ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

"A MIRAGE OF ESTABLISHING UNIVERSAL CYBER JURISDICTION"

Authored By: Laxmi Sagar PR
Law Student,
School of Law, CHRIST(Deemed to be University)
Email ID: laxmi.sagar@law.christuniversity.in

Co- Author: Tarun KM

ABSTRACT

Cyberterrorism and other terrible cyber-crimes represent the greatest danger to national and international security since the invention of mass destruction weapons. Taking into account all the concerns and hypotheses discussed, the employment of universal jurisdiction to combat cybercrime appears to be an effective and feasible strategy. Granted, the principle cannot be applied to all forms of cybercrime, but crimes such as the distribution of child pornography, extortion, the leaking and hacking of confidential State documents, cyber terrorism, etc., can be combated through the application of the Universality principle, as there is international consensus on the appropriate sanction for these offences. Due to the nature of the internet, it would be incredibly difficult to pursue such offenses. Brenner, one of the most renowned cybercrime experts, states in her 2014 book "Cyber Threats and Decline of the Nation State"[1] that cybercriminals utilize jurisdiction of law as a barrier to get away with their crimes.

In this paper, the research method used in this study is of a doctrinal nature and is based on the critical evaluation and assessment of numerous legal statutes, as well as a detailed discussion of the decisions of various national courts. Through this study, the researcher attempts to identify the jurisdictional concerns raised by the transnational nature of cybercrime and to propose recommendations.The States, Business sector, and international organizations have made considerable efforts to enhance international collaboration, but much more must be

[1] Brenner, SW. (2014) *Cyberthreats and the decline of the nation-state.* Milton Park, Abingdon, Oxon: Routledge.

ISSN: 2582-6433

done. However, when taking action, it must be noted that, due to the inherent fragility of the Internet's architecture, these additional measures will not totally prevent cyberterrorism. Consequently, international cooperation and international norms must be strengthened as part of a tiered strategy to Cyberterrorism.

Keywords: Cyber Terrorism, Universal jurisdiction, Universality Principle, International Norms.

1. INTRODUCTION

In today's scenario, the majority of human activities rely increasingly on technology, particularly Information Technology. Humans are superior to all other forms of life on earth because they possess the ability to think, evaluate, and act accordingly. Humans have the ability to adapt to any situation, and the concept of 'survival of the fittest' has motivated people to pursue their goals both legally and illegally. In the twenty-first century, power is measured in terms of one's information and expertise. It is believed that information technology has had the greatest impact on the evolution of those who possess knowledge and are in a position of power. Access to knowledge is no longer hindered by obstacles such as distance and cost as a result of the information revolution's fundamental alteration of society.

Anyone in the world with access to a computer and the internet can land in cyberspace and communicate with people even in the farthest reaches of the planet; he or she can collect information from anywhere or disseminate information; he or she can search for companionship or entertainment around the world or offer a variety of goods and services. Due to the inherent characteristics of the technology, nations are unable to effectively govern Internet transactions that originate or terminate within their borders. While nations may endeavor to enforce their different laws within the physical, geographical, and political boundaries outlined on a map, a borderless cyber world governed by ever-evolving technology presents numerous obstacles. Even while it was once believed that one could determine the actual location of the computer from which the transaction originated and the computer to which it was sent, technology can circumvent or "mask" this information. Consequently, the application and efficacy of our existing laws must be continually evaluated so that we can face the hazards of the present with confidence as questions of jurisdiction and sovereignty become increasingly pertinent.

ISSN: 2582-6433

Therefore, the author advocates applying the Universality Principle to address the challenges that occur while defining Jurisdiction. In the case of cyber-crimes, jurisdiction refers to judicial, legislative, and administrative competence. Although jurisdiction is a component of sovereignty, it is not coextensive with sovereignty. Even though a country possesses unbroken internal and external sovereignty, that does not mean it has unrestricted authority over all matters. Current international law restricts the ability of states to exercise jurisdiction. This makes international cooperation a precondition for addressing the Jurisdiction issue. However, international cooperation must be supported by the law; hence, the principle of universal jurisdiction in relation to specific cybercrimes and cyber terrorist activities can be an efficient means of ensuring cooperation for the same.

2. Legal Implications of Cyberspace

Cyber space may alternatively be referred to as a parallel universe developed and sustained by the world's computers and communication networks. Through its countless, unblinking eyes, distant places and faces, whether real or unreal, present or long-gone, can be conjured from the massive data banks that form the culture's accumulated treasure. Although there is an obvious place for industry-imposed regulation as well as self-regulation, this strategy leaves unrepresented the overwhelming majority of individuals who interact with Internet Service Providers and the growing number of businesses selling goods and services online. However, this does not imply that cyberspace is now unregulated. In fact, one of the difficulties involved in evaluating the issue is the excess of regulation. Laws pertaining to broadcasting, the media, data protection, evidence, contract, tort, defamation, intellectual property, etc., as well as civil and criminal law requirements, all play a role. In fact, depending on the nature of their actions, the vast majority of cyberspace's residents may conceivably fall under the jurisdiction of almost the whole global legal system.

Theory and practice diverge significantly, and the difficulty of devising effective enforcement mechanisms is significantly greater than that of discovering relevant legal provisions. In its 1988 "Green Paper on Copyright and the Challenges of Technology," the commission said that "these new technologies have resulted in the de facto eradication of national borders and increasingly render the territorial application of national copyright law outdated." Such arguments apply equally to other areas of the law, and it is necessary to take into account the awkward relationship between terrestrial limits and the jurisdictional claims

ISSN: 2582-6433

of the courts of a particular country and the operation of global communication networks such as the internet.[2]

Numerous Internet users believed that "the Internet cannot be regulated." There is a truism that "bit by bit," meaning that no bit can be treated differently from any other bit, and hence attempts to control are doomed to fail. Both claims are the work of techno-determinists. But both are incorrect, even from a technological standpoint: a bit is a bit with a particular probability, which may be altered. A bit is a bit with a particular priority, which can be altered. The second fallacy is the notion that the Internet is purely electrical, which is in fact difficult to manage. However, communications involve not just signals but also people and institutions. Senders, recipients, and intermediaries are alive, breathing individuals who reside in real space, or legally formed institutions with physical domiciles and hardware. The law has the ability to instruct them. It may be possible to circumvent this law, but the same holds true for tax restrictions. This does not prove that a law is inefficient or undesirable, only because it cannot completely prohibit a particular action.

Similarly, content-based regulation is near impossible. Content rules depend on values which are different in different societies. Major examples are sexual and political expressions. If an international agreement is a compromise, neither country will be happy[3]. For this and many other reasons, if international arrangements are unstable, the primary regulatory action will have to be taken by a country, not by international arrangements. What tools will a country then use? The answer is: the ones that affect these factors that are less mobile than electronic bits-people and physical assets. This means that the country will regulate static and physical elements ‘rather than mobile or intangible ones, such as content, information, and transactions. If one cannot grab the bits, grab the user or their non-mobile assets.

3. The Difficulties in Combating Cybercrime, with an Emphasis on Jurisdictional Issues

It has been said that there are three factors necessary for the commission of crime: a supply of motivated offenders, the availability of suitable opportunities and the absence of

[2] Dr. Amita Verma ,”Cybercrimes and Law”, central law publication, first edition,2009, page-31
[3] Eli Noam, Columbia University; “Regulating Cyber Space”, November 1997: retrieved June 29, 2016

ISSN: 2582-6433

capable guardians.[4] On all three counts the digital environment provides fertile rounds for offending. The growing popularity of digital networks however, comes out at a cost. As the business and societies in general increasingly rely on computers and internet based networking, cybercrime and digital incidents have increased around the world.[5] These attacks generally classified as any crime that downloading pornographic images from internet, virus attacks, E-mail stalking and creating websites that promotes racial hatred.[6]

Technology has both facilitated and impeded the investigation of crime, particularly crimes involving computing of crime and communication technologies or what is described as cybercrime. On the one hand, computers have enabled vast amounts of data to be searched and analyzed quickly and permitted documents and files to be scanned and transmitted across the globe in seconds. On the other hand, the sheer quantity of information creates considerable problems for investigators who sometimes have to examine gigabytes of data and break encryption codes before the material they are interested in can be discovered.[7] Adding fuel to the fire, the trans-border nature of cybercrime has created jurisdictional problems for law enforcement agencies and adjudicators.

The worldwide cybercrime landscape has altered considerably over the past few years, with cybercriminals deploying more sophisticated technologies and having a higher understanding of cyber security. Until recently, attacks were predominantly the work of computer whizzes demonstrating their skills. These attacks, which were infrequently malicious, have gradually transformed into cybercrime syndicates to steal money through unlawful cyber channels.

"With continually expanding information infrastructure, with numerous instances of international hacking, and with growing possibility of increased global espionage, it is important that the countries have jurisdiction over international computer crime cases"[8] The worldwide nature of digital crime renders national solutions insufficient. Oftentimes, the

[4] L.Cohen and M.Felson, 'Social Change and Crime Rate Trends : A Routine Activity Approach' (1979) 44, American Sociological Review 588,589.
[5] It is a time for countries talking about arms control on internet, Economist, July 1, 2010 4
[6] The world wide crime web. BBC news
[7] Dr. Russel G. Smithy,Investigating Cyber Crime: Barriers and Solution, Pacific Rim Fraud Conference,2003
[8] Cybercrime and Intellectual Property section of the National Informational Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice)

ISSN: 2582-6433

criminals' names and the location and scope of the incursion are first unknown. It is possible to access or destroy computer systems from anywhere in the globe, resulting in significant jurisdictional difficulties.

Cybercrime is difficult to combat because of the fact that criminal law is still a matter of national jurisdiction. The issue of sovereignty arises: to what extent can a nation assert jurisdiction over foreign evidence, foreign nationals, and foreign land, and which nation has the legal grounds to prosecute suspects and convict the perpetrator? And if more than one country has jurisdiction, which will have precedence and to what extent can claim extraterritorial procedural jurisdiction, i.e. the authority to probe on the territory of other countries.

Cyber jurisdiction is not at all simple. Several nations lack explicit legislation in this area. They depend solely on conventional jurisdictional provisions to determine whether or not they have jurisdiction. However, these jurisdictional provisions assert territorial jurisdiction. But when exactly can cybercrime or cyber investigation be recognised to occur on a territory when it fundamentally consists of material bits and bytes that traverse the world's internet cables? This prompted states to establish their own strategies. Some nations explored rather unorthodox ways of prosecution and enforcement to circumvent jurisdictional obstacles when confronted with international cybercrime.

In the infamous case of Russian hackers Alexey Ivonov and Vasiliy Gorskov, who were accused of extorting money from many U.S. corporations, the FBI employed a novel approach. In November of 2000, the federal agents, posing as businessmen to conceal their true identities, convinced the two Russian hackers to come to Seattle by offering them a job interview with a network security company. The agents then requested that Ivonov and Gorskov demonstrate their abilities on PCs easily infected with malware, after which they compromised the passwords Ivonov and Gorskov used to access their own computers. Later, the agent accessed the computers of Russian hackers, copied their contents to preserve evidence, and filed criminal charges based on this evidence.[9]

[9] Brenner .W. Susan,Bert-Jaap Koops " Approaches to cybercrime jurisdiction" Journal of High Technology Law 2004, p, (21-22)

ISSN: 2582-6433

Several African governments have not yet criminalized cybercrime, while those states that have criminalized cybercrime lack the means to track down suspects. When major cross-border crimes occur, it is feasible that numerous governments will be interested in prosecuting, but it is also possible that no particular country will assert jurisdiction due to the potential of a claim of primacy jurisdiction by another country that has suffered greater damage.[10]

Some countries that do have cybercrime jurisdiction rules have such a broad statute that they may conceivably assert jurisdiction over cybercrimes committed anywhere. Such provisions are not grounded in reality; countries must be able to differentiate between asserting and exercising jurisdiction. The problem stated above illustrates the complications of cybercrime jurisdiction. Existing conventional ideas are insufficient to combat cybercrime, and if they are applied, their international relations are likely to suffer.

4. ISSUES IN CYBER EXTRACTION

Extradition is frequently proposed as a solution to the majority of jurisdictional issues in international law. In this section, the researcher will attempt to demonstrate if extradition is capable of resolving all such issues or whether this is not the case. According to Starke, "extradition" refers to the process by which, pursuant to a treaty or on the basis of reciprocity, one state surrenders to another state at its request a person accused of committing a crime against the laws of the requesting state, with the requesting state having jurisdiction to try the alleged offender."[11] "Extradition, according to Oppenheim, is the delivery of an accused or convicted individual to the state on whose territory he is said to have committed or been convicted of a crime, by the state on whose territory the alleged criminal being is currently located."[12] The 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 criminal offense committed against the laws of the requesting state, such requesting state being competent to try the alleged offender.[13]

[10] Susan. W. Brenner and Bert Japp Koops "cybercrime and jurisdiction"
[11] J.G. Starke, Introduction to International Law, Tenth Edition (1989) p. 352
[12] L.Oppenheim, International law, Vol.I, Eighth Edition, p.696
[13] Starke.J.G. 'Public International Law

ISSN: 2582-6433

5. Legal Framework in India

The Indian Penal Code of 1860, which regulates criminal offenses, establishes the core jurisdictional concept that Indian courts have the authority to hear cases involving crimes committed in India. Section 3 of the Act[14] states, "Any person liable under any Indian law to be tried for an offense committed beyond India must be dealt with in accordance with the provisions of this Code for any act performed beyond India in the same manner as if such act had been committed within India." Section 3 allows for the extraterritorial application of the code if certain conditions are fulfilled. A major element of the rule is the phrase "any person responsible under any Indian law." This clause only applies where an Indian law specifies that an act done outside India may be prosecuted in India under that law. Thus, for Section 3 of the Indian Penal Code to apply, a person must be culpable under the Act. Similarly, Section 4 of the Act pertains to the expansion of the Criminal Code to extraterritorial offenses

.Procedure-wise, the jurisdictional grounds for crimes are outlined in the Code of Criminal Procedure, 1973. However, the application of the CPC to crimes committed outside of India is quite limited. Thus, it is clear from Section 4 that the provisions of the Criminal Procedure Code apply whenever an offense under the Indian Penal Code or any other legislation is being examined, probed, tried, or otherwise dealt with. The jurisdiction under Sec. 4 is comprehensive to the extent that no valid machinery is set up under any Act for the trial of any particular case, the jurisdiction of the ordinary criminal court cannot be held to have been excluded.[15] Section 188 relates only to procedure and does not constitute a substantive offense.[16] It is the counterpart of Section 4 of the Indian Penal Code in terms of procedure.[17]

6. ISSUES IN IMPLEMENTING UNIVERSAL PRINCIPALITY

One of the primary obstacles in combating cybercrime is defining it. No internationally recognized legal definition exists, though there are functional definitions that focus on general offense categories.[18] Cybercrime is, therefore, most accurately defined as crimes that are

[14] Section 3, India Penal Code, 1860.
[15] Bhim Sen vs. State of UP, AIR 1955 SC 435.
[16] Narayan MudlagiriMahale vs. Emperor, AIR 1935 Bom 437.
[17] Ibid.
[18] Nicholas W. Cade. An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court

ISSN: 2582-6433

perpetrated over the Internet and that generally fall into two categories: first, those that target computers and information stored on computers, and second, those that use a computer to facilitate another crime.[19] When a cybercriminal targets a computer (or, increasingly, a house that is vandalized. someone's mobile device), the computer may be attacked in ways similar to those of many other traditional crimes, similar to a person who is assaulted while strolling along the street or whose house is vandalized. Alternatively, the computer may be a victim to Internet-era crimes. There are numerous offenses that come under the second category, albeit the common computer user may not be aware of their distinctions. The majority of these offenses involve the use of malicious software.[20]

Viruses, probably the most well-known forms of harmful software (also referred to as "malware"), are programmes that change other computer programmes and can travel from one computer to another whenever a file is transmitted between them, whether via the Internet or a traditional disc. While most viruses require human intervention to go from one host computer to another, others are capable of self-replication and transfer. These autonomous programmes are known as "worms."[21]One of the most distinctive characteristics of cybercrime is that it occurs in a nonphysical domain without territorial boundaries. Cybercriminals are able to target computers or networks anywhere in the world and may employ third-party computers or networks situated in areas entirely distinct from their own or their victim's country. Any nation attempting to prosecute a cybercriminal will be forced to reckon with the fact that even a local hacker may have exploited Internet connections in other nations to commit a local cybercrime, even if unintentionally.[22] In addition, the cybercriminal may reside in a country with contradictory or nonexistent cybercrime laws."[23]

At the beginning of the twenty-first century, a notable instance of this type of enforcement difficulty occurred when hackers used stolen credit card information to extort money from multiple American banks. The Federal Bureau of Investigation ("FBI") identified

and Penal Code, 37 Brook. J. Int'l L. 1143 (2012).
[19] Charlotte Decker, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, 81 S. CAL. L. REV. 959 (2008).
[20] Dad Weissbrodt, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, 22 Minn. J. Int'l L. 347 (2013).
[21] Dominic Carucci, David Overhuls&Nicholas Soares, Computer Crimes, 48 AM, CRIM. L. REV.375, 378 (2011).
[22] Stephan Wilske; Teresa Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, 50 Fed. Comm. LJ. 117, 178 (1997).
[23] Nicholas W. Cade, *Supra Note 1* at 1148.

ISSN: 2582-6433

two Russian citizens residing in Russia as the suspected hackers. However, the United States and Russia did not have a mutual legal assistance treaty (MLAT) that would have permitted extradition of the suspects to the United States.

Currently, terrorism appears to be the crime (or class of crimes) with the most popular argument for universal jurisdiction and the best analogy to piracy. However, even terrorism has a low probability of facing truly global prosecution.[24] Jurisdiction over cybercrime is the unresolved set of constraints resulting from the absence of a consistent set of cybercrime definitions, as stated previously. Proponents of universal jurisdiction note that even piracy lacks international definitions. Theorists on both sides of the universal jurisdiction debate note the troubling fact that if the same acts that generally satisfy the elements of piracy are committed under the auspices of a sovereign state, they are considered privateering, an act that is neither subject to universal jurisdiction nor universally condemned.[25]

A cybercriminal may attack a global network using a virus that can self-replicate and adapt to different computer systems and programmes, making it impossible to precisely determine the nature and duration of the damage. In the event of such an assault, there may be millions of victims only within the prosecuting nation's borders, not to mention the number of victims who could be affected on a continuous basis throughout the world.[26] A case of this magnitude and complexity may overwhelm a nation's judicial resources, and there are few procedural tools that could effectively restrict the extent and complexity of such legal activities. Providing nations with universal jurisdiction is unrealistic as a singular method for combating cybercrime, despite the fact that it acknowledges a number of crucial realities.[27]

7. Conclusion and Suggestions

In light of the aforementioned concerns and hypotheses, the employment of universal jurisdiction to combat cybercrimes appears to be an effective and plausible strategy. Granted,

[24] Nicholas W. Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code, 37 Brook J. Int'l L 1160 (2012).
[25] 382 Nicholas W. Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code, 37 Brook J, Int'l L 1139 (2012) at 1160
[26] James D. Fry, Comment, *Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction*, 7 UCLA J. INT'L L. & FOREIGN AFF. 169, 175 (2002).
[27] Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 132 (2007).

ISSN: 2582-6433

the principle cannot be applied to all types of cyber-crimes, but crimes such as the distribution of child pornography, extortion, the leaking and hacking of confidential State documents, cyber terrorism, etc., can be combated through the application of the universality principle, as there is international consensus on the appropriate sanction for these offences. Due to the nature of the internet, it would be incredibly difficult to pursue such offenses. The perpetrator could be located anywhere in the world and utilize a server or computer in a different region. In such a case, locating the culprit and gathering the necessary proof becomes incredibly difficult.

Cyberterrorism and other terrible cyber-crimes may pose the biggest threat to national and international security since the invention of mass destruction weapons. As states and their economies grow more intertwined, mostly as a result of the Internet and the international financial system of global trade, the ramifications of a cyberattack will intensify. Likewise, if cybercriminals gain expertise upsetting national governments and shutting down vital infrastructure, their attacks will certainly become more effective. States, the business sector, and international organizations have made considerable efforts to improve international collaboration, but much more must be done. However, when taking action, it must be noted that, due to the inherent fragility of the Internet's architecture, these additional measures will not totally prevent cyberterrorism. In addition to deterrence, Cyberterrorism and other serious cyber-crimes must be confronted with a multi-pronged strategy that emphasizes international collaboration and international standards.

Due to the characteristics of cyberspace, international law's principle of universal jurisdiction is the most practical method for addressing such offenses. This is not to suggest that territorial jurisdiction (or nationality, passive personality, or protective jurisdiction) could not be utilized to prosecute these crimes, but adequate evidence and state willingness to exercise other forms of jurisdiction would be required. Universal jurisdiction is possibly the most practical means of prosecution and, consequently, deterrence. Cyberterrorism and other terrible cyber-crimes can be significantly deterred by a multi-layered strategy to mitigate and deterrence. Until states are willing to exercise universal jurisdiction over cybercriminal activities as part of this layered strategy, it is only a matter of time until they can unleash a cyber apocalypse.