JURISDICTION, EXTRADITION AND MUTUAL LEGAL ASSISTANCE AGAINST CYBER TERRORISM

Benjamin Okezie Kalu[1]

***Abstract*:** Cyber terrorism poses a significant global threat, exploiting the anonymity and transnational nature of cyberspace to conduct attacks that transcend geopolitical borders. The complexity of combating cyber terrorism is exacerbated by jurisdictional ambiguities, making the identification, extradition, and prosecution of offenders challenging. This paper explores the principles of jurisdiction, extradition, and mutual legal assistance (MLA) as they relate to cyber terrorism, highlighting the need for coherent international legal frameworks to address jurisdictional conflicts and gaps in procedural laws. It examines traditional principles of territorial, extraterritorial, and nationality jurisdiction, as well as emerging mechanisms like MLA, and underscores the importance of international cooperation to ensure effective prosecution and deterrence of cyber terrorism. The paper concludes by advocating for the establishment of a multilateral criminal law convention to provide uniform standards for handling cyber terrorism cases, thereby enhancing global legal coherence and cyber deterrence.

Keyword: Jurisdiction, Extradition, Mutual Legal Assistance, Cyber Terrorism.

INTRODUCTION

Jurisdiction refers to the legal authority, capacity, and power of a court to adjudicate on a matter in dispute, involving control over both the subject matter and the parties. It necessitates that the court is properly constituted and has legitimate power over the issue at hand. Without jurisdiction, any decision or order made by a court is deemed to be null and void, rendering it as "coram non judice," which means outside the purview of judicial authority, and therefore "non est," or not legally existent.

The nature of cybercrimes and cyber terrorism presents unique jurisdictional challenges. These crimes are characterized by their anonymity, cross-border operations, and ability to be executed remotely, which complicates the process of identifying the perpetrators or the exact location of the crime. Unlike traditional crimes, where

[1] Independent Research, Nigeria.

jurisdiction is typically determined by physical presence or direct impact within a territory, cybercrimes often involve multiple jurisdictions simultaneously, as they can target victims in various countries and be perpetrated from a different location altogether.

In cyberspace, cyber terrorism may involve numerous entities and government agencies, such as law enforcement, judicial bodies, and intelligence services, working together to track down suspects and establish the legal basis for prosecution. Due to the global nature of cyberspace, legal frameworks related to jurisdiction, extradition, and mutual legal assistance are fragmented, leading to significant challenges in ensuring swift, fair, and predictable legal processes. The diversity of national laws and procedural rules across different jurisdictions remains a major barrier to effective legal cooperation, as countries may have divergent definitions of cybercrimes, varying procedural requirements, and different approaches to legal assistance.

Additionally, the rapid advancement of technology and the proliferation of the Internet have facilitated the conduct of business and communication at both national and international levels. The Internet, as a cornerstone of modern information technology, offers a platform for instantaneous communication and commerce across the globe, eliminating traditional geographical barriers and reducing the relevance of distance in commercial transactions. This, however, also creates potential conflicts of laws when disputes arise in an international context, as it is often unclear which jurisdiction's laws should apply.

The dynamic nature of the Internet and the global reach of cyber activities pose a serious dilemma in terms of conflict of laws. As technology evolves, so too must legal principles and frameworks adapt to address these new realities. Determining the appropriate jurisdiction in cases involving cyber terrorism is crucial to ensure effective prosecution and deterrence. This involves an evaluation of existing national and international jurisdictional principles to determine which framework is best suited to addressing the complexities of cybercrimes in a manner that respects sovereignty while ensuring accountability and justice.

The objective of this work is to critically analyze and compare jurisdictional principles at the national and international levels to identify the most suitable approaches for establishing jurisdiction in the context of cyber terrorism. It seeks to explore how legal systems can be restructured or reformed to provide clarity and coherence in handling cyber-related offenses, thereby overcoming the limitations posed by traditional jurisdictional doctrines when applied to the borderless world of cyberspace. The research will address key questions related to jurisdictional conflicts, harmonization of laws, and international cooperation to enhance the global community's ability to combat cyber terrorism effectively.

INTERNATIONAL LAW OF JURISDICTION FOR CYBER TERRORISM

Public international law governs relations between independent sovereign States. It is the body of rules, which are legally binding on States in their intercourse with each other. The rules are not only meant only for the States but also for the international organisations and individuals. And in case of a private dispute, if any, settlement mechanism is increasingly being provided by the 'private international law'. Generally, private international law is that body of law, which comes into operation whenever a domestic (municipal) court is faced with a claim that contains a foreign element. Hence, the public international laws reflect the juxtaposition of States (as a legal person) and subject their jurisdictional sovereignties to certain limitations, *i.e.* there is a general prohibition in international law against the extraterritorial application of domestic laws[2]. The concept of judicial jurisdiction of a court emanates from the *Sovereignty Theory* and *Territorial Theory* of State. Under this classic formulation, each State is supreme and has unquestionable authority within its geographical limits. Outside a State's border, there has been another nation or State with complete authority over its own territory, foreclosing the exercise of jurisdiction by any other State.

[2] —In the absence of municipal laws, international treaties ratified by India can be taken into account for framing guidelines in respect of enforcement of fundamental rights‖ in *Vishaka* v. *State of Rajasthan,* AIR 1997 SC 3011; *Lakshmi Kant Pandey* v. *Union of India,* AIR 1984 SC 469.

Jurisdiction is the *sine qua non* for any dispute arising in the international arena, because it determines which state court has the authority to adjudicate such a dispute. It is an aspect of a State's sovereignty[3] and is confined geographically.[3] Jurisdictional rules vary in accordance to different state practices. Yet all States have rules that stem from the maxim *actor sequitur forum rei*[4]. Domicile as a jurisdictional connecting factor was developed in Ran law and maintained by civilian courts. At common law a court had no jurisdiction outside its territorial limits[4]. Jurisdiction in relation to State is understood as the terrestrial area within which the sovereign power of the administrator can be exercised. Jurisdiction in relation to a court is the territory and the subject regarding which a court has been empowered to take cognizance and to try a case. International law defines ―jurisdiction" as: ―jurisdiction describes the limits of the legal competence of a State, to make, apply, and enforce rules of conduct upon persons. It concerns essentially the extent of each state's right to regulate conduct or the consequences of events.[5]

The nature of the Internet gives the ability to the user to disguise its identity, leading to inherent difficulties in determining the states that fail to prevent an attack from being originated within their borders. Therefore, states must cooperate with each other to share information in order to attribute attackers.[6] The issue of jurisdiction which incapacitates a State under international law to prescribe or to enforce a rule of law, has to be looked into from three perspectives, in accordance to the level of authority, as: (a) Prescriptive

[3] I. Brownlie, *Principles of Public International Law*, 6th edn., Oxford University Press, 2003, p. 297.
[3] *Extra territorium jus dicenti, impune non paretur* (one who exercises jurisdiction out of his territory may be disobeyed with impunity): *Singh* v. *The Rajah of Faridkote* [1894] AC 670, 683 (PC). [4] The claimant must follow the forum of the thing in dispute. *See* R Phillimore, *Commentaries upon International Law*, 3rd edn, Vol. 4, Butterworths, London, 1879, p.891.
[4] *Lenders* v. *Anderson* (1883) 12 QBD 50, 56; *Ingate* v. *La Commissione de Lloyd Austriaco, Prima Sezione* (1858) 4 CB NS 704, 708 (CP); *Trower & Sons Ltd* v. *Ripstein* (1944) AC 254, 262 (PC); *Pennoyer* v. *Neff* 95 US 714, 722 (1877).
[5] V. Lowe, *Jurisdiction in International Law,* Malcolm D. Evans (ed.), 2nd edn, United Kingdom, 2006, p. 335.
[6] L. Grosswald, "Cyber Attack Attribution under Article 51 of the U.N. Charter', *Brooklyn Journal of International Law,* Vol. 36, 2011, p. 1151.

jurisdiction; (b) Enforcement jurisdiction and (c) Authority to adjudicate;[7] these can be discussed as follows:

(a) ***Prescriptive jurisdiction:*** The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things.[8] It provides authority to prescribe the capacity to establish and prescribe criminal and regulatory sanctions, normally prerogative of a government. As a general rule, a State's prescriptive jurisdiction is unlimited and a State may legislate for any matter irrespective of where it occurs or the nationality of the persons involved.[9] Hence, the State legislative enactments primarily reflect its prescriptive jurisdiction. For example Section 75 of the Information Technology Act, 2000 provides for extra territorial jurisdiction of the court as prescriptive jurisdiction.

(b) ***Enforcement Jurisdiction:*** A State's ability to enforce those laws and is necessarily dependent on the existence of prescriptive jurisdiction. It provides the authority to enforce the capacity to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgments, as well as the capacity to investigate suspect behaviours, both normally also prerogative of a government.

(c) ***Authority to adjudicate:*** It provides the authority to judge the competence to hear disputes, normally prerogative of courts. It is the legislative function of the Government to enact laws and judicial function (and/or administrative) to enforce those laws. It is important to note that the principles of jurisdiction followed by a State must not exceed the limits which international law places upon its jurisdiction. However, the sovereign equality of States means that one State may not exercise its enforcement jurisdiction in a concrete sense over persons or events actually situated in another State's territory irrespective of the reach of its

[7] Restatement (Third) of Foreign Relations Law of the United States, 1987, Sec. 401.
[8] *Ibid*. Sec. 402.
[9] Ian Brownlie, *Principles of Public International Law*, 5th ed., Oxford, University Press, 2002, p. 58, law-making capabilities are one of the factors that determine the coexistence between nations.

perspective jurisdiction. That is, a state's enforcement jurisdiction within its own territory is presumptively absolute over all matters and persons situated therein.

Besides these above manifestations of the jurisdiction, there are three generally accepted bases of jurisdiction/theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity. They are:

A) Territorial Jurisdiction;
   a) Subjective territorial jurisdiction; and
   b) Objective territorial jurisdiction.
B) Personality/Nationality Jurisdiction; and
C) Universal Jurisdiction.

Territorial jurisdiction

Generally, each state has competence in the assertion of jurisdiction over their citizens and incidents occurring within its national territory. Territorial jurisdiction is the most common and unanimous basis for jurisdiction and it is the most significant and applicable method in international law. It is divided into two categories, namely: —subjective territorial jurisdiction" and —objective territorial jurisdiction".

The *subjective territorial jurisdiction* happens when an attack begins in state A, but is completed in State B. State A would then have subjective territorial jurisdiction and State B, *objective territorial jurisdiction*. However, if this doctrine were applied, a complication arises which stems from the nature of the Internet and the realities of cyber terrorism, i.e. cyber terrorism operates without borders and cyber terrorism attacks target computer systems and power grids. Furthermore, the most difficult scenario is in determining the location of the perpetrator, its computer system and network. As discussed, cyber terrorism happens in cyberspace, and cyber terrorists utilise various advanced tools, which they operate from remote destinations, and from various computers located in different spaces. They use fake IP addresses or anonymous ones to conceal their real location and actual identity. In addition, they have sufficient technological tools to pretend that the attack came from elsewhere. They operate beyond the territory of any state and often use computers in multiple states in order to launch their attacks.

Therefore, it is almost impossible to determine where the information and international data exists or which jurisdiction's laws are applicable. On the other hand, even if this is feasible, it costs a huge amount of money.[10]

Consequently, according to the state principle, a state may exercise jurisdiction even when the act commences in one state and is consummated in another state. The broad scope of this principle may seem proper to combat cyber terrorism cases as two cases support this idea. In *R* v. *Waddan*[11], an English resident set up a pornographic website on a US-based server, published obscene material in the UK, and the users could access and download such material in the UK. The UK court allowed the prosecution of an English resident. In another case, the *Toeben Case*[12], a ―Holocaust Denial" website was established on an Australian server by an Australian resident. This website could be accessed in Germany. Thus, the prosecution vested in Germany under the German Anti-Nazi legislation. On the basis of the broad effect of these cases, territorial jurisdiction can be applied to a variety of offences in the same way as it would apply for cyber terrorism. Since usually the effect of a cyber-attack may be felt in many countries, then according to the territorial principle, each of these states has a right to prosecute.[13] Territorial jurisdiction may seem to be highly relevant to cyber terrorism, but the UN General Assembly (UNGA) and other international organisations consider it as a threat to international security and ―emerging universal offences".

Despite this, it seems that territorial jurisdiction is the best method to respond to transnational crimes; but it may face many problems. *Firstly*, in cyber terrorism cases, the intent of the crime may originate from a directly or indirectly government supported terrorist group; therefore, it is doubtful that that state would prosecute the offenders. *Secondly*, the act may remain unpunished under the law of that state as it is not forbidden

[10] Pardis Moslemzadeh Tehrani and Nazura Abdul Manap, A Rational Jurisdiction for Cyber Terrorism, *Computer Law & Security Review*, Vol. 29, 2013, pp. 689―701.
[11] *R* v. *Graham Waddon*, Southwark [Crown Court, 30/6/1999].
[12] German Federal Court, decided on 12 December, 2000.
[13] A. Bianchi, *Enforcing International Law Norms Against Terrorism*, 1st edn., Hart Publishing, United Kingdom, 2004, pp. 474-479.

according to its laws. However, due to the grave damage which occurs with these kinds of crimes, the state cannot leave the perpetrators without punishment because, according to the definition of territorial jurisdiction, ―states can assert jurisdiction over behavior occurring within their territorial border". In cyber terrorism cases, the physical location of the act is far from the effect of the act. Therefore, the commission of the act is not the same as the effect of the act.

Extraterritorial jurisdiction

Since time immemorial, the exercises of jurisdiction by states have been limited to persons, property and actions within a state's territory. However, with the rise of international corporations and the advent of the virtual world, states have been encouraged to exercise jurisdiction beyond their territorial harbours. States extend their jurisdictional authority beyond their territories by exercising extraterritorial jurisdiction. However, extraterritorial jurisdiction suffers from some technical ambiguity. On the one hand, each territory has the right to enact regulations and have their own regulations which cover behaviour occurring within their domestic territories. On the other hand, the acts of individuals and groups affect others beyond national territories and state borders.[14]

The globalised nature of the Internet poses conceptual challenges to the territoriality of a state. Territorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions.[16] In general, the national courts are based upon each state's domestic laws and their legislative courts are limited to their territory. The absence of geographical and political borders in cyberspace makes the use of territorial jurisdiction for sovereign jurisdiction problematic. As a result, due to the many territorial jurisdiction loopholes and the limited deterrence offered by these, territorial jurisdiction, when compared with universal jurisdiction, cannot provide sufficient methods to prosecute cyber terrorism.

[14] The IBA, Report of Task Force on Extraterritorial Jurisdiction, United States, 2009, p. 13. [16] Jack. L. Goldsmith *The Internet and the Abiding Significance of Territorial Sovereignty*, *International Journal of Global Legal Studies*, Vol. 5, 1998, p. 475.

In May and November 2000, a French court ordered the United States to block access of French users from a US website, because it offered online auctions of Nazi memorabilia, which is prohibited under French criminal law. Nevertheless, there was no such law in the United States and thereby it was possible for French users to take part in the online auction of Nazi memorabilia. The French court then handed down a decision based on the findings of an international panel of experts. They recommended blocking French nationals from the site by using screening technology based on the Internet protocol address of the users' computers. With such technology, they could block the French nationals' access by approximately 70 percent (however, they could increase the access to almost 90 percent by completing a nationality questionnaire by the Internet Service Provider). The French court thus attempted to regulate US activities within the US on the basis that such activities could be accessed by Internet users in France. Finally, a United States court held that the French court had no right to make such an order affecting the operation of a US website.[15] Thus, extraterritorial jurisdiction may often violate the national sovereignty of another state. This case, *the Yahoo Case*, that caused conflict of jurisdiction between the United States and France, is an example of a very wide extraterritorial effect.[16]

Nationality jurisdiction

Each of the State of the world has ability to assert jurisdiction over its citizens, even when they reside outside its borders in some cases. The personality or nationality principle includes active and passive nationality. *Active nationality* focuses on the nationality of the perpetrator. In doing so, the state has the ability to assert jurisdiction over crimes committed by its nationals abroad. Thus, a state can assert jurisdiction over a crime which is not committed within its borders solely on the basis of the perpetrator's nationality. *Passive nationality* refers to the victim's nationality. This enables a state to

[15] A. Manolopoulos, "Raising Cyber Borders: The Interaction between Law and Technology', *International Journal of Law and Information Technology*, Vol. 11(1), 2003, pp. 41-44.

[16] ValerieSedallian, Commentaire de l'affaire Yahoo (1), Revue du Droit des technologies de l'information, 24/20/00, at paragraph 20, retrieved from *http://www.juriscom.net* on 29/05/2011.

[19] The IBA, Report of Task Force on Extraterritorial Jurisdiction, United States, 2009, p. 14.

assert jurisdiction over a crime which happens outside its territory but against one of its nationals.[19]

Among [17]all countries, the United States is the most important example of having court decisions that adopt personal jurisdiction. The Fourteenth Amendment of the United States Constitution lays down the principles of personal jurisdiction. US courts have applied the principle of the International Shoe Case[20] in cases involving internet crime.[18] A person must have some relationship with a US state in order to be sued in that state. According to this principle, a United States court may exercise jurisdiction over a person for any dispute, if the person has substantial, systematic and continuous contact with the forum state and even if the conduct is unconnected to the forum state. In the case of *Helicopteros Nacionales de Colombia* v. *Hall*, the court held that due to the insufficient contacts which did not constitute continuous and systematic activity, the court could not assert general jurisdiction.[19]. The US Federal Court has long-arm statutes providing three basic grants of jurisdiction: *firstly*, it authorises federal courts to ―borrow" the long-arm statute of the state in which the federal court is located.[20] *Secondly*, federal rule authorises federal courts to exercise grants of personal jurisdiction contained in federal statutes.[21] *Thirdly*, federal rule grants long-arm jurisdiction in an international context, within the limits of the Constitution, over parties to cases arising under federal law who are not subject to the jurisdiction of any particular state.[22]

When the defendant is not domiciled in a state in order to be subject to personal jurisdiction, the defendant must be qualified under the state long-arm statute and simultaneously the state jurisdiction must be valid under the Due Process Clause of the Fourteenth Amendment. Consequently, such a person must have sufficient ―minimum

[17] U.S. LEXIS 1447.
[18] Amit M. Sachdeva, *International Jurisdiction in Cyber Space: A Comparative Perspective*, CTLR Oxford, Vol. 13, 2007, p. 250.
[19] *Helicopteros Nacionales de Colombia, S.A.* v. *Hall*, 466 US 408 (1984).
[20] Federal Rule of Civil Procedure, Rule 4(k)(1)(A).
[21] Federal Rule of Civil Procedure, Rule 4(k).
[22] Federal Rule of Civil Procedure, Rule 4(k)(2).

contact" with the state, thus the initiation of a suit does not go against ―traditional notions of fair play and substantial justice.[23] The court must decide what contacts are sufficient regarding ―notions of fair play and substantial justice" to use its power. As soon as the threshold of ―minimum contact" is crossed, the US court can assert its jurisdiction.[24] The minimum contact can be discovered by many methods, e.g. through the internet, business transactions, effects of cyber activities, and targets of cyber activities.[25]

The court must be inclined to find all contacts in all circumstances for the test of jurisdiction. This category needs more refinement to include the substantial requirement of personal jurisdiction as described in the *Zippo Case*. According to the Zippo Case, deliberate action is needed, either in the form of transactions between the resident of the forum state and the defendant, or the defendant's conduct must purposely target the resident of the forum state. Therefore, the United States does not apply single jurisdiction for all cases. According to *Bensusan* v. *King*, a mere advertisement on a website does not confer specific jurisdiction since the defendant

―did not contract to sell any goods or services to any citizens of the forum state over the internet site.

Universal jurisdiction

Universal jurisdiction is applied to crimes that are more serious.[26] Universal jurisdiction, compared to territorial jurisdiction, offers a more effective and efficient deterrent. It ―confers on any nation the authority to prosecute alleged international criminals, even when the prosecuting nation has no direct connection what so ever with

[23] T.D. Leitstein "565 A Solution for Personal Jurisdiction on The Internet', *Louisiana Law Review*, 1999. Retrieved from *http://cyber.law.harvard.edu/property00/jurisdiction/Leitstein.html* on 29/05/2017.

[24] Amit M. Sachdeva, International Jurisdiction in Cyber Space: A Comparative Perspective, Vol. 13, CTLR Oxford, 2007, p. 250.

[25] M. O. Rahman, Towards Understanding Personal Jurisdiction in Cyberspace, *International Journal of Law and Management*, Vol. 50, 2008, p. 110.

[26] S. Macedo, *Universal Jurisdiction: National Court and Prosecution of Serious Crime under International Laws*, University of Pennsylvania Press, 2006, p 4.

the offense." Universal jurisdiction was created based on international law, which permits all states to apply their laws to an act —even if it ...occurred outside its territory, even if it has been perpetrated by a non-national, and even if its nationals have not been harmed by it....."[27] It creates a new realm, forcing humankind to extend the traditional and existing rules to it.[28] However, when exercising the principle of universal jurisdiction, due to the competencies existing in it, only a limited number of offences are subject to its application.[29] Moreover, asserting jurisdiction under universal jurisdiction requires two factors: the crime must be serious enough to be hazardous to the international community, and the country which asserts jurisdiction must have the defendant in its custody.[30] Generally, the other forms of jurisdiction require some kind of link among elements of the crime, but the application of universal jurisdiction does not require any such link. The crimes come under international law in two ways: *firstly*, the heinous nature and scale of the offence, which encompass grave breaches of humanitarian law; or *secondly*, because of the inadequacy of legislation by the nations involved, these crimes are committed in territories that are not subject to the authority of any states. Extensions of the universal jurisdiction has been explained under following heads:

***Opinio juris* and state practice**

There are two basic criteria for the application of universal jurisdiction: the treaty regime and customary international law. Universal jurisdiction is prescribed for cyber terrorism as a matter of customary international law, and is based on the elements of customary international law. Two elements of customary international law that are included are *opinio juris* and state practice regarding terrorism. Terrorism has been considered in a number of treaties (state practice), and as mentioned above, numerous

[27] Roslyn Higgins, *Problems and Process: International Law and How We Use It*, United Kingdom, 1995, p. 57.
[28] *Ibid*. p. 57.
[29] Ilias Bantekas and Susan Nash, *International Criminal Law*, 2nd edition, Cavendish Publishing, United States, 2003, p. 156.
[30] Kenneth C. Randall, Universal Jurisdiction under International Law, *Texas Law Review*, Vol. 66, 1998, p. 785.

treaties have recognised various types of terrorism. Although they do not mention cyber terrorism per se, it is accepted that cyber terrorism is generally a form of terrorism, As well as terrorism is considered a heinous crime against humanity (*opinio juris*).[31] Thus, these two elements of customary law i.e. *opinio juris* and state practice are suitable for application against terrorism and subject terrorism to universal jurisdiction. The international community condemns all aspects of terrorism because of their heinous nature, which is also a characteristic the nature of cyber terrorism acts.

State responsibility

Resolutions 1368[32] and 1373[33], adopted by the UN Security Council following 11 September 2001, mandated states to take affirmative steps as a duty under international law to prevent terrorist acts and to cooperate in shouldering this burden. Therefore, countries must attempt to prevent terrorist acts. In other words, state responsibility obliges states to arrest, prosecute or to extradite anyone accused of being associated with a cyber terrorism act. According to state jurisdiction, states must prevent and respond to cyber terrorism acts. Resolution 1373 creates binding international law by containing the word ―decided" which means all United Nations member states are duty bound to implement the Security Council decision. Accordingly all states have a duty to prevent terrorist acts, a duty to prevent territories from harbouring anyone associated with terrorist acts and from being used for committing terrorist acts. States must also adopt proper domestic law to criminalise and punish terrorist acts. Although Resolution 1373 does not specifically address cyber terrorism, but act of cyber terrorism acts being a type of terrorist activity should be covered under the Resolution as well. As soon as an attack is identified as a cyberattack, the duty to respond requires states to provide evidence and

[31] John H. Jackson, "Sovereignty Modern: A New Approach to an Outdated Concept', *The American Journal of International Law*, Vol. 97, 2003, pp. 795-800.

[32] Security Council Resolution passed on 12/09/2001. Accessed from *https://documents-ddsny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement*, on 14/06/2017 at 17:21 hrs.

[33] Security Council Resolution passed on 28/09/2001. Accessed from *https://documents-ddsny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement,* on 14/06/2017 at 17:21 hrs.

to cooperate with criminal investigations and to bring the alleged cyber terrorism perpetrators to justice by either prosecuting or extraditing them.

Treaty law provides a legitimate basis for exercising universal jurisdiction over cyber terrorism. Numerous treaties have been affected on terrorism and as cyber terrorism is a part of traditional terrorism which launches its attack via the internet, such treaties may cover cyber terrorism as well. Good examples of this are the Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes against Persons and Related Extortion, and the International Convention for the Suppression of Terrorist Bombings. Multilateral treaties may conform to customary international law if a large proportion of non-member states follow the provisions of treaties without any legal obligation.[34]

Universal jurisdiction was applied to pirates because they were considered enemies of all mankind such as genocide, piracy etc. Cyber terrorism as a new type of traditional terrorism should be subject to universal jurisdiction, because of the heinous nature of such crimes. The heinousness of cyber terrorism acts is also on par with genocide, crimes against humanity which are subject to universal jurisdiction because they are analogous to piracy in the heinous nature of the crime and their matching the definition of piracy as a ―crime committed more or less indiscriminately against citizens of different nations on the high seas". Thus, international treaties have increasingly mandated universal jurisdiction, even though the *autdedereautjudicare* ('extradite or prosecute') principle has only recently been included in customary international law.[35]

BUDAPEST CONVENTION

As the Budapest Convention on Cybercrime on 23rd Nov. 2004 is the only existing international treaty to fight against cross-border crime and a large number of countries have ratified it as well as recognised the standard jurisdiction approach of the Convention

[34] Roozbeh B.Bakher, Customary International Law in the 21st Century: Old Challenges and New Debates, *European Journal of International Law*, Vol. 21, 2010, p. 173.

[35] Nadya Leila Sadat, Universal Jurisdiction: Myths, Realities, and Prospects: Redefining Universal Jurisdiction, *New England Law Review*, Vol. 35, 2001, p. 245.

to enact their federal and state legislation's jurisdiction over criminal offences committed in cyberspace, it is vital to consider jurisdiction under this Convention.[36] Article 22 of the Convention on Cybercrime deals with jurisdictional issues over offences enumerated in Articles 2-11 of the Convention. It stipulates:

A. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. 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.

B. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

C. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

D. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

E. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate,

[36] C. V. Sanmartin, *Internet Jurisdiction and Applicable Law in Latin America. Towards The Need for Regional Harmonisation in the Field of Cybercrime*, The Octopus Interface, Conference on Cooperation Against Cybercrime, Strasbourg, 2009, p 89.

consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 22 of the Convention on Cybercrime establishes extraterritorial jurisdiction over information technology offences in three aspects: (i) the place where the offense was committed; (ii) which laws should accordingly apply in case of multiple jurisdictions; and (iii) how to solve positive and how to avoid negative jurisdiction conflicts.[37]

Although many treaties exist, none of them provide a binding regulatory jurisdiction. Most of them deal with limited areas and apply at regional level. The most prominent treaty in the field of cybercrime does not encompass cyber terrorism. Thus, since it does not offer personal and territorial jurisdiction covering cyber terrorism, the best thing to do would be to add a protocol specifically relating to cyber terrorism.

CONFLICT OF JURISDICTIONS

In actual fact, conflict of jurisdictions in cyberspace may easily occur. It may occur particularly because the effect of cyber terrorism often takes place in a country or countries other than the country in which the attack originated.[38] A new idea arises here, that since the state has the state responsibility, in order to determine which state has the proper jurisdiction to be take action in the ambit of conflict of jurisdiction, territorial jurisdiction is the most feasible jurisdiction to be prescribed. Due to the cross-border nature of cybercrime, jurisdiction conflicts may easily occur, because, the effect and start of such crime frequently happens in more than one country. Furthermore, as a specific and holistic jurisdiction and method has not been determined for cyber terrorism in cyberspace, the conflict of jurisdictions is not a surprising issue. In fact, universal jurisdiction is offered by international and multilateral treaties. The relevant international treaties encourage their member states to expand jurisdiction over international offences.

[37] Henrico W. K. Asperse, "Jurisdiction in the Cyberspace Convention' in Cybercrime and Jurisdiction: A Global Survey, Bert-Jaap Koops & Susan Brenner (*et al*.), Chapter 2, *Information Technology & Law Series*, T.M.C. Asser Press, The Hague, Vol. 11, 2006.

[38] S. W. Brenner (*et al*.), "Approaches to Cyber Crime', *Journal of High Technology Law*, Vol. IV, 2004, P. 40.

Then such jurisdiction is established with respect to incorporation of municipal law regarding the international offence. As is articulated in Article 5 of the 1984 United Nations Torture Convention, if the alleged offender is located in a state that does not wish to initiate criminal proceedings, it is obliged to extradite the offender to the country which has the closest connection to the offence. Such extradition is based on a bilateral extradition treaty. The extradition process in universal jurisdiction must be based on the legitimacy of the requesting country. In other words, conflicting extradition requests can be decided on the basis of relevant connecting factors. Furthermore, they must not conflict with other agreed rules of international law.[39]

A good example of an international treaty here is the Convention of Cybercrime which states in Article 5 that when the target's victims of an offence are located in several states, several parties assert jurisdiction over the crime. The Convention states that they must consult with each other to determine the appropriate location for prosecution.[40] Some of the aspects of territorial jurisdiction seem appropriate to settle the conflict that arises among jurisdictions. Another conflict which must not be forgotten is the positive conflict that happens mostly in cyberspace cases, particularly cyber terrorism incidents, since the cross-border nature of these lead to it involving a large number of nations. For instance, the ―Love Bug" virus or the ―Blast Worm" qualified many countries to claim jurisdiction on the basis that the effects were taking place on their territories. For e.g., when a Polish citizen uses a computer in the Netherlands to hack a Malaysian computer and the data is transferred via Singapore and the United States, all these states will be able to claim jurisdiction. Thus, in this situation more than one country can claim jurisdiction over a perpetrator based on the same general course of conduct.[41] However, some circumstances may mitigate the ability of claiming jurisdiction, such as lesser

[39] Ilias Bantekas and Susan Nash, *International Criminal Law*, 2nd edn, Cavendish Publishing, United States, 2003, pp. 162-164.

[40] Armando A. Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime'.

[41] The IBA, Report of Task Force on Extraterritorial Jurisdiction, United States, 2009, p. 197.

damage compared to that occurring in other involved countries, and the fact of data merely passing through the territory of a country without causing damage.

Although there are some factors in prioritising a jurisdictional claim to resolve and prevent jurisdictional conflict, such as place of commission of the crime, custody of the perpetrator, the amount of harm, and the nationality (victim's nationality, perpetrator's nationality), conflict still exists in the cyber terrorism and cybercrime situation, since every individual factor has its intrinsic problem.[42]

EXTRADITION: CONCEPTION, EVOLUTION AND DEFINITION

Term extradition has been derived from Latin words— '*ex*' and '*tradium*', meaning thereby 'delivery of an alleged accused or convicted individual to the state where he is accused of a crime by the state, on whose territory he physically present for the time being'. It is the process by which a person charged with or convicted of a crime under the law(s) of one state is returned to the former state for the trial or punishment. Generally, extradition is facilitated by mutual, bilateral or multilateral treaties. It is usual to derive from existing treaties on the subject certain general principles, e.g. that of double criminality, i.e. that the crime involved should be a crime in both/every states concerned[46] and that of specialty, i.e. a person surrendered may be tried and punished only for the offence for which extradition has been sought and granted.[43] In general, offences of a political character have been excluded,[44] but this wouldn't cover terrorist activities having political justification.[45]

---

[42] S. W. Brenner, "Cybercrime Jurisdiction', Vol. 46, *Crime Law Social Change*, 2006, pp. 197- 204. [46] See the decision of the House of Lords in *Government of Denmark* v. *Nielsen* (1984)2 All ER 81; *US Government* v. *McCaffey* (1984)2 All ER 570.

[43] Oppenheim's International Law, p. 961; As in Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 686.

[44] *Ibid*., p. 962.

[45] *McMullen case*, 74 AJIL, 1980, p. 434. Article 1 of the European Convention on the Suppression of Terrorism, 1977, enlists certain offences which aren't to be regarded as political offences or inspired by political motives, an approach which is also adopted in Article 11 of the Convention for the Suppression of Terrorist Bombing, 1997. As in Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 686.

The following rational considerations have conditioned the law and practice as to extradition:

a. The general desire of all states to ensure that serious crimes do not go unpunished. Frequently a state in whose territory criminals have taken refuge cannot prosecute or punish them purely because of some technical rule of criminal law or for lack of jurisdiction. Therefore to close the net round such fugitive offenders, international law applies the maxim, '*aut punire aut dedere'*, ie offenders must be punished by the state of refuge or surrendered to the state which can and will punish them.

b. The state on whose territory- the crime has been committed is best able to try the offender because the evidence is more freely available there, and that state has the greatest interest in the punishment of the offender, and the greatest facilities for ascertaining the truth.[46]

According to the *Starke*, term 'extradition' denotes the process whereby under treaty or upon a basis of reciprocity one state surrenders to another state at its request a person accused or convicted of a criminal offence committed against the laws of the requesting state, such requesting state being competent to try the alleged offender. Requests for extradition are usually made and answered through the diplomatic channel.[47]

Malcolm, in his book[4849], elaborates that, the practice of extradition enables one state to hand over to another state, suspected or convicted criminals who have fled to the territory of the former. It is based upon bilateral treaty law and doesn't exist as an obligation upon states in customary law.

Brownlie has explained that, apart from trial in absentia, an unsatisfactory procedure, states have to dependent on the cooperation of the other states in order to obtain surrender of suspected criminals or convicted criminals who are, or have fled, abroad.

[46] *Starke's International Law*, Oxford University Press, 11th ed., 1994, p. 317.
[47] *Ibid*, p. 317.
[48] Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 53/

Where this cooperation rests on a procedure of request and consent, regulated by certain general principles, the form of international judicial assistance is called extradition.[50] The *Central Bureau of Investigation (CBI)* elucidates that 'extradition may be briefly described as the surrender of an alleged or convicted criminal by one State to another. More precisely, extradition may be defined as the process by which one State upon the request of another surrenders to the latter a person found within its jurisdiction for trial and punishment or, if he has been already convicted, only for punishment, on account of a crime punishable by the laws of the requesting State and committed outside the territory of the requested State.'[51]

Extradition is one of the oldest forms of international cooperation; its roots can be traced to antiquity. Originally designed to seek the return of persons alleged to have committed political offences, the concept has grown and evolved so that it now covers a plethora of criminal offences, and obligations related thereto have been solidified by way of bilateral, regional and multilateral treaties. Although extradition has been used for centuries, the law has not developed to the point where it places a positive obligation on any State to extradite. The obligation to extradite arises only in the presence of a treaty and, even then, there are certain limitations, as shall be shown below, regarding certain offences and classes of persons, who, depending upon the jurisdiction may not be extraditable.

EXTRADITION AS A TOOL OF INTERNATIONAL COOPERATION

With the increasing speed and services of international transport and communications, extradition began to assume prominence in the nineteenth century, although actually extradition as a practice, date from the eighteenth century. Because of the inert attitude of customary international law on the subject, extradition was at first dealt with by bilateral treaties. These treaties, inasmuch as they affected the rights of private citizens, required in their turn alterations to the laws and statutes of the states

[50] Ian Brownlie, *Principles of Public international Law*, 7th Ed., Oxford University Press, 2008, p. 316.
[51] *http://cbi.nic.in/interpol/extradition.php*; retrieved on 14/11/2016 at 11:07 hrs.

which had concluded them. Hence the general principle became established that without some formal authority either by treaty or by statute, fugitive criminals would not be surrendered nor would their surrender be requested. There was at international law neither a duty to surrender, nor a duty not to surrender. For this reason, extradition was called by some writers a matter 'of imperfect obligation'. In the absence of treaty or statute, the grant of extradition depended purely on reciprocity or courtesy.[52]

How extradition is governed is as varied as the States that entertain such an action, as it is usually within a State's domestic laws or its treaties that the rules of procedure and evidence are articulated.[56] The following issues are usually addressed in domestic law, and as such it is instructive to review the legislation of the State from which extradition is being sought, in order to set the tone for the communications that will later be made with the requested State's central authority:

(a) Procedures for arrest, search and seizure and surrender
(b) How an extradition request will be acted upon
(c) What refusal grounds apply and whether refusal is mandatory or discretionary
(d) Which decisions, if any, are taken by the executive and which, if any, by the judiciary
(e) What evidentiary requirements govern that decision-making and to what extent, if any, evidentiary rules exclude relevant material from consideration
(f) Whether persons sought remain in custody pending those decisions and, if not, what conditions are set to ensure that the person does not flee.
(g) Which review and appeal mechanisms apply to which decisions and at what stage(s) of the extradition process
(h) How much time elapses between receipt of an extradition request and the final decision on whether or not to return the person.

[52] Reference should be made to the European Convention on Extradition, 13 December 1957 (Council of Europe) as an illustration of a multilateral extradition treaty. On the necessity of a treaty to confer a

Article 16, paragraph 7, describes the interplay between the Organised Crime Convention and the domestic law of a State as it relates to extradition: Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, *inter alia*, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

Depending upon the domestic legislation of the State, a number of factors may be considered by a requested State when dealing with an extradition matter. The decision to surrender a person to another State is usually the result of a bifurcated system involving the judiciary at the outset of the process and the executive branch during the latter part of the process. Depending on the jurisdiction, the courts may consider a number of diff erent factors in deciding to extradite, among them dual criminality, identity, sufficiency of the supporting evidence and the existence of an extradition treaty.

ESSENTIALS OF EXTRADITION

International law acknowledges that the grant of and procedure regarding extradition are most properly determined by the municipal law, and does not preclude states from legislating so as to refuse the surrender of fugitives by them, if it appears that the request for extradition had been made in order to prosecute the fugitive on account of race, religion, or political opinions, or if the fugitive may be prejudiced thereby upon eventual trial by the courts of the requesting state. There are some differences on the subject of extradition between the different municipal laws, particularly as to the following matters: extraditability of nationals of the state of refuge; evidence of guilt required by the state of refuge; and the relative powers of the executive and judicial organs in the procedure of surrendering the fugitive criminal.

Before an application for extradition is made through the diplomatic channel, two conditions are as a rule required to be satisfied:

i. There must be an extraditable person;
ii. There must be an extradition offence;
iii. Evidentiary test;

iv. Dual criminality;

v. Rule of specialty;

vi. Retroactivity.

We shall discuss each of these conditions.

i. ***Extraditable persons:*** There is uniformity of state practice to the effect that the requesting state may obtain the surrender of its own nationals or nationals of a third state. But many states usually refuse the extradition of their own nationals who have taken refuge in their territory, although as between states who observe absolute reciprocity of treatment in this regard, requests for surrender are sometimes acceded to.

ii. ***Extraditable offence:*** The first precondition that must be looked at by both the requested and requesting State is whether the offence alleged in the extradition request is an offence for which the law allows extradition. The issue of what is an extraditable offence is found in two ways in a treaty: either by the listing method or the penalty method. The listing method means that the treaty lists the offences for which extradition may be allowed. This method is usually found in older treaties and can be problematic, as it requires a degree of accuracy that is difficult for the requesting State to attain. In the penalty method, the extraditable offence is determined by the seriousness of the penalty that may be imposed. In this case, the definition can be more general because the potential length of punishment will be the deciding factor in whether it is an extraditable offence. The Organised Crime Convention recognises both methods in Article 16, paragraph 1.[53]

Certain states, for example, France, extradite only for offences which are subject to a definite minimum penalty, both in the state requesting and in the state requested

[53] Article 16, paragraph 1, of the Convention defines the scope of the obligation to extradite by providing that an extradition request is to be granted, subject to the double criminality requirement, with respect to ―the offences covered by this Convention or in cases where an off ence referred to in article 3, paragraph 1 (a) or (b), involves an organised criminal group and the person who is the subject of the request for extradition is located in the territory of the requested State Party…‖. [59] *Starke's International Law*, Oxford University Press, 11th ed., 1994, p. 319.

to grant extradition. This is also the case in the United Kingdom under the Extradition Act, 1989.[59]

iii. ***Evidentiary tests:*** As mentioned earlier, the evidentiary requirements for an extradition request will be found either in the treaty that is being utilised or within the domestic law of the requested State. There will always be variations in the requirements, based on the legal tradition and legal system of the State and possibly the specific requirements of the treaty, particularly if it is bilateral. Article 16, paragraph 8, of the Convention also seeks to further break down the barriers to extradition by exhorting States to simplify their evidentiary requirements.[54]

Listed below are the three major tests that are used in extradition; it is usually one of these, or a variation of them, that is found in most domestic legislation or treaties:

(a) The —*no evidence*" test requires no actual evidence of the offence that is alleged; instead, a statement of the offence, the applicable penalty, the warrant of arrest for the person and a statement setting out the alleged criminal conduct are required to found a request for extradition in jurisdictions using this test.

(b) The —*probable cause*" evidence test requires sufficient evidence to create reasonable grounds to suspect that the person sought has committed the alleged offence.

(c) The —*prima facie*" evidence test requires actual evidence that must be presented to the authorities that would allow them to form the opinion that the person sought would have been required to stand trial had the alleged conduct of the criminal o ffence occurred in the requested State.

i. ***Dual criminality:*** Dual, or double, criminality is a concept prevalent in the law of extradition, although efforts have been made to limit the difficulties that it had previously posed. When looking at the question of dual criminality with respect to extradition, it is good to keep the following factors in mind:

[54] Article 16, paragraph 8 reads as — States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies. United Nations Convention against Transnational Organised Crime and the Protocols Thereto, United Nations Office on Drugs and Crime, Vienna, 2004.

(a) The focus of dual criminality should be the substantive underlying conduct and not the technical terms or definitions of the crime. Article 43, paragraph 2, of the United Nations Convention against Corruption[55] defnes the conduct-based test as follows:

In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the off ence for which assistance is sought is a criminal offence under the laws of both States Parties.

(b) The laws of the requesting and requested States generally need only be substantially similar as to the harm they seek to prevent and the activity they intend to punish

(c) If the law of one State is broader than the that of the other in scope, so long as the conduct for which extradition is sought could be included in both laws, then it is an extraditable offence

(d) Purely jurisdictional elements of statutes need not be replicated under both systems in order for the conduct to be an extraditable offence.[56]

ii. ***Rule of specialty:*** A further principle sometimes applied is known as the *principle of specialty*, i.e. the requesting state is under a duty not, without the consent of the state of refuge, to try or punish the offender for any other offence than that for which he was extradited. In Great Britain its application is a little uncertain; in *R* v. *Corrigan*[63] the Extradition Act was held to prevail over a Treaty of Extradition with France embodying the specialty principle, and it was ruled that the accused

[55] United Nations, Treaty Series, vol. 2349, No. 42146.

[56] Charles A. Caruso, ―Legal Challenges in Extradition and Suggested Solutions‖, in *Denying Safe Haven to the Corrupt and the Proceeds of Corruption*. Papers Presented at the 4th Master Training Seminar of the ADB/OECD Anti-Corruption Initiative for Asia and the Pacific Kuala Lumpur, Malaysia 28–30 March 2006, p. 58. [63] (1931) 1 KB 527.

there could be tried for an offence for which he was not extradited, but one which was referable to the same facts as alleged in the extradition proceedings.[57] The rule of specialty is designed to ensure that the offence or offences for which the requesting State seeks the return of the suspect to answer pursuant to the extradition request are the only offences for which the suspect will have to answer in the requesting State.

iii. ***Retroactivity:*** The Organised Crime Convention is silent with respect to the question of whether the Convention applies retroactively. The question to be answered is whether the Convention applies to conduct that occurred prior to the entry into force of the Convention in the requested State. It is not clear if any court has yet addressed this issue with respect to the Convention. Several domestic courts, however, have addressed this issue, with respect to the retroactive application of other treaties, and have held that a treaty may be applied retroactively, as an extradition proceeding is not a criminal proceeding.

The above mentioned list of requirements for extradition aren't exhaustive, because with respect to changing international relationship as well as society, some of these may be striked out while some new may be added.

GROUNDS FOR REFUSAL OF AN EXTRADITION REQUEST

Many states will not allow the extradition of nationals to another state,[58] but this is usually in circumstances where the state concerned has wide powers to prosecute nationals for offences committed abroad. Besides this one there are other factors also which are pivotal for the decision to refuse an extradition request. Traditionally there have been a number of principles that can prove to be either an impediment or an outright bar to extradition. These principles or factors, discussed in further detail below, are:

[57] *R* v. *Aubrey-Fletcher, ex parte Ross-Munro* [1968]1 QB 620.

[58] E.g. Article 3 (1) of the French Extradition Law, 1927 and Article 16 of the Basic Law of the Federal Republic of Germany. As in Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 686.

i Non-extradition of nationals ii Concerns over the severity of punishment of the fugitive in the

requesting State iii Human rights issues, with respect to either punishment or the fairness of the trial in the requesting State iv Non-extradition for fiscal offences v The political offences

i. ***The doctrine of non-extradition of nationals*** is found in many States, particularly those with a civil law tradition. Depending on the country, the refusal may be mandatory or discretionary; as always, it is worthwhile to look at the domestic legislation of the requested State to see if there is a possibility that the suspect who is a national of that State can be extradited under its legal system. It should be noted, however, that non-extradition does not necessarily mean non-prosecution. There are no safe havens in the world for many types of crimes, including those contemplated by the Organised Crime Convention. Those States which are parties to the Convention should enact domestic laws pursuant to the Convention that are designed to punish those who are guilty of these offences. The principle of *aut dedere aut judicare* (extradite or prosecute) is a principle that should be explored in cases in which a national cannot be extradited. The Convention recognises this principle in article 16, paragraph 10; however, that paragraph does not go so far as to compel a State to prosecute.

ii. Considerations of the likely ***severity of punishment*** have been a concern with respect to extradition cases. If the domestic law of the requested State contains provisions regarding refusal of extradition on the basis of the potential imposition of the death penalty, the requested State may consider exercising the following options:

(a) Seeking assurances or obtaining necessary information from the requesting State that the death penalty will not be imposed should the suspect be convicted

(b) If legally possible, prosecuting the case in its own jurisdiction, given the commonality of offences in the Organised Crime Convention

(c) Seeking the return of the suspect upon conviction from the requesting State to serve his or her sentence in the requested State's jurisdiction

iii. ***The issue of human rights***, particularly the potential of extradition to lead to torture, is also a concern that has to be considered when engaging in the extradition process. If concerns do arise, States should communicate with one another and seek assurances that this type of prohibited conduct will not occur. If these assurances cannot be given, States should consider having the suspect, if convicted in the requesting State, serve his sentence in the requested State. The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment[59] imposes specific obligations upon signatory parties with respect to the transfer of individuals to other countries. Article 3 of that convention requires that no State party expel, return or extradite a person to another country where —there are substantial grounds for believing that he would be in danger of being subjected to torture." Thus, requested States are required to consider whether grounds exist to believe an individual would be in danger of being subjected to torture.

In the *Soering Case* the United Kingdom intended to extradite a person to the United States for a crime carrying a possible penalty of death. The European Court of Human Rights held that such circumstances, where a fugitive might spend years on 'Death Row' awaiting the result of appeals, would constitute inhuman and degrading treatment contrary to the European Convention on Human Rights, and that extradition was thus inadmissible.[60] Article 16, paragraph 15, of the Convention prohibits the refusal of extradition based upon the fact that the alleged *crime of fiscal nature*. In doing so, the Convention reflects the growing concern that offences with fiscal overtones, such as

[59] United Nations, *Treaty Series*, vol. 1465, No. 24841.

[60] (1989) 11 EHRR 439. The death penalty as such is not contrary to either the European Convention on Human Rights or the International Covenant on Civil and Political Rights, but optional protocols to both instruments allow parties to declare that they will not apply it.

moneylaundering, are major components of transnational organised crime and should therefore not be immune to investigation, extradition and prosecution.[61]

In *R* v. *Governor of Brixton Prison, ex p Kolczynski*[62], the court favoured an even more extended meaning, holding in effect that offences committed in association with a political object (e.g. anti-Communism), or with a view to avoiding political persecution or prosecution for political defaults, are 'political crimes'. In this connection, the question of war crimes gives rise to difficulties; to some extent the issues involved are matters of degree, insofar as a war crime may or may not transcend its political implications.[63] The political offences exception is founded on three basic premises:

(a) The recognition of political dissent

(b) The guarantee of the rights of the accused

(c) The protection of both the requesting and requested States.

The forced disappearance[64] has been declared as a crime against humanity and according to the Convention on the Protection of all Persons from Enforced Disappearance, 2006, such offences are deemed to be included as an extraditable offence in any extradition treaty, while the offence isn't to be regarded as a political offence or as an offence connected with a political offence or as an offence inspired by political motives.

Based upon the above, it can be seen that the premise behind the exception is the balancing of two main competing interests: the recognition of political dissent as a form of protest and the rights inherent in the pursuit of that ideal; and the rights of states to protect themselves from influences that may be bent on harming or destroying them.

---

[61] United Nations Office on Drugs and Crime, Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters, para. 23. Available from *www.unodc.org/pdf/model_treaty_extradition_revised_manual.pdf,* on 11/10/2016 at 11:25 hrs.

[62] [1955] 1 QB 540.

[63] *Re Wilson, ex p the untness T* (1976) 135 CLR 179 (decision of High Court of Australia), and *Re Gross, ex p Treasury Solicitor* (1968) 3 All ER 804.

[64] When a person is secretly abducted or imprisoned by a state or political organisation or by a third party with the authorisation, support, or acquiescence of a state or political organisation, refusing to acknowledge the person's fate and whereabouts, with the intent of placing the victim outside the protection of the law.

Thus, terrorist acts, such as bombing or the financing of terrorism, do not benefit from this protection.[65] The political offences exception is sometimes used as a reason for refusing extradition. It sometimes proves to be problematic, as what constitutes a political offence is poorly defined.[66]

The universal counter-terrorism instruments prohibit States parties from rejecting another State party's extradition request (concerning any offence based on those instruments) on the grounds that it concerns a political offence, an offence connected with a political offence or an offence with political motives; hence, this principle may be applied to the cases of cyber terrorism. The International Convention for the Suppression of Terrorist Bombings[74] explicitly rejects the political offence exception for the offences defined in the Convention. All subsequent conventions and protocols against terrorism contain the same provision: None of the offences set forth in Article 2 shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence or as an o ffence connected with a political offence or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an off ence may not be refused on the sole ground that it concerns a political offence or an off ence connected with a political offence or an offence inspired by political motives.[67]
Security Council resolution 1373 (2001) validated this approach by extending the exclusion of the political offence exception to acts of terrorism in general. In paragraph 3 (g) of that resolution, the Council called upon States to —ensure ... that claims of political motivation are not recognised as grounds for refusing requests for the extradition of alleged terrorists".

EMERGING CONCEPT OF MUTUAL LEGAL ASSISTANCE

[65] Article 11 of the International Convention for the Suppression of Terrorist Bombings (United Nations, *Treaty Series*, Vol. 2149, No. 37517); and article 14 of the International Convention for the Suppression of the Financing of Terrorism (United Nations, *Treaty Series*, vol. 2178, No. 38349).
[66] Schmid, —Legal Problems in Mutual Legal Assistance from a Swiss Perspective‖, p. 48. [74] United Nations, *Treaty Series*, vol. 2149, No. 37517.
[67] United Nations, *Treaty Series*, vol. 2149, No. 37517, Art. 11.

Mutual Legal Assistance (MLA) is an agreement, usually by treaty and sometimes by the virtue of reciprocity, between two or more countries to provide assistance to each other on criminal legal matters, for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal. Modern states have developed this mechanism for requesting and obtaining evidence criminal investigation and prosecutions.[68] The MLA developed from the comity-based system of letter rogatory[69], though it is now become more common for the states to make requests directly to the designated central authority within each state. The types of assistance that can be provided through MLATs traditionally include: service of documents; search and seizure; restraint and confiscation of proceeds of crime; provision of telephone intercept material; and the facilitation of taking of evidence from witnesses. The most resilient way of obtaining data is, however, by invoking MLAT. The MLA process is determined by a combination of domestic law and bilateral and multilateral treaties on international crime. MLA is resilient because it is the only process that ties together the laws of both receiving and requesting country, making it legally robust at all stages. However, the MLA process is long. It requires an administrative legal process in each country and duplicate checking of paperwork.

Article 25 of the Budapest Convention provides for the mutual legal assistance as, —

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences

[68] The 2006 extradition treaty between the Government of Estonia and the Government of the United States and the Council of Europe's Convention on Cybercrime by whose virtue three persons were extradited by Estonia to the United States.

[69] The term letters rogatory denotes a formal request from a court in which an action is pending, to a foreign court to perform some judicial act. Examples are requests for the taking of evidence, the serving of a summons, subpoena, or other legal notice, or the execution of a civil judgment. Letters rogatory are requests from courts in one country to the judiciary of a foreign country requesting the performance of an act which, if done without the sanction of the foreign court, could constitute a violation of that country's sovereignty. Letters rogatory may be used in countries where multilateral or bilateral treaties on judicial assistance are not in force to affect service of process or to obtain evidence if permitted by the laws of the foreign country. *See also* Section 166B, Code of Criminal Procedure, 1973.

related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27-35.

PRINCIPLES OF MUTUAL LEGAL ASSISTANCE

To obtain evidence, judges and prosecutors must rely on the goodwill of foreign states even in the presence of international obligations stated in treaties and agreements.[70] No matter how involved the treaties or agreements between two States are, mutual legal assistance is still a matter of asking another state for help. Mutual legal assistance is meant to allow for a wide range of assistance between States in the production of evidence. Article 18, paragraphs 1 and 2, of the Organised Crime Convention speak of States parties affording ―one another the widest measure of mutual legal assistance" and mutual legal assistance being ―afforded to the fullest extent possible", but these actions can only take place when the request itself is communicated effectively and ongoing communication takes place during its execution.

Mutual legal assistance in criminal matters is a process by which States seek and provide assistance in gathering evidence for use in criminal cases. Extradition is the formal process whereby a State requests the enforced return of a person accused or convicted of a crime to stand trial or serve a sentence in the requesting State. The basis for request for mutual legal assistance or extradition usually made under either a treaty or under domestic law or by way of the principle of reciprocity. Following conditions are to be observed before extending mutual legal assistance in the case of cyber terrorism:

1. ***Sufficiency of evidence:*** In order for a successful mutual legal assistance request to be prepared, there must be sufficient evidence to make that request. The amount of evidence required is dictated partly by the legislation of the requested State and

[70] Rabatel ―Legal challenges in mutual legal assistance‖, p. 38. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 88, p. 65.

partly by the nature of the assistance sought. Generally, the more coercive the means of obtaining the evidence, the more involved and complex the evidentiary requirements become. For example, the interviewing of a witness who provides a statement to the police will require less evidence than a mutual legal assistance application that seeks the conducting of a search of a person's business or home. The evidentiary requirements to obtain the same type of assistance in different States will vary greatly, depending on treaty requirements, domestic legislation and the legal systems of the States involved.

2. ***Double criminality:*** Dual or double criminality is a legal principle that requires that the conduct of the person who, in this case, is the subject of a mutual legal assistance request be conduct that can be viewed as a criminal offence in both the requesting and the requested State. It is a concept that tends to play a larger role in the law pertaining to extradition; however, it can be found from time to time in the law pertaining to mutual legal assistance. It can range from not being required at all, to being required for certain coercive acts of mutual legal assistance, to being required for any type of mutual legal assistance.[71] All of this will be dependent upon the domestic legislation of the requested State, and drafters of a mutual legal assistance request should keep this in mind when drafting their request.[72] It should be emphasised that the test for dual criminality is whether the conduct that is the subject of the mutual legal assistance request is criminal in both States, not whether

[71] Prost, ―Practical solutions to legal obstacles in mutual legal assistance‖, in *Denying Safe Haven*, p. 32. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 93, p. 69.

[72] ―For this reason, it is important to describe the underlying crime very clearly, so that the foreign authorities can identify a similar offense in its own legal system. For example, the French offense of *abus de biens sociaux*, or the misuse of company property, needs to be explained in a manner that allows the foreign authorities to determine whether the conduct amounts to breach of trust or embezzlement in their jurisdiction. A clear description of the criminal conduct also has the advantage of preventing misunderstandings about the rule of "*Non bis in idem*' (double jeopardy).‖ (Rabatel, ―Legal challenges in mutual legal assistance‖ in *Denying Safe Haven*, p. 40). Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 94, p. 69.

the conduct is punishable as the same offence in each State.[73] ***iii. Limits on transmission or use of information obtained by mutual legal assistance:*** Article 18, paragraph 19, of the Organised Crime Convention enshrines the principle of limiting the use of information gathered as a result of the mutual legal assistance request to the investigation, proceeding or prosecution that is the subject matter of the request unless permission is granted to use it in other matters. Information that has been gained that is exculpatory in nature may be disclosed to an accused. If this action is to be taken, —the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

GROUNDS FOR REFUSAL OF A MUTUAL LEGAL ASSISTANCE REQUEST

Prayer of a nation for mutual legal assistance in the case of cyber terrorism may be refused on following grounds:

i. ***National or public interest:*** The principle of national or public interest is a broad concept that covers a multitude of aspects that a State may wish to protect. Although not commonly used, it can usually be applied in cases with national security overtones.[74] What practitioners may see in this day and age is a situation in which a number of different agencies—some law enforcement and while some intelligence—are looking at the same target for a variety of reasons.[75] These types of scenarios may be more prevalent than initially suspected, and this principle may

[73] Prost, —Practical solutions to legal obstacles in mutual legal assistance‖, in *Denying Safe Haven*, p. 33. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 95, p. 69.

[74] Prost, —Practical solutions to legal obstacles in mutual legal assistance‖, p. 34. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 96, p. 70.

[75] McMafa Glenny, *A Journey Trough the Global Criminal Underworld*, pp. 110-111. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 97, p. 70.

be used more frequently in the future. Article 18, paragraph 21(b)[76] of the Convention lists this as one of the grounds on which mutual legal assistance may be refused. The judgment of the International Court of Justice dated 4 June 2008 in the case of *Certain Questions of Mutual Assistance in Criminal Matters* (*Djibouti* v. *France*)[77] is instructive, as it enshrines the principle that States have the discretion to refuse mutual legal assistance in certain cases but that the underlying premise is to provide assistance to the fullest extent and only refuse a request in good faith and within a limited category of permitted exceptions.

ii. **Severity of punishment:** More recently, considerations of the likely severity of punishment have arisen in mutual legal assistance cases. This principle has been concerned with respect to extradition cases, but it has been seen in mutual legal assistance cases as well. There are treaties and laws of States that include provisions for the refusal of mutual legal assistance in cases in which the investigation may lead to charges that may result in the imposition of the death penalty or cruel, inhuman, degrading punishment or torture. The challenge for a requested State is that there could be little to indicate that this would be the likely outcome of an investigation, particularly if the investigation is in its early stages.

iii. **Political offences:** As like in the case of extradition, the political offences exception is a potential ground for refusal of mutual legal assistance. The law and constituent elements that make up this exception are the same as those articulated for the extradition. The same caveats exist with respect to mutual legal assistance requests as for extradition, and efforts should be made to look behind what is being alleged as the crime in the mutual legal assistance request to see if it is indeed a political o

[76] Art. 18, *Para 21 (b) —If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.* United Nations Convention against Transnational Organised Crime and the Protocols Thereto, United Nations Office on Drugs and Crime, Vienna, 2004.

[77] *Certain Questions of Mutual Assistance in Criminal Matters (Djibouti* v. *France), Judgment,* I.C.J. Reports 2008, p. 177. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 98, p. 70.

ffence in and of itself or if the charges shield what is essentially a request that is political in nature.

iv. **Human rights considerations:** Human rights considerations are an important component in preparing an outgoing mutual legal assistance request and taking action on an incoming one. The following aspects of human rights will have to be looked at in relation to mutual legal assistance matters:

(a) The right to liberty and security of the person[78]

(b) The right not to be subject to torture or cruel, inhumane or degrading punishment[79]

(c) The right to equality before the law[80]

(d) The right to a fair and public hearing[81]

(e) The right to counsel and interpreters[90]

(f) The right to be presumed innocent[82]

(g) The right not to be held guilty of offences retrospectively or to have retrospective penalties imposed[83]

(h) The right to not be compelled to incriminate himself[84]

v. **Double jeopardy:** Double jeopardy is a principle that can sometimes prove problematic when dealing with issues of mutual legal assistance. Different States have different definitions of what constitutes double jeopardy in treaties to which they are party and in their domestic legislation. Various definitions take into account the following:

(i) Has the person been punished for the crime in the requested and/or requested State?

(j) Has the person been punished for the crime in a third State?

(k) Sometimes the question is not whether the person has been punished but whether the person has been (a) tried, (b) convicted or (c) acquitted?

---

[78] Universal Declaration of Human Rights, Art. 3.
[79] *Ibid*., Art. 5.
[80] *Ibid*., Art. 7.
[81] International Covenant on Civil and Political Rights, art. 14, para. 1
[90] *Ibid.*, Art. 14, para. 3.
[82] Universal Declaration of Human Rights, art. 11, para. 1.
[83] *Ibid*., Art. 11, Para. 2.
[84] International Covenant on Civil and Political Rights, Article 14, para. 3 *(g)*.

Article 25, para 4 of the Budapest Convention provides for the refusal by parties for the mutual legal assistance, as—

Except as otherwise specifically provided in Articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

CONCLUSION

Jurisdiction seems to be the most problematic issue in the fight against cybercrime and cyber terrorism. The transnational nature of cyber terrorism leads to jurisdictional complexity, thereby investigation and prosecution is difficult procedures. Lack of harmonisation in legislating among countries leads to difficulty in investigation and prosecution of cyber terrorism offences. Although many steps have been taken to combat the menace of cyber terrorism, from legal to technical steps, these attempts are not sufficient to prevent cyber terrorism. It appears that greater international cooperation is required. The fact that cyber attacks can come from anywhere in the world makes investigation, producing evidence and taking the offenders to court an immense task that can only be achieved through international cooperation creating bilateral and multilateral treaty or conventions. There should be international coordination as well as cooperation against cyber terrorism in order to create global cyber deterrence. Therefore, it seems that the best feasible solution is providing a treaty (or convention) to regulate particular transactions to uniform international standards.

The best means for the prosecution of cyber terrorism under universal jurisdiction is to create a multilateral criminal law convention that will oblige member states to prosecute and extradite offenders through the '*autdedereautjudicare*' principle established through the treaty and applicable to state parties to the convention. If no extradition treaty or other legal arrangements exist then investigation and prosecution efforts will be

handicapped. Even if an extradition treaty exists, it can be complicated for a number of reasons. For instance, different legal traditions and legal systems require different procedures and requirements for obtaining evidence during an investigation and using that same type of evidence at trial. Another obstacle to investigations is the disparity that exists between the cybercrime laws of different nations. So in such cases MLAT is viable, which provides for the cooperation in the fields of exchange of information about cyber terrorists and evidence sharing.

Bibliography

A. Bianchi, *Enforcing International Law Norms Against Terrorism*, 1st edn., Hart Publishing, United Kingdom, 2004, pp. 474-479.

A. Manolopoulos, "Raising Cyber Borders: The Interaction between Law and Technology', *International Journal of Law and Information Technology*, Vol. 11(1), 2003, pp. 41-44.

Amit M. Sachdeva, *International Jurisdiction in Cyber Space: A Comparative Perspective*, CTLR Oxford, Vol. 13, 2007, p. 250.

Amit M. Sachdeva, International Jurisdiction in Cyber Space: A Comparative Perspective, Vol. 13, CTLR Oxford, 2007, p. 250.

Armando A. Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime'. The IBA, Report of Task Force on Extraterritorial Jurisdiction, United States, 2009, p. 197.

C. V. Sanmartin, *Internet Jurisdiction and Applicable Law in Latin America. Towards The Need for Regional Harmonisation in the Field of Cybercrime*, The Octopus Interface, Conference on Cooperation Against Cybercrime, Strasbourg, 2009, p 89.

Charles A. Caruso, ―Legal Challenges in Extradition and Suggested Solutions‖, in *Denying Safe Haven to the Corrupt and the Proceeds of Corruption*. Papers Presented at the 4th Master Training Seminar of the ADB/OECD Anti-Corruption Initiative for Asia and the Pacific Kuala Lumpur, Malaysia 28–30 March 2006, p. 58.

Henrico W. K. Asperse, "Jurisdiction in the Cyberspace Convention' in Cybercrime and Jurisdiction: A Global Survey, Bert-Jaap Koops & Susan Brenner (*et al*.), Chapter 2, *Information Technology & Law Series*, T.M.C. Asser Press, The Hague, Vol. 11, 2006.

I. Brownlie, *Principles of Public International Law*, 6th edn., Oxford University Press, 2003.

Ian Brownlie, *Principles of Public International Law*, 5th ed., Oxford, University Press, 2002.

Ian Brownlie, *Principles of Public international Law*, 7th Ed., Oxford University Press, 2008, p. 316.

Ilias Bantekas and Susan Nash, *International Criminal Law*, 2nd edition, Cavendish Publishing, United States, 2003, p. 156.

Ilias Bantekas and Susan Nash, *International Criminal Law*, 2nd edn, Cavendish Publishing, United States, 2003, pp. 162-164.

Jack. L. Goldsmith *The Internet and the Abiding Significance of Territorial Sovereignty*, *International Journal of Global Legal Studies*, Vol. 5, 1998, p. 475.

John H. Jackson, "Sovereignty Modern: A New Approach to an Outdated Concept', *The American Journal of International Law*, Vol. 97, 2003, pp. 795-800.

Kenneth C. Randall, Universal Jurisdiction under International Law, *Texas Law Review*, Vol. 66, 1998, p. 785.

L. Grosswald, "Cyber Attack Attribution under Article 51 of the U.N. Charter', *Brooklyn Journal of International Law,* Vol. 36, 2011, p. 1151.

M. O. Rahman, Towards Understanding Personal Jurisdiction in Cyberspace, *International Journal of Law and Management*, Vol. 50, 2008, p. 110.

Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 686.

Malcolm N. Shaw, *International Law*, Cambridge University Press, 1st South Aisan Edition, 2011, p. 53.

McMafa Glenny, *A Journey Trough the Global Criminal Underworld*, pp. 110-111. Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012.

Nadya Leila Sadat, Universal Jurisdiction: Myths, Realities, and Prospects: Redefining Universal Jurisdiction, *New England Law Review*, Vol. 35, 2001, p. 245.

Pardis Moslemzadeh Tehrani and Nazura Abdul Manap, A Rational Jurisdiction for Cyber Terrorism, *Computer Law & Security Review*, Vol. 29, 2013, pp. 689—701.

Rabatel, ―Legal challenges in mutual legal assistance‖ in *Denying Safe Haven*, p. 40). Cited in Manual on Mutual Legal Assistance and Extradition, United Nations Office on Drugs and Crime, Vienna, United Nations, New York, 2012, footnote 94, p. 69.

Roozbeh B.Bakher, Customary International Law in the 21st Century: Old Challenges and New Debates, *European Journal of International Law*, Vol. 21, 2010, p. 173.

Roslyn Higgins, *Problems and Process: International Law and How We Use It*, United Kingdom, 1995, p. 57.

S. Macedo, *Universal Jurisdiction: National Court and Prosecution of Serious Crime under International Laws*, University of Pennsylvania Press, 2006, p 4.

S. W. Brenner (*et al*.), "Approaches to Cyber Crime', *Journal of High Technology Law*, Vol. IV, 2004, P. 40.

S. W. Brenner, "Cybercrime Jurisdiction', Vol. 46, *Crime Law Social Change*, 2006, pp. 197-204.

Schmid, Legal Problems in Mutual Legal Assistance from a Swiss Perspective, United Nations, *Treaty Series*, vol. 2149, No. 37517.

Starke's International Law, Oxford University Press, 11th ed., 1994, p. 317.

T.D. Leitstein "565 A Solution for Personal Jurisdiction on The Internet', *Louisiana Law Review*, 1999. Retrieved from *http://cyber.law.harvard.edu/property00/jurisdiction/Leitstein.html* on 29/05/2017.

V. Lowe, *Jurisdiction in International Law,* Malcolm D. Evans (ed.), 2nd edn, United Kingdom, 2006.

ValerieSedallian, Commentaire de l'affaire Yahoo (1), Revue du Droit des technologies de l'information, 24/20/00, at paragraph 20, retrieved from *http://www.juriscom.net* on 29/05/2011.