Indian Journal of Economics and Business
Vol. 20 No. 3 (July-December, 2021)
Copyright@ Ashwin Anokha Publications & Distributions
http://www.ashwinanokha.com/IJEB.php

# Contemporary Challenges of Digital World and Cyber Crime and Management Solutions in the light of Cyber Crime Bill 2016 of Pakistan and Islamic Management Perspective

**Muhammad Umar Riaz Abbasi*[1], Dr. Rabia Aamir[2], Dr. Nabegha Mahmood[3]**

[1]*PhD Scholar Islamic Studies, National University of Modern Languages Islamabad Pakistan.*
*Lecturer, Researcher, Academic writer and Well-known Columnist, Author of Five Books.*
*ORCID: http://orcid.org/0000-0001-6977-9516*
[2]*Assistant Professor of English, National University of Modern Languages, Islamabad, Pakistan.*
[3]*Ph.D. Leadership and Management Studies, Assistant Professor, Management Sciences Department, Virtual University of Pakistan.*

**Received:** 6th May 2021
**Revised:** 9th June 2021
**Accepted:** 16th August **2021**

**Abstract:** A computer and a network are all that is needed for any criminal activity of cybercrime. A vigorous cybercrime legislation has, therefore, become a necessity in today's digital age. Many nation-states take great measures to draft the inclusive laws regarding this legislation. The government of Pakistan is also working hard to amend the present laws which pursue to make sure the regulation with regards to the cyber security. Digital technology has many advantages but also has a dark side. Unfortunately, its dark side is paid much heed to which does not sit well with any code of ethics. The existence of Islam in the cyber world has created an opportunity for dialogue besides forming a new method of learning for mental and physical health The Electronic Transactions Ordinance ETO 2002 in the Islamic Republic of Pakistan forbade the illegitimate and unauthorized accessibility towards the information. It preceded the declaration of Prevention of Electronic Crimes Act PECA 2016. The Act lays down the laws for cyber-terrorist crimes which are conducted with the intent of committing terrorism. The penalty for this offense is based on the 14-year term of custody or a charge of Rs 5 million, which makes up to US $47,450. Understanding the Islamic perspective in this regard can be helpful for the betterment of the lives. Islam strictly forbids a spread of fake news through news sourcing which has increasingly become rampant in today's cyber world which can lead towards malprctices. Thus, this research aims at sharing all the contemporary challenges with regards to the cybercrimes and possible solutions in the light of constitution in Pakistan.
**Keywords:** Cyber Crime, Islamic Law, Pakistan, Challenges, Solution, Health Care, Digitalization, Management.

## Introduction

This is an extensive study that is conducted on a sensitive topic. Cybercrime cases have been increasing in the past years since digital technology has invaded every sector. Some people are misusing it at a higher level that is unlawful. Pakistan has reported cases of cybercrime and being an Islamic nation, it has passed

cybercrime law as well. Verily, this study will reveal all such key aspects related to cybercrime. Moreover, the study is majorly based on revealing the conceptual view with regards to Islam as well as the cyber world.

**Research Problem**

The arrival of the digital age has emphasized the need for vigorous cybercrime legislation to be framed through the nation-states, though, there has been a great level of struggle going on in terms of drafting the inclusive laws regarding this. Technological growths are outstripping the solutions which are proposed through the state institutions that are based on addressing the new experiments rising from the growing usage of digital media. The government is even working hard to amend the present laws which pursue to make sure the regulation with regards to the cybersecurity[1]. In the Islamic Republic of Pakistan, preceding the declaration of PECA that stands for the Prevention of Electronic Crimes Act, back in the year 2016, ETO, the Electronic Transactions Ordinance 2002 had been the ordinance to regulate the illegitimate and unauthorized accessibility towards the information[2]. Lacking direct protection of the data legislation, the ETO requirements tentatively controlled data privacy as well as protection. However, it does not directly control the data protection though, banning illegitimate or unauthorized accessibility towards the information. This research is to find out such contemporary challenges of cybercrimes considering the Islamic Law execution in Pakistan[3].

**Aims and Objectives**

The study aims to find out the contemporary challenges of cybercrimes as well as solutions in the light of Islamic law while also considering the cybercrime bill 2016 of Pakistan. The key objectives of the study are, To study the cybercrimes and their types in the light of Islamic teachings

- To find out the contemporary challenges of cybercrimes and how the country is dealing with it
- To review Islamic law for understanding the cybercrimes
- To study the cybercrime bill 2016 of Pakistan and its impact as well
- To find out how Islamic teachings are directing the people to restrain from cybercrime

**Significance of the Research**

Though many researches have been conducted with regards to the cybercrime activities in Pakistan, this paper is a comprehensive discussion based on the cyber bill 2016. This research has also incorporated data concerning Islamic law and cybercrime[4]. The discussion in this report is based on the Islamic ideology and Surah that prohibits any such activities that today we may define as cybercrime activities. This research paper may be significant as there are no such researches found yet that have been based on the blend of digital technology crime as well as the Islamic viewpoint.

---

[1] Rehman, T. U. (2020). International Cooperation and Legal Response to Cybercrime in Pakistan. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 424-434). IGI Global.

[2]Windiarti, I. S., Norcahyono, A. P., & Prabowo, A. (2020, December). Digital Literacy for the Millennial Generation in Industrial Revolution 4.0 Era in Islamic Norms Perspective. In *ICIC 2020: Proceedings of the 1st International Conference on Islamic Civilization, ICIC 2020, 27th August 2020, Semarang, Indonesia* (p. 467). European Alliance for Innovation.

[3] Ibd

[4] Ibd

**Research Methodology**

This paper is a qualitative analysis of some relevant data available through different sources regarding cybercrime and Islamic law. The available data is triangulated while consulting various studies and only the authentic sources are added in this research. Using the critical insights of some principal resourses from Quran, Hadith, sunnah, constitution of Islamic Republic of Pakistan pertaining to cyber laws, and international cyber laws, this descriptive paper critiques upon different aspects of cybercrime law in Pakistan 2016. Extracting the data from existing studies, this is a diagnostic exploration that suggests some futuristic recommendations for the merits and limitations of cybercrime law in Pakistan. The methodology for this study combines the available data analysis and textual analysis tools in order to study the ethical importance of cybercrime laws in a given society.

**Literature Review**

**Cybercrime and Contemporary Challenges**

Two among many challenges to comprehend cybercrime activities are lack of awareness and poor culture of cyber security both at individual and organizational level. There is no such trained or competent manpower for the implementation of the security measures. Moreover, there is no email account policy, particularly with regards to the defense forces, police department as well as security action personnel. Additionally, cyber-attacks have been reported, not only from the side of the terrorists but even from the neighboring state conflicting with the National interests. Furthermore, the least obligatory eligibility for joining the police does not involve any of the knowledge with regards to the computer sector.

Thus, they are more or less uneducated in terms of cyber-crime. The speed with regards to the changing cyber technology tends to beat the development of the government sector. Therefore, they cannot recognize the source of such cyber-crimes. The advancement with regards to the Research & Development related to ICTs is rather poor. The security forces as well as law enforcement workers are not armed for addressing the high-tech criminal activities. The current protocols are rather not self-sufficient to classify the responsibility of any officials with regards to the crimes which are committed internationally. In addition, the budgets with regards to the security purpose through the government, particularly for the training of law implementation, security workers, as well as detectives in ICT are very poor in comparison to the other crimes.

Cybercrime and its Types

Cybercrime refers to criminal activity which includes a computer, interactive device, and a network. As most of the cybercrimes are conducted for generating a profit that the cybercriminals desire, most of the cyber crimes are done to deactivate the computer systems[5]. Most of them tend to use PCs or networks for spreading malware, unlawful information, undesirable images, or other poor content. Cybercrimes tend to target the computers and infect them with a virus that is then dispersed to other operating systems and even in the overall network. Cybercrime has many types that are discussed below,

**DDoS Attacks**

This refers to making an online service inaccessible and plug off (deject) the network through devastating the site with the traffic from different sources. Greater levels of the network with regards to the infected

[5] Nurse, J. R., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. *arXiv preprint arXiv:1901.01914*.

devices, also called, Botnets are made through the deposition (changing the position) of the malware on the computers of the users[6]. After this, the hacker then plans to hack into the system as the network gets down.

**Botnets**

Botnets refer to the networks from the cooperated computers which are operated externally through remote hackers. They then tend to send spam or attack the other computers with such botnets. Botnets can even be utilized for acting as malware and performing malevolent tasks[7].

**Identity Theft**

This happens when the criminal aims at gaining access to the personal information of a user for stealing the funds, accessibility towards the confidential information, or participating in fraudulent activities against the tax or health insurance[8]. They can even operate a phone/internet account in the name and may conduct cybercrime while claiming the benefits of the government benefits from others' names[9].

**Cyberstalking**

This type of cybercrime includes online harassment as in which the user is exposed to an overabundance of online messages as well as emails. Normally, cyber-stalkers tend to use social media, websites as well as search engines for intimidating a user as well as imparting fear. In this case, the cyber-stalker is aware of their victim and scares the person as well.[10]

**Social Engineering**

Social engineering includes criminals who tend to make direct contact with the other person, normally through the phone or via email. They aim at gaining confidence as well as generally behave as the customer service agent to provide the essential information that is required. This is normally a password, which regarding the company in which one is employed or the bank account information[11]. Cybercriminals tend to find out anything about a person through the internet and then try to make a personal friend on social media accounts. When they succeed in accessing the account, they tend to sell the information of the person whenever they want.

**PUPs**

PUPS stands for the Potentially Unwanted Programs. They are less aggressive in comparison to the other cybercrimes, however, are a kind of malware. It includes uninstalling the essential software in the system involving the search engines as well as pre-loaded applications. They can involve spyware or adware[12]. Thus, it seems to be a good idea for installing antivirus software for avoiding malevolent downloads.

---

[6] Ibd

[7] Smith, K. T., Smith, M., & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*.

[8] Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems*, *41*(3), 669-682.

[9] Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). Various Types of Cybercrime and Its Affected Area. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3* (pp. 305-315). Springer Singapore.

[10] Ibd

[11] Ibd

[12] Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

**Phishing**

Such a type of attack includes the hackers who send malicious email attachments or URLs to the users for gaining access to their accounts or PCs. Cybercriminals are turning out to be keener and such emails are not highlighted as spam.[13] Users are easily fooled through the emails which claim that they require to put a new password or change their billing details, which gives access to the criminals.

**Prohibited/Illegal Content**

This includes the criminals who tend to share and distribute unsuitable content that is very upsetting and aggressive. Offensive content may involve sexual activity among the adults, or videos based on penetrating violent or criminal activities[14]. Illegal content involves the materials which tend to advocate terrorism-based acts as well as material based on child exploitation. Such type of content is both on the daily internet as well as on the dark web that is an unidentified network.

**Online Scams**

These are normally the ads or spam emails which the promises have based on rewarding or offering impracticable amounts of cash. Online scams involve tempting offers which are way too much expected to be advantageous[15]. However, when they are clicked on, they usually can result in malware for interfering and compromising the information.

**Exploit Kits**

Exploit kits require a vulnerability that means a bug in the code of the software. This is done for gaining the control of the computer of a user. They are convenient tools that criminals tend to buy online and utilize in contradiction of anyone having a computer[16]. Such exploit kits are elevated on regular basis just like the normal software and are accessible on dark web hacking sites.

Cyberworld in Islamic Communication

Two key types of knowledge are there in Islam. First is the heavenly knowledge whereas, the other is learned by the efforts of a person with a balanced approach in investigation depending on his/her experience as well as observation. Cyber technology refers to a baby of Information, Communication, and Technology (ICT) and is related to the second category[17]. Nowadays, internet has turned out to be the most prevalent medium concerning communication in the digital era. The internet is declared to be religiously, socially, as well as ethically significant for having positive as well as negative impacts. Many scholars believe that Islam is attacked by the internet. However, they are of the view that the Muslim community must use it as a weapon for defending themselves with the development of the skills which may let them use this source.

Internet has increasingly become an appealing medium for conducting knowledge and Muslims must not segregate and ignore the new technologies as avoiding them will have negative consequences on the Islamic

[13] Rantala, R. R. (2008). *Cybercrime against businesses, 2005*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

[14] Magutu, P. O., Ondimu, G. M., & Ipu, C. J. (2011). Effects of cybercrime on state security: Types, impact and mitigations with the fiber optic deployment in Kenya. *Journal of Information Assurance & Cybersecurity*, *2011*(1), 1-20.

[15] Ibd

[16] Ibd

[17] Possamai, A., & Turner, B. (2014). Authority and liquid religion in cyber-space: the new territories of religious communication. *International Social Science Journal*, 197-206.

community[18]. Most of the Muslims earlier had a negative perception with regards to technology. However, many scholars have challenged this thought in the light of Islamic knowledge. As according to the Holy Quan:

> ***"And (He has created) horses, mules and donkeys, for you to ride and use for show; and He has created (other) things of which ye do not know"*** (Surah An Nahl -8)[19].

This means that digital technology is one of the mediums that has emerged for the help of the nations. It does not have any concept related to evil works. The scholars say that internet can be used as a wonderful device for teaching Muslims about Islam. Muslims, specifically, are permitted for exploring the cyber world, to avail themselves of the opportunities from the technology and abandon its evils. The existence of Islam in the cyber world has even made an opportunity for dialogue as well as forming a new method of Da'wah[20]. Digital technology has many benefits but it also has many disbenefits. Unfortunately, its negative features are paid much heed to which may be un Islamic due to their unethical aspects.

Many people are victims of cyber crimes either deliberately or accidentally. In this case, the teenagers, as well as the children, are also included. It is because technology is available for everyone[21]. Following are some of the misconducts that are being conducted in the cyber world, however, they need to be condemned on moral, ethical, and religious grounds.

**Internet Gambling**

One of the prevalent crimes is Internet gambling. Most people watch internet gambling while considering it a relative as well as time-out activity. Whereas, others consider it as a source of trick. The virtually arbitrated casino games, slot machines, bingos, lucky draws, sports staking, horse race gambling, as well as skill games are easily accessible, in new forms with regards to gambling[22]. New sites are added on annual basis for the people. However, Allah has advised in the Al-Qur'an,

> "***O you who have believed, indeed, intoxicants, gambling, [sacrificing on] stone alters [to other than Allah], and divining arrows are but defilement from the work of Satan, so avoid it that you may be successful. Satan only wants to cause between you animosity and hatred through intoxicants and gambling and to avert you from the remembrance of Allah and prayer. So will you not desist?"*** (Al-Qur'an, al-Maidah: 90)[23]

In simpler terms, Islam has strictly prohibited any kind of gambling due to its detrimental consequences for any given society, the least of which are hate, humiliation, dejection, and hostility.

---

[18] Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World. *Journal of Educational and Social Research*, *4*(6), 513.

[19] Muiz, A., & Gaffar, A. (2018, July). Study Living Qur'an: The Analysis of Understanding Surah al-Nahl (125) against Demonstration-Based Communication Behavior. In *IOP Conference Series: Earth and Environmental Science* (Vol. 175, No. 1, p. 012180). IOP Publishing.

[20] Ibd

[21] Ibd

[22] Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World. Journal of Educational and Social Research, 4(6), 513.

[23] Ibd

**Digital Piracy**

This is another form of criminal attitude. It refers to the unlawful copying of the digital products, software, digital papers, as well as audio, plus music or voice, for the aim of backup storage of date while not having the obvious permission from the holder of the copyright holder[24]. In the year 2003, Faraz Rabbani has given an online fatwa that most of the Islamic scholars in the present time have declared that copyright laws are binding and mendatory[24]. Intellectual property in the present society is a highly valuable asset and thus, copyright law in no way obstructs the extent of knowledge. Most of the Islamic councils believe that copyright laws need to be implemented in true letter and spirit and going against the copyright laws is unethical.

**Online Victimization**

Though the Internet has made ample information as well as prospects for the youth available, an reliance based on computer technology entirely tends to increase the rate of cybercrime and has an impact on the various aspects of life. The US Department based on Justice has explained that teenagers, as well as children, are provided with the basic knowledge about the committers of the internet crime in the OVC bulletin online[25]. The Predators tend to contact teenagers as well as children on the Internet and persecute them while tempting them with online contact to engage them in sexual acts. They use the Internet for producing, manufacturing, and distributing child pornography, through the Internet for exposing the youth to child pornography and motivate them for exchanging pornography, alluring and manipulating the children for sexual tourism[26]. It is done to engage in sexual behavior for commercial purposes and personal satisfaction.

Considering this cybercrime as well as the types of victimizations at the hand of offenders, both the human society as well as religious body has considered online victimization as a condemnable act. Islam has laid down principles that are more than applicable in today's world and most relevant to stop any such promiscuous behavior. Therefore, we are advised to adopt a just behavior through the Holy Al-Qur'an:

> ***"O you who believe! Stand out firmly for justice, as witnesses to Allah, even though it be against yourselves, or your parents, or your kin"***...(Al-Qur'an, an-Nisaa: 135)[27]

> ***"O you who believe! Be upright for Allah, bearers of witness with justice, and let not hatred of a people incite you not to act equitably; act equitably, that is nearer to piety, and be careful of (your duty to) Allah; surely Allah is Aware of what you do"***. (Al-Qur'an, al-Mai'dah:8)[28]

[24] Mundiri, A. and Tohet, M., 2018. Contestation of Religious Identity in the Cyber World: A Case Study of arrahmah. com and VOA Islam Dealing with Religious Others on Facebook. *Walisongo J. Penelit. Sos. Keagamaan*, *26*(2), pp.391-416.

[25] Hidayatullah, M.S., Dimyathi, M.S., Abdullah, Z. and Handayani, R., 2020. The Cyber Islam Contestation In Indonesia. *International Journal of Advanced Science and Technology*, *29*(7).

[26] Kort, A., 2005. Dar al-Cyber Islam: Women, domestic violence, and the Islamic reformation on the World Wide Web. *Journal of Muslim Minority Affairs*, *25*(3), pp.363-383.

[27] Ibd

[28] Ibd

At times, online victimization tends to result in the form of spreading the harmful software in types of viruses that in return abolishes the data files in the computer and eventually identifies the theft[29]. This identification becomes helpful in adopting a just behavior to combat any cybercriminal activities in line with what the Prophet Muhammad (SAWW) has stated that:

***Do not transgress and do not allow yourself to be transgressed upon.***[30]

**Cyber Stalking**

With its irresistible competencies, the internet technology even unlocks many hidden places in the cyber world. The criminal activity of prying into someone's private matters is known as cyberstalking. Cyberstalkers are the ones who make use of the Internet like a weapon for sorting, harassing, threatening, and generating the feeling of fear and concern in the victims by classy stalking strategies, which are highly misinterpreted and, many of the cases, are considered illegal[31].

Allah has warned against such acts of mischief as stalking. He says,

> "***But seek, through that which Allah has given you, the home of the Hereafter; and [yet], do not forget your share of the world. And do good as Allah has done well to you. And desire not mischief in the land. Indeed, Allah does not like mischievous".***(Al-Qur'an, al-Qasas: 77)[32]

Therefore, through these words, God Almightly and His Messanger (SAWW) guard us against any activities that prove harmful and create chaos and disorder and is a threat to the sustainance of societies.

Cybercrime Bill 2016

In the year 2016, the lower house of Pakistan, the National Assembly, had passed a contentious cybercrime law named the Prevention of Electronic Crimes Act, 2016[33]. After a lot of deliberations, contextualized discussions, and many amendments, the Council had solidly approved the law. The President of the country has given his agreement based on the legislation that year. As per the act, the aim of the legislation is based on preventing the illegal acts related to the information systems as well as offenses and mechanisms for the exploration, trial, and international collaboration. The Act presents a variety of crimes including illegal accessibility, broadcast, repetition, or intrusion in the information system or data[34]. Strict penalties were set for such crimes if they include the information systems or data related to the acute infrastructure. The Act even presents the crime of cyber-terrorism. A cyber-terrorist crime is a crime which is linked to acute infrastructure and is conducted with the intent of committing terrorism. The penalty for this offense according to this law is 14-year term of custody or a charge of Rs 5 million, which makes up US $47,450[35].

---

[29] Larsson, G., 2007. Cyber-islamophobia? The case of WikiIslam. *Contemporary Islam*, *1*(1), pp.53-67.

[30]Bukhari,Al Sahih,Chaper 15, P 258 Beirut Lebanon 1987

[31] Iner, D., Asquith, N., Ip, R.H.L., Islam, Z., Mason, G., Vergani, M. and Zayied, I., 2019. Islamophobia in Australia-II (2016-2017). Charles Sturt University.

[32] Ibd

[33] Mohammed, F. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. *UCLA J. Islamic & Near EL*, *15*, 71.

[34] Fraser, D. (2020). Small Nations Cybercrime Law: The Guyana Case.

[35] Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 241-250.

Even the support of terrorism-based crimes, hate speech, generating enrolment forms or funding, and planning with regards to the terrorism by any of the information systems or devices is indictable crimes as per this Act. This act emphasizes upon removing or blocking harmful information, and issues the directions for elimination or blockage of accessibility to the information by the information system, if it believes it to be be against the injunctions of Islam[36].

***Salient Features of the New Bill***

It was mentioned that for more than three years of imprisonment, there will be a fine of Rs1 million for unauthorisedly accessing the key infrastructure information system or any other data. The government may collaborate with the foreign government through 24x7 networks to investigate and proceed towards the evidence collection of the crime[37]. It is mentioned that for seven years, the fine charge would be Rs10 million for having a dishonest intention. If the identity information had been used while not taking any authorization, then according to the bill, the person can apply to the consultants for securing, destroying, or preventing the broadcast of the information.

***Criticism on Bill***

The bill was signed in terms of law through President Mamnoon Hussain. However, there were many critics of it. While Anusha Rehman, the IT Minister believed that the criticism based on the bill is groundless because the planned amendments are involved in it[38] there were many other foras which criticized it. Non-governmental companies, as well as civil society representatives, have opposed the bill because of a particular agenda. Ali Raza Abidi, the MNA of MQM thought that the government had to forcefully pass the bill with the use of the necessary force[39]. Naveed Qamar who was the PPP of MNA thought that the bill might be misrepresented through the authorities as well as government departments[40]. The 'draconian' bill was highly disapproved by the private sector IT industry, civil society companies, as well as civil rights activists for restricting human rights and providing the outwitting powers to the agencies of the law enforcement.

Critics thought that this bill is punitive, which tends to address the punishments which are excessive according to the crime[41]. They believed that the recommendations with regards to the key stakeholders were not taken into consideration while forming the law. It has restricted the freedom of countenance and accessibility to the information. The crimes are too abundant, overlapping with the other present laws. The wording with regards to the bill has left most of the clauses open for interpretation. The bill definitely can

[36] Ibd

[37] Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World. *Journal of Educational and Social Research*, *4*(6), 513.

[38] Ibd

[39]Baloch, H., 2016. Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016. *Accessed on 23rd June*.

[40] Kamran, A., ul Arafeen, Q. and Shaikh, A.A., 2019. Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), pp.241-250.

[41] Liaquat, S., Qaisrani, A. and Khokhar, E.N., 2016. Freedom of Expression in Pakistan: A myth or a reality.

be distorted for targeting the sources of the journalists and informers. Standards with regards to the surveillance are also quite open-ended in comparison to the Fair Trial Act of 2013[42].

Some critics of this law also believed that in the cyberlaw of Pakistan, pornography is not completely addressed. Since it is an Islamic state, it should have addressed this issue as well in the bill and must declare the punishment accordingly[43]. Section 13 with regards to the law has defined cyberstalking unclearly for incriminating anyone with the use of electronic communication determined to force, threaten, and annoy any person[44]. It gives the impeaching authorities a chance for using their discretion as well as declaring anything depraved and indecent.

While these criticisms may seem valid the following section of the article will dicuss the validity of this cybercrime law in the light of ever relevant Islamic injunctions.

The Islamic Concept of News

Dealing with the fake news with regards to the Islamic perspective is highly helpful for the betterment of lives. Islam strictly forbids spreading of fake news without authentic news sourcing. Fake news tend to evolve erratically on the online platforms as compared to the previous times[45]. In addition to this, the role of technology with regards to the growing risk of fake news in contemporary communication is mentioned in Islam. This context is well described in the given section.

Surah Al Hujraat and Communication Ethics

Surah Al Hujraat is quite helpful in understanding what communication ethics are and how a Muslim should benefit from them. Cybercrime is also related to the spread of fake news. Surah Al Hujraat declares that whatever had been the conduct of the non believers till then would be disregarded and pardoned by Almighty Allah if they mend their earlier habits of unsolicited gossiping in unethical ways. According to this surah, the foregoing behaviour that was giving distress to the Prophet (SAWW) needed to be be amended[46]. One of the primary injuctions in this surah is about the communication ethics. The spread of fake news is highly unethical. This Surah has focused on this key aspect. As stated in Ayat 6:

يٰٓاَيُّهَاالَّذِيۡنَاٰمَنُوۡٓااِنۡجَآءَكُمۡفَاسِقٌۢبِنَبَاٍفَتَبَيَّنُوۡٓااَنۡتُصِيۡبُوۡاقَوۡمًۢابِجَهَالَةٍفَتُصۡبِحُوۡاعَلٰىمَافَعَلۡتُمۡنٰدِمِيۡنَ

The believers who tend to get a piece of news from other people must carefully determine its authenticity, so that one may not hurt a person unsuspectingly[47]. This is the crux of this ayat which warns the people to be watchful and that they should not trust anyone's fake news easily.

Another ayat from this Surah mentions a case as per which the Prophet (SAWW) was uncertain for taking any armed action against Bani al-Mustaliq, a tribe who were reported to have denied paying alm giving

[42] Yamin, D., 2021. Cyberspace Management in Pakistan. *Governance and Management Review*, *3*(1).

[43] Ibd

[44] Ibd

[45] Al Seini, S. (1986). An Islamic concept of news. *American Journal of Islamic Social Sciences*, *3*(2), 277.

[46] Muna, M. K., & Subekti, M. Y. A. (2020). TUJUAN PENDIDIKAN ISLAM DALAM AL QURâ€™ AN [Kajian Surah Al-Hujurat Ayat 11-13 Tafsir Al-Munir Karya Wahbah Al-Zuhaili]. *Piwulang: Jurnal Pendidikan Agama Islam*, *2*(2), 167-189.

[47] Ibd

(Zakat). Some people were of the opinion that they must be attacked at once. However, when the matter was investigated it became known that it was a fake allegation against Bani al-Mustaliq. Therefore, the people were reminded that the Prophet (SAWW) was the one amongst them, who knew about Bani al-Mustaliq well than they did[48]. Thus, their mindset that the Prophet (SAWW) must act as per their counsel in significant matters was inappropriate. If he would have started acting as per their wishes, it might have led towards an anarchaic situation causing everyone to suffer. Therefore, at the end of the same Ayat mentioned above, Allah reminds us that confirming any piece of news that comes to us is a just way to conduct the affairs of human life and it is a blessing from Him. As is stated:

فَضۡلًا مِّنَ اللّٰهِ وَنِعۡمَةً ؕ وَاللّٰهُ عَلِيۡمٌ حَكِيۡمٌ

Hadiths and Communication Ethics

From the hadiths of Prophet Mohammad (SAWW), it came to know that,

***A Muslim should mind his own business*** *(Al-Muatta, 1604).*

This hadith is referring to that being a good Muslim, one should not interfere in someone's matters and leave all of their business activities on their own. It is prohibited by Prophet (SAWW) to be curious regarding someone else's business. In the modern times, therefore, it may be inferred that getting the information of a person without his/her knowledge from his or her computer systems is unethical[49].

Another relatable hadith is,

***Permission is for having a look***(Al-Bukhari, 5887).

It seems that the Prophet (SAWW) refers to not being a spy or putting his or her nose in someone else matters. Moreover, the others are not allowed to conduct any mischievous act to know the personal matters of a person or use his or her computer as it is their property. Such acts result in breaking trust and putting questions of loyalty[50].

**Findings**

E-crime in the existing world poses one of the key challenges for any law enforcing body. Information technolog has the double responsibility catering and protecting the interest of the individuals utilizing Web technology while being mindful of the cybersecurity laws. Such laws are derived from the collective laws as well as legislation that are applicable for universal crimes. There are more than one billion Muslims in the world, for whom, numerous calls have been made in the Islamic countries like Pakistan for the establishment of a law that is appropriate to deal with the computer crimes that are according to the Islamic Shariah law[51]. Under this section, substantiating Islamic injunctions about cybercriminal activities, an in-depth analysis is done taking into account the evidence from the Holy Quran, Hadiths, and the Sharia (Islamic Law and Jurisprudence).

[48] Dalimunthe, N. D. (2019). *Nilai-Nilai Pendidikan Islam Dalam Alquran Surah Al-Hujurat* (Doctoral dissertation, Universitas Islam Negeri Sumatera Utara Medan).

[49] Mansoor Al-A`ali , 2007. Computer Crime and the Law from an Islamic Point of View. *Journal of Applied Sciences, 7: 1558-1565.*

[50] Ibd

[51] Khan, S., Tehrani, P.M. and Iftikhar, M., 2019. Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. *Journal of Management Info*, *6*(2), pp.7-11.

Cyber Laws in Pakistan and Shariah

Cyber activities are being conducted by businesses, that involve the purchasing and sales of the products while using the credit card as well as digital cash. People tend to transfer the data among various companies with the use of networks, like the Internet. Furthermore, e-commerce refers to collecting the tools as well as practices including the Internet technologies which let the company create, sustain, and enhance the business relations with clients as well as the other businesses[52]. Technology has penetrated all corners concerning modern business. It tends to promise in terms of the concentrated costs, greater scales of the margins, more effectual operations as well as a greater amount of the profits.

However, some businesses have found a boundless place in terms of cyberspace with the provision of easy accessibility to the probable clients in the world, which may not have had, otherwise, any means to access business. While it is convenient to use technology, all the activities must meet the legal conditions provided through Shariah[53]. In Islamic law, if any prohibited element according to the Shariah is included, the formation of a contract on the Internet or in cyberspace is entirely illegal. This is actually a mindful reminder to human beings of the covenant that they have done with their Creator before even coming on this earth. Therefore, they need to fulfil all sorts of pomises and obligations that they have done with God Almighty or do with their fellow human beings. Consequently, a contract enforceable through law refers to an agreement. The Holy Quran reminds us:

***O ye who believe! Fulfill (all) obligations ('Uqud).***(Surah Al-Maida 5)[54]

Aqd is the singular of uqud in Arabic that refers to conjunction. It means to tie in between two ends both physically as well as morally. In Islamic law, the contract includes the overall field of a broad variety of obligations including also which are unworldly, social, political as well as commercial. Particularly, 'aqd means to meet the offer as well as accept in conformism with the convention that is given by the Shariah[55].

The formation of the contract on the Internet is a conventional business contract that tends to have essential amendments made for adapting to the cyberspace setting. Two individuals do not interact physically. They connect by the words while typing on the keyboard[56]. It refers to the alternative paperless media communication that is used in the case of face-to-face communication. There have to be two parties who must act as the offeror as well as the offeree. There has to be a valid offer that is recognized through a lawful acceptance for legal consideration, or else, no contract enforceable by the law may tend to exist. These are the cyber laws that are discussed in the light of Islamic teachings.

There is a general rule, which says that the acceptance should be communicated, and must be given acknowledgment for the contracts that are formed in cyberspace. As per the exclusive feature, any of the data message communication must be considered to be received when it reaches the information system of

[52] Khalil-ur-Rehman Khan, J.R., 2012. CYBER LAWS IN PAKISTAN.

[53] Ibd

[54] Iftikhar, S. and Saba, I., 2020. Blockchain Based Smart Sukuk as Shariah Compliant Investment Avenues for Islamic Financial Institutions in Pakistan. *Journal of Finance and Economics Research*, *5*(1), pp.30-45.

[55] Ibd

[56] Riaz, S., Hakeem, M.T. and Mahmood, M.A., 2014. issues that interest lawyers the world over. The journal is abstracted and indexed by ProQuest.

its envisioned recipient[57]. Thus, it is highly prudent that the offeror must involve in his offer a delivery that shows the acknowledgment of the receipt with regards to the offer. It has been narrated through Abu Daud, Ibn Majah, and Tirmizi from 'Amr Ibn 'Auf that Prophet (SAWW) stated,

> ***"Friendly settlement is allowed for Muslims except a settlement to forbid what is permissible or to approve what is forbidden, and Muslims are bound by their conditions except for the condition that forbids what is permissible or approves what is forbidden".***[58]

Thus the validity with regards to the contract, as per the Islamic contract law is subjective to four classes of conditions. It includes the conditions that are essential as the foundation for the formation of the contract, for instance, requiring the subject matter of the contract to be delivered. The second condition refers to a legal requirement to be fulfilled for the cogency of contract, such as the contract may not include gharar‌l (indecision)[59]. The third is the necessary enforceability of the contract, which refers to having ownership as well as a legal entitlement on the subject matter with regards to the contract. The last is the necessity of enabling the performance of the contract, which means the contract for sale must be free from bias.

Islamic Computer Crime Law Proposal

Under this heading, the Islamic laws based on cybercrime are discussed as per some of the key factors which must be taken into consideration while using computers or doing any cyber activity.

Privacy

ALLAH lays down some cardinal principles about human conduct in a given society in Surah Al-Hujarat of Quran. For instance, in ayat 29

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَلَا
تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ
لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ ١٢

> ***"O you who believe, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of repentance and Merciful".***
>
> And,
>
> ***"O, believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent."*** (An-nessa, 24)[60]

Therefore, Islam strictly forbids a person from poking his or her nose in someone else's matters unnecessarily behind one's back. One is not allowed to pry into others' privacy either physically or through

[57] Ibd
[58] Al-A'ali, M., 2007. Cybercrime and the law: An islamic view.
[59] Ibd
[60] Ibd

computers or the accessories with unlawful curiosity without taking previous permission[61]. Similar injunction may be seen in case of business matters as Prophet Mohammad (SAWW) states:

***It's prohibited to take the Muslim wealth without his complete permission***."

(Al-Baihaqi, 1994).[62]

There are, therefore, clearly laid down principles for a Muslim entity not to be even remotely involved in any cybercrime activities of spying, phishing Scams, website deceiving, ransomware, IoT hacking, etc. as all these results in the betrayal and interruption in anyone's private matters[63].

Trust

It is mentioned in Quran that,

"***One of the women said, "O my father, hire him. Indeed, the best one you can hire is the strong and the trustworthy***"[64] (Surah Al Qasas, 28:26)

This means that a person who is in knowledge of even someone's intimate information or a password etc. for some lawful need is a trustee for accessing a computer and must not give sensitive information to another person without taking permission from the key person. Muslims, as well as non-Muslims, must be treated equally in terms of trustworthiness. It is not surprising that this sentence is not referring to the culture or religion of a person but emphasizes on being truthful with everyone[65].

Allah also commands in the Holy Quran,

***"Give back the trusts to their rightful owners"***. (An-nessa, 58)[66]

The person is strictly forbidden to become a part of any of the activities that result in betrayal or denial. Allah has stated:

***"O, believers! Do not betray the trust of Allah and His Prophet, nor violate your trusts knowingly"***. (Al-Anfal, 27)[67]

This ayat reminds Muslims that they have to maintain trust and keep their promises. He or she must not indulge in such acts which verily result in harm to one's values, promises, level of trust, or to any personal belongings.

***Theft***

Islam prohibits taking other persons' property unlawfully. It is not allowed to attain the benefits with regards to the contents of a computer or by it while not having permission. Any action like this is theft.

ALLAH mentions in the Quran:

[61] Saba, I., Kouser, R. and Chaudhry, I.S., 2019. FinTech and Islamic Finance-Challenges and Opportunities. *Review of Economics and Development Studies*, *5*(4), pp.581-890.

[62] Ibd

[63] Ibd

[64] Surah Al Qasas, 28:26

[65] Rashid, T., 2011. Negotiating rights through transnational puritan networks: Religious discourses; cyber technology and Pakistani women. In *The Politics of Religion in South and Southeast Asia* (pp. 254-272). Routledge.

[66] Ibd

[67] Ibd

> ***"Male or female, whoever is guilty of theft, cut off their hand (that was used in theft) of either of them as a punishment for their crime. This is exemplary punishment ordained by Allah".*** (Al-Maaeda, 38)[68]

This ayat is not only applicable in the case of physical robbery or snatching but is also extendable to a deliberate and unprovoked instance of theft.[69] Cybercrime is one of those advanced ways that have let people get a chance of conducting criminal activities through a computer that works like a weapon which results in fraudulent or unlawful gambling[70]. The computer is being used for stealing unlawful information. The criminal deserves to get the same punishment as mentioned by Allah (SWT) in the Holy Quran.

***Promise***

Muslims must respect their relations and values. It means that it is forbidden to use other person's computer documents without permission. Muslims, as well as non-Muslims, are equal in this condition.

Prophet Mohammad (SAWW) has clearly stated that,

> ***"The signs of a hypocrite are three. Whenever he speaks, he tells a lie. Whenever he promises, he always breaks his promise. If you trust him, he proves to be dishonest. If you keep something as a trust with him, he will not return it."*** *(Al-Bukhari, 1987).*[71]

This Hadith clearly indicates that a person is a hypocrite who lies, breaks promise or trust. And a cybercriminal does all three wrongs besides other illegal activities. The one who does it ultimately will tell a lie for hiding his or her crime. Moreover, he or she will surely be breaking the promise of someone while spying on their personal belongings. If not, then the promise towards Allah (SWT) is surely broken as he is committing a crime[72]. Lastly, cybercriminals are dishonest because they intend to harm someone through the immoral act of theft or breaking promises.

**Recommendations**

Many reasons are there regarding cyber-crime activities. Criminals do this for their recognition and for making quick money. Moreover, one of the reasons is also the low marginal cost with regards to the online activity because of the global reach[73]. Based on this, it is recommended for the government of Pakistan to ensure that cyber bill 2016 is followed. Moreover, from time-to-time amendments in the law are needed as per the emerging problems. In being an Islamic nation, the government has to make sure that the citizens are abiding by the Islamic teaching and not committing any illegal cyber activity.

---

[68] Ibd

[69] The important thing to note here is that there are proper contexts of application of this punishment. However, it is a separate discussion out of the purview of this paper and would be discussed elsewhere.

[70] Abbasi, A., 2019. Islamization of Laws: The Role of media; from an impediment to facilitator. *Islamabad Law Review*, *3*(3&4), pp.44-62.

[71] Ibd

[72] Ibd

[73] Windiarti, I. S., Norcahyono, A. P., & Prabowo, A. (2020, December). Digital Literacy for the Millennial Generation in Industrial Revolution 4.0 Era in Islamic Norms Perspective. In *ICIC 2020: Proceedings of the 1st International Conference on Islamic Civilization, ICIC 2020, 27th August 2020, Semarang, Indonesia* (p. 467). European Alliance for Innovation.

## Conclusion

The contemporary challenges of cybercrimes and solution in the light of Islamic law while considering the cybercrime bill 2016 of Pakistan are discussed in this study. The digital age is here to stay and therefore, makes the need for a dynamic cybercrime legislation an imperative across all nation-states. However, there are many challenges to draft an all inclusive bill because it is a fast evolving situation in the cyber world. Technological growths are exceeding the solutions that are projected by the state institutions, addressing the new experiments related to cybercrime. However, Islam forbids all kinds of cybercrimes and warns the Muslims from spreading any such fake news, or utilize any sensitive information unlawfully, or do any felony that has any aspects of blackmailing. This has been supported through the Quranic teachings in this study. Thus, it is recommended that the government should endorse the ethical philosophy of Islam; must take action against the ongoing cybercrime, take strict action against such criminals, and work as vigilantly and effectively as the quick rise in cybercrimes.

## Bibliography

Abbasi, A., 2019. Islamization of Laws: The Role of media; from an impediment to facilitator. *Islamabad Law Review*, *3*(3&4), pp.44-62.

Al Seini, S. (1986). An Islamic concept of news. *American Journal of Islamic Social Sciences*, *3*(2), 277.

Al-A'ali, M., 2007. Cybercrime and the law: An islamic view.

Baloch, H., 2016. Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016. *Accessed on 23rd June*.

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems*, *41*(3), 669-682.

Dalimunthe, N. D. (2019). *Nilai-Nilai Pendidikan Islam Dalam Alquran Surah Al-Hujurat* (Doctoral dissertation, Universitas Islam Negeri Sumatera Utara Medan).

Fraser, D. (2020). Small Nations Cybercrime Law: The Guyana Case.

Hidayatullah, M.S., Dimyathi, M.S., Abdullah, Z. and Handayani, R., 2020. The Cyber Islam Contestation In Indonesia. *International Journal of Advanced Science and Technology*, *29*(7).

Iftikhar, S. and Saba, I., 2020. Blockchain Based Smart Sukuk as Shariah Compliant Investment Avenues for Islamic Financial Institutions in Pakistan. *Journal of Finance and Economics Research*, *5*(1), pp.30-45.

Iner, D., Asquith, N., Ip, R.H.L., Islam, Z., Mason, G., Vergani, M. and Zayied, I., 2019. *Islamophobia in Australia-II (2016-2017)*. Charles Sturt University.

Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 241-250.

Kamran, A., ul Arafeen, Q. and Shaikh, A.A., 2019. Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), pp.241-250.

Khalil-ur-Rehman Khan, J.R., 2012. CYBER LAWS IN PAKISTAN.

Khan, S., Tehrani, P.M. and Iftikhar, M., 2019. Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. *Journal of Management Info*, *6*(2), pp.7-11.

Kort, A., 2005. Dar al-Cyber Islam: Women, domestic violence, and the Islamic reformation on the World Wide Web. *Journal of Muslim Minority Affairs*, *25*(3), pp.363-383.

Larsson, G., 2007. Cyber-islamophobia? The case of WikiIslam. *Contemporary Islam*, *1*(1), pp.53-67.

Liaquat, S., Qaisrani, A. and Khokhar, E.N., 2016. Freedom of Expression in Pakistan: A myth or a reality.

Magutu, P. O., Ondimu, G. M., & Ipu, C. J. (2011). Effects of cybercrime on state security: Types, impact and mitigations with the fiber optic deployment in Kenya. *Journal of Information Assurance & Cybersecurity*, *2011*(1), 1-20.

Malik, H.A., 2017. Naqd Al-Hadits sebagai Metode Kritik Kredibilitas Informasi Islam. *Journal of Islamic Studies and Humanities*, *1*(1), pp.37-66.

Mansoor Al-A`ali , 2007. Computer Crime and the Law from an Islamic Point of View. *Journal of Applied Sciences, 7: 1558-1565.*

Mohammed, F. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. *UCLA J. Islamic & Near EL*, *15*, 71.

Mohammed, F., 2016. PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. *UCLA J. Islamic & Near EL*, *15*, p.71.

Muiz, A., & Gaffar, A. (2018, July). Study Living Qur'an: The Analysis of Understanding Surah al-Nahl (125) against Demonstration-Based Communication Behavior. In *IOP Conference Series: Earth and Environmental Science* (Vol. 175, No. 1, p. 012180). IOP Publishing.

Muna, M. K., & Subekti, M. Y. A. (2020). TUJUAN PENDIDIKAN ISLAM DALAM AL QURâ€™ AN [Kajian Surah Al-Hujurat Ayat 11-13 Tafsir Al-Munir Karya Wahbah Al-Zuhaili]. *Piwulang: Jurnal Pendidikan Agama Islam*, *2*(2), 167-189.

Mundiri, A. and Tohet, M., 2018. Contestation of Religious Identity in the Cyber World: A Case Study of arrahmah. com and VOA Islam Dealing with Religious Others on Facebook. *Walisongo J. Penelit. Sos. Keagamaan*, *26*(2), pp.391-416.

Nurse, J. R., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. *arXiv preprint arXiv:1901.01914*.

Possamai, A., & Turner, B. (2014). Authority and liquid religion in cyber-space: the new territories of religious communication. *International Social Science Journal*, 197-206.

Rantala, R. R. (2008). *Cybercrime against businesses, 2005*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Rashid, T., 2011. Negotiating rights through transnational puritan networks: Religious discourses; cyber technology and Pakistani women. In *The Politics of Religion in South and Southeast Asia* (pp. 254-272). Routledge.

Rehman, T. U. (2020). International Cooperation and Legal Response to Cybercrime in Pakistan. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 424-434). IGI Global.

Riaz, S., Hakeem, M.T. and Mahmood, M.A., 2014. issues that interest lawyers the world over. The journal is abstracted and indexed by ProQuest.

Saba, I., Kouser, R. and Chaudhry, I.S., 2019. FinTech and Islamic Finance-Challenges and Opportunities. *Review of Economics and Development Studies*, *5*(4), pp.581-890.

Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World. *Journal of Educational and Social Research*, *4*(6), 513.

Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World. *Journal of Educational and Social Research*, *4*(6), 513.

Smith, K. T., Smith, M., & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*.

Windiarti, I. S., Norcahyono, A. P., & Prabowo, A. (2020, December). Digital Literacy for the Millennial Generation in Industrial Revolution 4.0 Era in Islamic Norms Perspective. In *ICIC 2020: Proceedings of the 1st International Conference on Islamic Civilization, ICIC 2020, 27th August 2020, Semarang, Indonesia* (p. 467). European Alliance for Innovation.

Windiarti, I. S., Norcahyono, A. P., & Prabowo, A. (2020, December). Digital Literacy for the Millennial Generation in Industrial Revolution 4.0 Era in Islamic Norms Perspective. In *ICIC 2020: Proceedings of the 1st International Conference on Islamic Civilization, ICIC 2020, 27th August 2020, Semarang, Indonesia* (p. 467). European Alliance for Innovation.

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). Various Types of Cybercrime and Its Affected Area. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3* (pp. 305-315). Springer Singapore.

Yamin, D., 2021. Cyberspace Management in Pakistan. *Governance and Management Review*, *3*(1).