NEED OF INTERNATIONAL LEGISLATION REGARDING CYBER CRIMES: PAKISTAN PERSPECTIVE

Ashraf Ali
Associate Professor, Department of Law, Abdul Wali Khan University Mardan, Pakistan, ashrafali@awkum.edu.pk

Ilyas Khan
Assistant Professor, Department of Law, Abdul Wali Khan University Mardan, Pakistan, drilyas@awkum.edu.pk

Sobia Bashir
Assistant Professor, Law College, University of Peshawar, Pakistan, sobiabashir@uop.edu.pk

Abstract
This research study focused on computer and internet have benefitted man immensely but have also simultaneously begotten cybercrimes having serious implications on society. The international community is seriously concerned about the surge of cybercrimes. Inadequacy of domestic cyber laws and lack of international cooperation in the field hamper to fight this menace. The difficulty to establish jurisdiction in the ubiquitous and borderless cyberspace, while investigating and prosecuting cybercrimes, further adds to the issue. Current domestic laws governing cybercrimes in many states are weak to combat cyber offenses. The conventional legal mechanisms cannot cope with the adverse aftermath of the mushrooming Information Technology which renders the cyberspace a sanctuary for criminals who torment the unaware internet users. Prosecuting these anonymous and veiled offenders require appropriate legal framework at national and international level. Some international institutions like UN and other organs are striving to fight cybercrimes and likewise the Council of Europe has introduced an international treaty in this regard. It is the only available treaty about cybercrimes with many benefits for the member states. This research article has also focused on the grey areas in domestic criminal laws relating cybercrimes in a global perspective. The study concludes that Budapest Treaty is the best international legal framework to fight cybercrimes and needs the comity of nations to ally with.

Keywords: Cybercrime, Cyberspace, Cyberlaws, Jurisdiction, Pakistan

INTRODUCTION
Crime is a social as well as an economic phenomenon, being as old as human society. In a theological perspective, history of crime can be traced back to Cain and Abel (Gillani, 2009). Aspiring and fighting, at times maliciously, since long to control the four corners of a state, man has now gained admittance to the newest arena of human activity, the fifth domain which is the cyberspace (Ball, 2017). The crime committed in this new domain is called cybercrime and the offender is a cyber-criminal.

Not deterred by the apprehension of prosecution or punishment, the malicious intruders of the cyberspace, the cyber offenders, lurk on this borderless realm, unlawfully interfering with the privacy of internet users, endangering financial health of business, fracturing trust of the clients and threatening security of nations (Sprinkel, 2001). More alarmingly, the international community is gravely concerned over using the cyberspace and internet for terrorist purposes (Fidler, 2016)

Undeniably, Internet is one of the most fascinating phenomena of this technological epoch. It has revolutionized our way of thinking, living and working. According to a research conducted in 2015, three billion people are connected to the internet world over. It is almost to 42 percent of the global population. whereas 70 percent are involved in using of networks (Gunduz, 2017).
Internet has furnished man with sophisticated form of communication; cybercrime is its ugly outcome which has plagued the modern human society. Although the benefits of internet have expanded exponentially, cyberspace has also become a powerful magnet and sanctuary for the criminals, mainly due to their low possibility of being detected (Park, 2017). Cyber criminals have become increasingly innovative to bust security measures. They evade punitive actions for limitations of territorial and legal jurisdictions which provide these offenders protection because of outdated and or non-harmonized legal regimes. Further, police usually have insufficient skills as well as resources to monitor Internet traffic, probe complaints and prosecute or take timely action against the offenders. The global and borderless nature of the cyberspace permits cooperation and coordination among cyber criminals to dissipate their assets over several jurisdictions and achieve their malicious designs with impunity (Jica, 2013).

In the previous couple of years, the quantity of reports concerning focused on assaults against important infrastructure has expanded. Modern technology facilitates wireless communication, allowing the globalization of Internet Services like Google, Yahoo, Facebook, and others that operate in one country but can be accessed by users’ world over. From a perspective of crime prevention, such state of affairs is inexpedient to the effect that cybercrime do not require the victim and the criminal to be situated in the same country. Thus, most of the cyber offences are dimensionally transnational (McCusker, 2006). Therefore, to strive cybercrime, measures including adequate national legislation, proper training of law enforcement personnel and multinational agreements asking for effective international cooperation is required.

**Meaning of Law and Cyberlaw**
Law can be defined as “A system of rules created by a society to regulate behavior and punish crimes” (Blackwell, 2008). Laws can be made by assemblies through enactment, the government officials through declarations and regulations, or judges through precedents. Formulation of laws may be commanded by a written or unwritten constitution.

Laws dealing with the Internet, including statutes, regulations, cases, and disputes that have an impact upon people as well as their transactions via computers are called cyber laws and can also be called cyberspace laws.

In other words, cyber law deals with issues of interacting with people through online medium and having capital transactions that emerge in this respect, including intellectual property rights, freedom of expression, secrecy, internet business and safety, as well as questions of jurisdiction (Garner, 2009).

**Meaning of Crime and Cybercrime**
Black Dictionary of Law defines crime as “An act that the law makes punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding”.

The term cybercrime is a crossbreed of ‘cyber’ and ‘crime’. Cybercrime is facilitated by a computer through a specialized gadget or a transmission media recognized as the cyberspace and worldwide system called the Internet. Taking it in a customary perspective, cybercrimes simply constitute a sub-set of conventional crimes where information and communication technology is used as a vehicle or instrument to commit them. The definition sticks to the basics of legal interpretation related to traditional criminal offences. (Brown, 2015). Various terms like cybercrime, computer-related crime, digital technology crime or e-crime are generally used synonymously.

Chung. W. et al have defined cybercrime as “illegal computer-mediated activities that often take place in the global electronic network” (Chung, 2006). This definition restricts the cybercrime to internet related unlawful conducts. An article “A socio-technological analysis of cybercrime and cyber security in Nigeria” proposes a definition for cybercrime which includes every single unlawful action where the computer, computer frameworks, data system or information is the objective of the crime and those known unlawful activities or crimes that are effectively carried out through or with the help of computer, computer system, network data or information (Olayemi, 2014). A simple definition of cybercrime could be “an unlawful act or conduct wherein the computer is either a target, tool or both” (Dashora, 2011).

**Meaning of Cyberspace**
Since antiquity till about a century ago, man operated in only two physical domains, the land and the sea. A century back, man added a third physical domain, the air or rather the aerospace to operate in. With the
advancement of science and technology, in fifties, man entered the outer space as the fourth domain. With the evolution of computer technology in the last few decades, human activities have now extended to the fifth domain, the cyberspace. Not only this domain has characteristics different from the other four domains, but also there are problems to define it. The title ‘The Lessons of Lucas films Habitat’ truly depicts that the definition of cyberspace is related more to its social interactions involved than its technical implementation (Morningstar, 2008). The word ‘Cyberspace’ emerged in science fiction literature in eighties and was rapidly and extensively used by computer professionals in nineties as household term. In this period, there was a dramatic growth of digital communication, networking and internet with the emergence of the term ‘cyberspace’ as a new phenomenon.

In a social perspective, internet is used by individuals for interacting, exchanging ideas, sharing information, trading, engaging in social work, playing games, directing actions, creating art, participating in political debates etc. The term cyberspace traditionally describes anything related to Internet and the multiform Internet culture.

There are issues to exactly define cyberspace. First, we try to study the cyberspace in a philosophical perspective. Together, the metaphor of ‘cyberspace’ and the distinctive spatial and social practices associated with it permits the virtual to take on an ontic (real) character. ‘Cyberspace’ in this logic, is cognized as both an ethereal alternate dimension which is at the same time infinite and ubiquitous (because everybody with an Internet connection can visit it), and as fixed in a distinct location, though a non-physical one (because in spite of being infinitely open to all, intending participants can enter into the same social space, marketplace or civic forum). The ontic character assigned to ‘cyberspace’ is likely also supported by the English language grammar rules applied to the internet. Familiar prepositions related with internet use (e.g. to go online, to get on the internet or to visit or go to a website) suggest spatiality applied to the internet. Such is the ‘movement’ to the cyberspace that is not spatially proximate to the internet user.

Cyberspace is virtual, as one cannot specifically locate it as a tangible object but being associated with the streaming of digital data through a network connecting computers, it is ‘real’ in its effects (Graham, 2013). In a technical perspective, Daniel T. Kuehlhas defined cyberspace as “A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies” (Kuehl, 2009).

Territorially-based laws are alien to this new environment which needs new laws of its own. Though the participants of cyberspace try to self-regulate it, the state and international community must, apart from doctrine tied to territorial jurisdictions, frame rules to govern the new cyber phenomena having no clear parallel in the physical world. These new laws will have to resolve legal issues of the cyberspace (Johnson, 1996).

**Meaning of Jurisdiction and Cybercrime Jurisdiction**

According to Microsoft Encarta Premium 2009, Jurisdiction is authority practiced by a country, a legal body or an authoritative body over people, territories, behaviors and property. In law, the term for the most part alludes to authority of a court to hear and arbitrate legal issues. The jurisdiction of the court may be determined according to various criteria. Subject matter is one common criterion in this regard. Courts are set up to handle specific types of cases; for example, criminal courts hear criminal cases and family courts hear suits for divorce etc.

One of the unique features of the Information Technology of our era is that it has defeated the territorial, legal and jurisdictional boundaries of sovereign states and we can say that web-sites are nowhere but they are everywhere. In this perspective, Information Revolution has given birth to one of the most debated contemporary controversies, i.e. the issue of jurisdiction, the sine qua non of administration of justice. The question of jurisdiction is also of fundamental importance in fighting cybercrimes in international scenario and needs deliberation. Golak Prasad Sahoo has referred to the concepts of jurisdiction, as given in the Encyclopedia America wherein Jurisdiction is power or authority. Generally, the term is applied to quasi-judicial bodies and courts outlining the scope of their actions. In this context, jurisdiction is the authority of a court to hear and declare judgment in respect to a particular matter within certain geographical boundaries (Sahoo, 2010).
State legislatures have the power to enact, modify or repeal legislation, not overriding international law. The jurisdiction of Law of Nations has classified usefully into three classes. Firstly, purview to jurisdiction or enact (called prescriptive jurisdiction, lawmaking powers, subject matter or lawmaking authority) alludes to a nation’s capacity refers to a nation’s ability (by and large through its legislature) to form its laws pertinent to persons or things. Prescriptive jurisdiction could be paramount state’s specialist to criminalize a given conduct or ‘apply its laws to certain people or things’. Secondly, jurisdiction to settle alludes to a nation’s capacity to subject people or things to the method of its courts or authoritative tribunals, whether in civil or in criminal procedures, whether or not the state may be a party to the procedures. It is, in other words, a national court’s control to bring an individual or thing into its adjudicative handle. Thirdly, jurisdiction to implement (enforcement jurisdiction and administrative powers) alludes to the capacity of a country to execute its law or to rebuff noncompliance with its laws. Authorization jurisdiction is the state’s right to implement its enactment through, for illustration, the police and open prosecutors, by examining a wrongdoing and capturing a suspect (Brenner, 2004).

**Territorial Principle**

Territoriality has traditionally been the most common basis of criminal jurisdiction. The very spirit of sovereignty begins with the national-state which, by definition, has the competency to forbid a criminal conduct that occurs wholly or partially on its territory. As per this rule, a state cannot practice its jurisdiction in any form in the domain of another state until some global settlement permits it to do as so. Two categories of territorial jurisdiction exist, subjective and objective. Subjective(ordinary) territoriality applies where a material or constituent element of a crime occurs within the territory of a state but is accomplished abroad. Likewise, objective (the effects theory) territoriality is the one where the result or effect of the criminal conduct strikes the asserting nation, but the other essentials of the crime occurs entirely beyond its territorial borders (Blakesley, 2007).

**Active Personality Principle**

Active personality principle, also called ‘nationality theory’, accords jurisdiction on the basis of the nationality of the criminal, irrespective of the location where the crime occurred. This introduce takes root from the principle that a state, by the quality of sway, work out boundless control over its people. States may hence be permitted to apply purview over their citizens neglecting their citizen areas when they commit wrongdoing. Additionally, till nationals hold their citizenship, they ought to follow to their national laws when they are in foreign country (Stockton, 2014).

**Passive Personality Principle**

The doctrine, also termed ‘passive nationality principle’, speaks of jurisdiction on the basis of the nationality of the victim. In this regard, the assumption is that nations are responsible to care for their citizens, even when abroad. Every so often, states have amplified the principle to work jurisdiction over violations committed counter to their citizens (McCarthy, 1989). The sentencing of the Kazakhstan citizen, Oleg Zezev, living in Almaty, to 51 months’ imprisonment for computer hacking charges in the federal court of Manhattan US is an example of this principle (Cottim, 2008). Nevertheless, such practice has been uncommon and controversial.

**The Universality Principle**

The universality principle, also called ‘principle of universal jurisdiction’, is the doctrine wherein all nations claim jurisdiction over crimes that are unanimously known to be crimes against humanity and perpetrator of such crimes are judged as *hostis humani generis*—the enemy of all mankind. These crimes include piracy, slave trading, torture, genocide, gross human right violations and likely terrorism (Reydams, 2003).

**The Protective Principle**

It is also called “protective theory”, “security principle” and 'harmed “injured forum theory”, the protective theory enables a nation to practice jurisdiction when an action that happens outside of its borders undermines its security or essential functions. Examples of such acts include forging of its authorized seal or coinage, espionage and treason (Oraebgunam, 2015). Concurring to this guideline, a nation-state may state locale over acts executed exterior its borders jeopardizing its dominion and autonomy.
Nature and Classification of Cybercrimes

The ways of committing crimes have changed drastically over time. In developed world, highway dacoity, for example, is a thing of the past. Presently, we have moved into the dominion of cybercrimes. Many of the cybercrimes are some forms of conventional crimes. For example, fraud is a conventional crime which can also be committed through a computer and the internet. Such crimes may be dealt through the conventional crime laws. However, with the developing information technology, cybercrime has emerged as new category of crime having attributes different from conventional crimes needing independent taxonomy (Wales, 2012).

Types of Cybercrimes

Cybercrime are of various types and have been classified in different ways. Ajeet Singh Poonia has broadly classified cybercrimes in to 04 major groups (Poonia, 2014) with some degree of overlap among different groups:

Crime against Individuals
These crimes include harassment of any one with the utilization of PC, for example, email, Transmission of Child Pornography, Cyber Defamation, Hacking, E-mail Spoofing, Internet Relay Chat, Malicious Code, Net Extortion, Posting, Trafficking, Phishing, Credit Card Fraud and Dissemination of Obscene Material alongside Software Piracy, Indecent Exposure and so on.

Crime against Property
This includes Computer Vandalism, Intellectual Property Crimes, and Salami Attacks. Such crimes usually have financial implications and at times may not be observed.

Crime against Organization
Another category of cybercrimes is those against organizations or states. Cyber Terrorism is a distinct kind of crime in this category. Cyber-attacks against a government or military installations fall in this category.

Crime against Society
This category includes Web Jacking, Forgery, Cyber Terrorism, Polluting the Youth through Indecent Material, Sale of contrabands like drugs, Financial Crimes, Cyber Contraband, Net Extortion, Data Diddling, Logic Bombs, Salami Attacks, etc. Currency notes, mark sheets, revenue stamps, etc can be counterfeited through computers, scanners and printers. In Web Jacking, hacker takes control of some website and may even change the substance of website to fulfill political, social or financial objectives.

Cyber Laws Pakistan

The legislative history of Pakistan tracks back to the British colonial era and many Pakistan laws are its continuation. In Pakistan the following laws are governing issues related to communications, information, transactions, documents and record in electronics form, The Telegraph Act, 1885 as under,

a) The Wireless Telegraph Act, 1933
b) The Electronic Transaction (Re-organization) Act, 1996
c) Electronic Transaction Ordinance, 2002
d) The Payment Systems and Electronic Fund Transfers Act, 2007
f) Prevention of Electronic Crimes Act, 2016

Telecommunication Laws of The Colonial Era

Two pre-partition Acts were adapted in Pakistan through ‘The Adaptation of Central Acts and Ordinances Order, 1949’ (Munir, 2005). These laws were as follows:

The Indian Telegraph Act, 1885

Essentially interested in broadcast communications as a law-and-order apparatus, the first transmit lines in the subcontinent were laid in 1851 by the British government which later on passed the Indian Telegraph Act, 1885 (Indian Telegraph Act, 1885). The Act empowers the Government and any other licensed body to provide telecommunication services and to place, maintain and safeguard telegraph lines and posts. According to Section 7 of this Act, the Central Government capacities as the administrative specialist to control the act of whole or any transmit system, kept up or worked by the government or few other persons permitted under this Act.
The Indian Wireless Telegraphy Act, 1933
The Indian Wireless Telegraphy Act, 1933 (Indian Wireless Telegraphy Act, 1933) forbids the control of wireless devices deprived of licensee. Under the Act, The Director General, Pakistan Post Office, or an officer authorized by him is competent to issue such license. The Act makes that state is the sole controller and owner of the radio communication channel, including VSAT links for Internet traffic.

Pakistan Telecommunication (Re-Organization) Act, 1996
Pakistan Telecommunication (Re-Organization) Act, was propagated in 1996, aiming to restructure the telecom sector of Pakistan. The Act commands for the institution of:

a) Pakistan Telecommunication Authority (PTA)
b) Pakistan Telecommunication Company Ltd. (PTCL)
c) National Telecommunication Corporation (NTC)
d) Frequency Allocation Board (FAB)

PTA contains three individuals selected by the Federal Government for a tenure of four years. One of them was appointed Chairman of the Authority and was given executive powers. One of the duties of the PTA is to ensure the availability of a wide range of high quality, skilled, practical and fight telecommunication facilities throughout Pakistan. The Authority is also responsible for protecting consumer interests and encouraging fair competition in the field of broadcast communications. The Act provides for the privatization of PTCL by transforming it from a corporation to a public limited company. PTCL has been granted exclusive fixed-line communication rights for a long time, which will end in 2003. The NTC was formed to provide telephone services to government agencies and workers. The Frequency Allocation Committee consists of six people representing each sector of concern ministry. Under Section 42 of the Act, FAB took over the functions performed by Pakistan Wireless Board established in 1951.

Pursuant to Section 43 of the Act, the FAB has the special authority and other discretionary powers to allocate and release radio spectrum to all customers, including government, providers of media communication services and telecommunications systems, radio and television broadcasting activities, and public and private broadcasting operators from April 2007. The FAB is under the administrative control of the PTA (Wilson, 2008). Under the legal powers granted to PTA, at times websites, including You Tube, considered unpleasant, are blocked through Internet Service Providers (Shaheen, 2008).

The Electronic Transaction Ordinance, 2002
In the recent past, electronic banking has been a fascinating offshoot of modern technology. Internet Banking, Tele-Banking, ATMs, Debit Cards and Credit Cards have mostly replaced the conventional banking system. To further promote electronic banking, the Government of Pakistan promulgated the Electronic Transaction Ordinance 2002 to facilitate and organize records, documents, information and transactions and communications in electronic form and to control of certification benefit suppliers. The main aim of the law was to push Pakistan into electronic dealings from old paper-based transactions. The digital documentation and signature were given legal recognition by the Ordinance which dropped the risks linked through the practice of electronic media in marketable. The law boosted the domestic banks and presently, nearly entirely banks in Pakistan have established their own ATMs, issuance credit and debit cards (Kaleem, 2008).

The Payment Systems and Electronic Fund Transfer Act, 2007
Later the exponential development of financial applications, services, and products, there has been a need of administering and managing the banks' payment systems. Subsequently, an independent arrangement of laws and guidelines on designating a payment system has been enacted in Pakistan through the Payment Systems and Electronic Fund Transfer Act, 2007.

After the exponential growth of financial applications, products, and services, there has been a need of supervising and regulating the banks’ payment systems. Consequently, an independent set of laws and regulations on designating a payment system has been enacted in Pakistan through the Payment Systems and Electronic Fund Transfer Act, 2007 (Shaikh, 2017). Through the Act, The State Bank of Pakistan has encouraged electronic banking which has laid down the foundation for Pakistan’s wide connectivity of financial institutions. As far back 2007, about half of the Pakistan’s bank branches were engaged in electronic fund transfer, supported by the legal coverage provided by Act (Akhtar, 2007).
Prevention of Electronic Crimes Act 2016
The issue of the said Act, for its inherent controversies, had been lingering on in Pakistan for several years starting from Pakistan Electronic Crime Ordinance, 2007 which lapsed in 2009. Ultimately, having been passed by the National Assembly and Senate, in August 2016, The President of Pakistan has agreed to the controversial Prevention of Electronic Crime Act (PECA) of 2016. The law aims to prevent unauthorized activities related to information systems and provides for associated crimes and their investigation, prosecution mechanisms, hearings and global collaboration.

The Act presents a scope of offenses including unapproved access, transmission, duplicating or impedance in a data or information system. Harsher punishments are set for these violations on the off chance that they involve data systems or information linked with critical infrastructure. The Act additionally presents the offense cyber-terrorism, the adoration of terrorism, employment for or backing terrorism, by somewhat info system or gadget and proclaims these offenses culpable under the Act.

The Act additionally presents offences of junking, spoofing, circulating and conveying hateful code. Unlawful tampering and so forth of communication device have likewise been criminalized. Crimes counter to the humility of a normal somebody or minor have been incorporated into the Act. Other recently incorporated offences are cyber pestering, distribution, possession, having or obtaining online youngster pornography.

The investigative process involves saving, searching, seizing and retaining information, as well as collecting and recording data in real time through search warrants or court orders. Section 29 of the Act grants the federal government the power to establish or designate law enforcement agencies “as investigative agencies” to investigate crimes under this Act. Under the bill, cybercrime is investigated and dealt with by the FBI (Hoor-Ul-Ain, 2016).

Section 37 of the Act empowers the Pakistan Telecommunications Regulatory Authority to, in its opinion, for the glory or integrity of Islam, security or defense of Pakistan or any part thereof, public order, decorum or morals or in connection with contempt of court or the commission or incitement of this Act related crimes.

PECA in International Legal Perspectives
The International Covenant on Civil and Political Rights (ICCPR) and the COE Convention on Cybercrime remains the core international legal initiatives considered by nations while shaping electronic and cybercrime strategies. Agreeing with multilateral cybercrime initiatives persuades states to develop pertinent legislation with the intention of international cooperation.

In the case of Pakistan, section 42 of the PECA 2016 provides for collaboration to any state or international entity that requests for data needed in crime analysis or hearing of crimes related to cybercrimes. Under this provision, numerical statistics of citizens collected in text, audio, graphic or further arithmetic settings may be provided to affiliates without the authorization of the court. This commitment is testimony to Pakistan determination for global collaboration, as per stated in the Introduction of the Act.

Domestic Reaction to PECA
In comparison of cybercrime laws across the world, PECA commands sever punishments for cyber offences and even criminalize acts which are not considered illegal in other countries. The Act restricts internet independence, curbs liberty of speech, right to privacy and access to information. The act has been criticized by the civil society as well as IT industry for restricting human rights and giving excessive powers to law governmental agencies and has been named the ‘draconian’ (Khan, 2016).

CONCLUSION
Keeping in view the rising use of computers and internet, exponential growth of cybercrimes with grave effects on the society, borderless nature of cyberspace, ineffective national laws and lack of international cooperation, world nations and global community have serious concerns about cyber offenses and cyber security. In the scenario depicted, there is strong need of an international treaty which should have wide following to effectively fight cybercrimes. It is evident that, not ruling out any alternative legal framework, Council of Europe Convention on Cybercrimes, also called Budapest Treaty, is the ultimate and currently
the only international legal framework available to serve the purpose and ensure reasonable global cyber security.

RECOMMENDATIONS
The writers are of the view that, to make the cyberspace secure in the best interests of mankind, all the states of world should join Budapest Treaty on cybercrimes. The UN may own the Treaty and help in its global accession.

REFERENCES


