If ICCAN receives a decision of an Administrative Panel requiring such action in any administrative proceeding to which domain name holder was a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN.
  \item d. The ICANN may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of Registration Agreement or other legal requirements.
\end{itemize}
analogous problems in real-space. In *Yahoo! Case*, criminal act was not punishable in other court but still the court had initiated the proceeding against Yahoo! US. The logic given in Yahoo! Case was that the material had access in French territory. Therefore, despite the person being out of the territory, he may be held responsible for the act committed in cyberspace. Does this mean that before doing activities in the cyberspace, laws of all the countries shall be kept in mind? Traditional International Law does not compel a person to observe the laws of other nations unless he/she enters into that territory or that territory is directly affected. In the era of internet, it is difficult to observe, how many countries are directly or indirectly affected. In this chaotic situation there is a need to establish a supra-national organization to deal with problems posed by cyberspace.

As discussed above, the established principles of law and international law are either not responding to or are not able to resolve the problems posed by cyberspace. The cyberspace is fundamentally different from physical space. It is fundamentally different in its nature, control, extent and impact. Internet is new and separate jurisdiction in which the rules and regulations of physical world do not apply as it is. According to some of the authors it is a seamless global-economic zone, borderless and unregulatable.

Further, the cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network has destroyed the link between geographical location and application of laws. It has dire impact upon: (1) the *power* of local governments to assert control over online behavior; (2) the *effects* of online behavior on individuals or things; (3) the *legitimacy* of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply.

---

182 Yahoo!, Inc. v. La Ligue Contra Le Racisme et L'Antisemitisme, 145 F.Supp.2d 1168 (N.D.Cal.2001)
As discussed earlier, according to old philosophy of law the activities in a territory shall be governed by the laws and regulations of a respective sovereign state. The said philosophy cannot be applied to cyberspace. The cyberspace needs to be recognized as a separate jurisdiction because neither individual sovereign state is able to control it nor the legitimacy of any rules governing online activities be naturally traced to a geographically situated polity.\textsuperscript{185} There is no geographically localized set of constituents with a stronger claim to regulate it than any other local group; the strongest claim to control comes from the participants themselves, and they could be anywhere.\textsuperscript{186} According to David R. Johnson and David G. Post, many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle i.e. conceiving cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between cyberspace and the “real world”.\textsuperscript{187} This solution is subject to lots of limitations. A number of questions are required to be answered to realize the above mentioned solution for the multiple problems posed by the cyberspace. The first and foremost question needed to be answered is: who shall enact the rules and regulations for the cyberspace? Who is authorized to enact such types of rules under international law? What shall be the nature of rules and regulations? Shall it follow the common law system or civil law system, or should it be a neutral set of rules and regulations?\textsuperscript{188} In case of conflict with national laws what will be the consequences? Who should have authority to investigate and prosecute the infringer? Who shall finance these organizations? Who shall have authority to punish the person international or intra-national tribunal or national court? What shall be the place of such organization?\textsuperscript{189} What about the rights of the accused person? The problem will be more acute in the event of nations adopting the dualism theory to implement international law. If national court or authority refuses to accept the investigation or

\textsuperscript{185} David R. Johnson and David G. Post, Law and Borders: The Rise of Law in Cyberspace, in CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 151 (Peter Ludlow ed., 2001).


\textsuperscript{188} For detailed explanation on the different and conflicting standards and principles followed in different jurisdictions- see chapter no. III. Pp. 56-91.

\textsuperscript{189} In case said organization is authorized to arrest, investigate, prosecute and punish the culprit. It may not be feasible for them to travel thought the world and investigate.
prosecution of such authority, what shall be the remedy against such stubborn nation?\textsuperscript{190}

To answer the above questions globe needs to move from territorial philosophy to new legal philosophy known as global transnationalism. The international law will have to act in such a way so as to resolve the conflict considering the rights and interests of every affected party. For that purpose the cyberspace shall be declared as \textit{res extra commercium} (i.e. territory not subject to national appropriation, such as high seas). To manage this territory, there shall be a supra-national organization under the control of UNO. Establishment of such organization under UNO would have multiple advantages such as: a) the State would get bargaining power while taking decisions; b) the technologically powerful countries will not be able to use arbitrary domination over other nations; c) it would lead to harmonization of the rules and systems, which would lead to amicable and faster solutions to the conflicts.

At present the use of principle of co-operation, comity,\textsuperscript{191} justice by giving due regard to the international duties can be a solution to the problem of jurisdiction posed by the cyberspace.

\textsuperscript{190} Under International law normally states claim right to punish to their own citizens. Though the cyberspace may be recognized as a separate ‘place’ or ‘space’ all nations may not be agree to prosecute and punish the culprits in their custody or their citizens according to the rules and regulations recognized for cyberspace. At present International law is a weak law. There is no effective measures and mechanism to control stubborn nations. The international community is facing the same problem in case of terrorism activities also.

\textsuperscript{191} The doctrine of comity, in the US Supreme Court’s classic formulation, is “the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law.” See, Hilton v. Guyot, 159 U.S. 113, 163-164 (1895). See also- David R. Johnson and David G. Post, \textit{Law and Borders: The Rise of Law in Cyberspace}, in \textit{CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS} 165 (Peter Ludlow ed., 2001).