Competitive Social Sciences Research Journal (CSSRJ), 3(2), 151-158
ISSN (Print):2708-9029,ISSN(Online):2708-9037
www.cssrjournal.com

# Cyber War in a Cyber-Led World and Legislative Measurements taken by Pakistan

**Rashida Zahoor**
Assistant Professor, Department of Law, Bahauddin Zakariya University, Vehari Campus
***Muhammad Asif Safdar**
Assistant Professor of Law, Gillani Law College, Bahauddin Zakariya University Multan
**Waqas Rafiq**
Lecturer, Department of law, University of the Punjab, Gujranwala Campus
**Farhana Aziz Rana**
Assistant Professor, Department of law, University of the Punjab, Gujranwala Campus

*Email of the corresponding author: asif.safdar6@gmail.com

## ABSTRACT

*While cyber war is increasingly being referred to as a "fifth-generation warfare(5G)", Policymakers, legislatures and the general public are unaware of this development's legal and strategic consequences. This paper addresses some of the legal and strategic issues that arise when developing successful international and national policies for preventing, regulating, and resolving cyberwar. It is vital to examine the mutually constitutive link between the law, actual events on the ground, and the cyber war discourse in order to give critical information regarding the role of law in the governance of cyberwar. In Pakistan, military, political, and commercial entities are all pushing to bring cyber security challenges into the realm of conflict.*

***Keywords*:** Cyber war, E-Crime, Internet, Legislation, Pakistan

**To cite this article:** Zahoor, R., Safdar, M,A ., Rafiq, W & Rana, F,A (2022). Cyber War in a Cyber-Led World and Legislative Measurements taken by Pakistan. Competitive Social Science Research Journal (CSSRJ), 3(2), 151-158

## INTRODUCTION

Over the last two decades, the internet has become one our the basic needs of lives. Almost every person depends on it for daily life activities. The internet has revolutionised our lives and has brought more excellent connectivity. In short, it has reduced distances mainly. According to a rough estimate, more than a quarter of the world's population is a regular internet user. Social networking is now the flavour of the month without realising that people without procrastination share fragments of their identities, like date of birth etc., ideas like online shopping and giving your address to a stranger. Whatsapp users share their exact location leaving almost no doubt about where they are right now, and their

followers can quickly get aware of their precise location. A psychologist (Suler, 2004) gave a concept of the online disinhibition effect. According to this, people having severe disinhibition go opposite to what they actually are.

People are no longer afraid of their real identities so they can leash their demons. These types of communications lead their way to crimes because fear of being known as a criminal in society is lost. The main reason for cybercrime is not the internet but its potential to facilitate crime(Williams, 2008). As compared to the traditional crimes, the reactions to cybercrimes are different. There are many factors for it, including that public and political systems do not directly influence cyber as they usually do in society(Hinduja, 2007). Moitra defines cybercrime as "Any Unauthorised, deviant, or illegal activity over the internet that involves a computer as the tool to commit the activity and a computer as the target of that activity" (Moitra, 2005).

For a cybercrime, three things are necessary. Firstly, a computer from which criminal action originates; secondly, A computer which is a victim; thirdly, An intermediate network. The expeditious growth of computer usage and the internet has necessitated governments to address the demand for safety on the ways of internet highways. The concurrence of computing and the immense growth of internet technologies has benefits as well as risks. The exceptional development and advancement of cyber it has also brought vulnerability. The immense use of technologies and growing dependence on internet have brought greater risks. And these risks need a continuous check and require specific attention on all sides. These sides comprise national and international aspects. Controlling crime is never easy; when it involves a computer, it becomes more complex. To prevent crime on internet, require more networks. That means a network between crime controlling agencies of government like police and other agencies that work for the state's security. It will also require more outstanding networking between private agencies not only within state borders but across borders also. Because cyber has vaporised the borders, a cybercrime will influence without any demarcation of the border. The awareness of cybercrime has begun and developed in the past decade mainly. And many states have made significant progress in their response to cybercrime, and they have developed the capacity of police to respond timely and efficiently to cybercrime. As much as this awareness is encouraging, there is still a long road to success.

The latest international developments regarding this cybercrime involve the convention on cybercrime CETS No: 185 made by the Council of Europe(Council of Europe, 2004). And the second development internationally is the United Nation's convention against transnational organised crime. Its scope is over the globe dealing with criminals when cybercrime is carried out internationally through criminal networks and involves serious crimes. The increasing international need led to the UN draft in 2003 in the General Assembly 58th session to address this problem globally(Rahman, Ahmed, Rahman, & Hoque, 2011).

**Challenges**

Agencies enforcing the law in states have not been able to cope with cybercrime effectively. Now, the 'jacking' of web pages is a frequent threat that companies face. And it is one of the most effective ways of stealing the identification of customers. The same thing happened in China when a duplicate site of 'Hong Kong and Shanghai banking and

corporations' online banking stole customer identification and was termed cyber theft. A 14-year-old boy was convicted for creating false site and placing false information that led to panic in the Hong Kong community (*HKSAR v Sum CheukWa, FLS 700017*, 2003). Nowadays, forensics specialists face new kinds of challenges every day while investigating cybercrime because such software has been made that are specialised in stealing personal information like identifications and use of more complex codes and high use of encryptions, making it near to impossible to get any evidence. One of the many problems is that victims of such crimes are either unwilling to come in front or even sometimes they are unaware that they have been victimised. The availability of new methods of controlling other computers has also increased a large number of cybercrime.

Many countries still do not have highly developed information and technology sectors, so they automatically lack in the field of defence from all problems it brings along. According to the report of the UN in 2000, the statistics of network users in different regions are different. It is more significant in regions like Europe and America but less in regions like Africa and Asia. The concept of the 'digital divide' can easily be observed in Asian countries where Singapore and Hong Kong, on the one hand, are heading ahead in the field of telecommunication, and on the other hand, Cambodia and Mongolia had less than 1% of their population connected(Davis, 2012).

**Terrorism in cyber**

A few years back, it was a threat in the back of minds in all states that terrorists may use information technology for their purposes. But now, it's no more a mere apprehension. We all see with our very eyes how the terrorists are using and applying the latest technologies in their missions. And soon, it all will be done with the help of the internet. It creates a big threat to the sovereignty of states. States not only have to defend on borders but in cyber fields also. Now comes the point of prevention from cyber-terrorism; this again is a big challenge because the technology drafted for the prevention is equally vulnerable and can also be attacked.

Moreover, instead of preventing a terrorist attack, they can be used to aid in it. It is how delicate and complex it's becoming. Terrorists use computers and cellular phones to plan their attacks well; on the other hand, the agencies working against them are also highly equipped to compete with them. Cases have been seen where either terrorist abducts higher officials and put them under the influence to extract or manipulate secret information. After the incident of 9/11, governments and states have become more conscious about these attacks. Now governments try to adopt more innovative methods to check on activities and try to hinder them as well.

**Criminality**

Industries and market consumers are closely linked with the governments, and increased internet dependency have made them vulnerable to this cybercrime threat. The most familiar term in cybercrime is 'viruses'. In 2004 viruses were named 'Norvag" and 'MY doom'. It was in combination with the effects of worms as well. It spread widely on the internet and caused shut off services. As a result, the targeted computers came under the influence and were easily commanded to act. Cybercriminals now operate through various chat rooms and proliferate. For any act to be termed as criminality or criminal, it must fulfil

some basic concepts like there must be an offender, a victim, injury or violation of right. Moreover, it should b condemned as a crime by the state legislature.

**What is Cybercrime?**

The consequences of cybercrime and cyber activities can be summarised as the first, including conventional cybercrimes in which computer are the main instrument of offence, such as intellectual property theft. The traditional type of cybercrimes in which evidence is there in digits are

- Interruption in lawful computer usage
- Cyber terrorism: Insertion of different cyber viruses for interruption of internet services
- Offensive materials provision
- Online treason, pornography, the context for racism etc.
- Stalking
- Forgery
- Offences related to copyrights, identifications etc.
- Fraud
- Fraud in the transfer of e funds
- E-money laundering

**Threats**

The task of bringing cyber criminals to justice has proved to be a more significant challenge for law enforcement agencies throughout the globe. Sometimes it's also seen that criminals tamper with the evidence at the crime scene. Most important scholars of crime prevention, Newman and Clarke in 2013, provided a review on cybercrime prevention in e-commerce(Newman & Clarke, 2013). According to them, the commission of online theft keys are trust and manipulation of identity. 'Crime is an opportunity when following conditions combine in place and time, motivated and tempted offenders, tempted targets in the absence of effective guardians'. Whenever such opportunities happen, crime is doomed to occur. To reduce cybercrime, law enforcement agencies need to understand the concept of availability and opportunity for crime. Moreover, the pathways that lead to such opportunities. No doubt, one of the crucial factors is to obtain trust in e-commerce dealings. The risk of attention is more significant in the post-transaction phase when the goods have to be delivered to the customers who had paid online and at that time risk of fraud is much higher.

**International Dealing**

In 2001, the Council of Europe passed a convention regarding cybercrime that activated cybercrime and its prevention(Council of Europe, 2001). The convention addressed issues like cybercrime involving racism, xenophobic cybercrimes, hate speech, and pornography mainly of children.

In dealing with cybercrime, we need to know that the government needs to be vigilant, and that international cooperation is also vital. Because while committing a crime through the internet, boundaries do not exist anymore. Cybercrime brings along with it the problem of jurisdiction. Mostly the victims of a single offence belong to different countries involving cases of copyrights and virus attacks. This again brings another conflict of jurisdictions where there is a conflict. It should be kept in mind that the primary purpose is to bring the offender to justice, and the method adopted shall be such as to avoid maximum prosecutions and any sort of inconvenience to the witnesses(Bullwinkel, 2005).

There must be some immediate summary to be taken

- Improvement in awareness regarding security
- Improvement in coordination between private and government sectors
- While advancing with new technology, it should be kept in mind that the new technology must not supersede the law
- Offenders must be condemned and criminalise with no general exception for juvenile offenders
- One of the very important steps in strengthening international relations through better harmony, treaties, and agreements
- Development and production of highly skilled men and equipment that are ready to face any sort of challenge

**Cyberwar**

In the near future, criminals will recruit IT specialists to do their jobs without the threat of being caught. Terrorism and war can easily be done by means of the internet. Computers can be automated, and they can be artificial intelligence to attack at specific times and place without any involvement of humans directly. Such attacks will be severe in nature. Drone attacks can be considered as the initial phase of cyberwar. These attacks are by remote, so national sovereignty is disregarded. With many risks of internet also comes the opportunity of contacting with police efficiently example of which is an online complaint centre.

**Cybercrime in Pakistan**

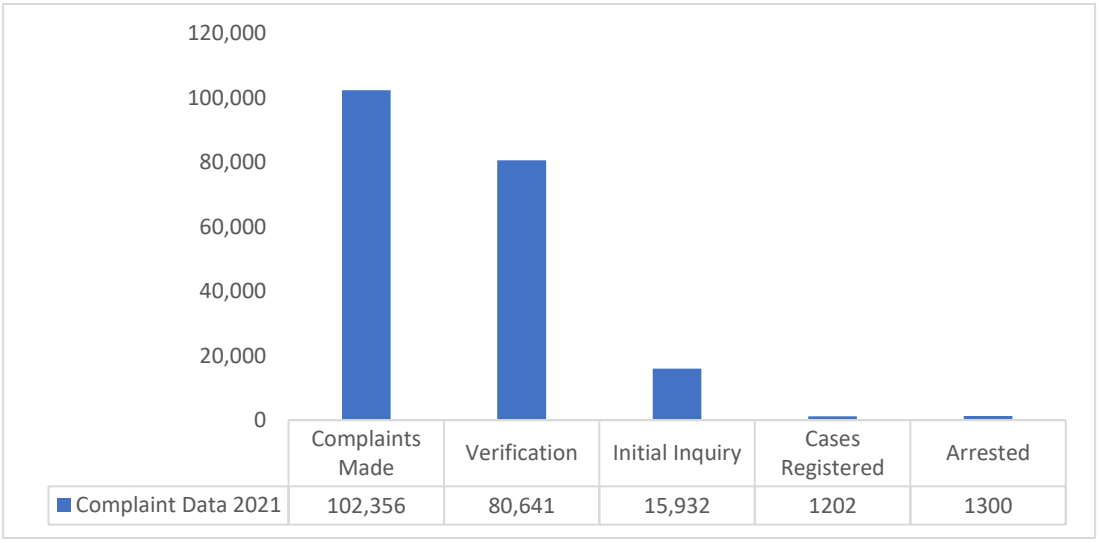
In Pakistan, the quest for cybercrime law mainly arose when Bolo Bhai filed a petition in Islamabad against the inter-ministerial committee for the Evaluation of websites (IMCEW) for their legality. After filing the petition, they found out that (IMCEW) has no legal standing for giving orders to block contents from sites. And they were giving orders even though the content was not blasphemous or pornographic. The (IMCEW) was banned because courts realised the fact that the body is totally unconstitutional. PTA was given the authority to manage online content. And PTA was issued power by law for which the need for cybercrime law arose.

Under the Federal Investigation Agency (FIA), a Cybercrime Wing (CCW) was established in Pakistan under the Prevention of Electronic Crime Act (PECA), 2016. CCW is concerned with the rising risk of cybercrime. This high-tech crime-fighting team was formed in 2007 to identify and combat the phenomena of technology misuse in Pakistan. It is Pakistan's only organisation of its sort, receiving complaints directly and taking legal

action against cyber offenders. CCW is dealing with various cybercrimes. Figure 1 Shows the crimes dealt with by CCW(Federal Investigation Agency, 2007). Figure 2 shows the complaint data for 2021(Dawn, 2022). According to the data, in 2021, 80,641 of the 102,356 complaints received were verified, and 15,932 met the requirements for initiating inquiries. Over 1,300 arrests were made after 1,202 charges were filed under relevant parts of the PECA.

**Figure 1:** Crimes dealt by CCW


**Figure 2:** Cybercrime Complaints Data 2021



## Legislation for Cybercrime in Pakistan

Before the Prevention of Electronic Crimes Act, 2016 no proper law existed in Pakistan that would criminalise the cybercriminals(Prevention of Electronic Crimes Act, 2016). It was the first to be enacted of such nature. It was enacted to prevent unauthorised acts concerning information systems and provide for related offences and mechanisms for their investigation, prosecution and trial. Moreover, international cooperation was made in order to avoid cybercrimes.

## Recommendations and Conclusion

So it is evident that many countries have addressed this issue either by national or international enactments, but the risk is up high that still no solid enactment or a way out has not been found. Countries are trying their best to learn new technologies because they do not want their conflict countries to supersede them. But in this quest, they are forgetting what is at stake. Government, markets, industries even the very personal life of every citizen is at risk. Moreover, if no proper solution is found, and the lust for power keeps on increasing, it will only cause destruction of our future.

While enacting a law, it shall also be in the minds of legislatures that the new cyber law shall be made to facilitate people and not to snatch away their fundamental rights. New methods and proper bodies should be made to deal with these types of situations especially, and the police department should not be burdened with it; rather, separate forces should be made. International dealings should be such that if there is an offender who has absconded or is about to abscond into a different jurisdiction, the government of that jurisdiction should help capture him. Our law enforcement agencies are not prepared for equipment or skills. Manpower, proper training, and proper equipment are required to deal with such a situation. Legislation should be done with the complete application of mind. Violation of rights makes a law, not a good law. For this, more and more research should be done. Experts in this field should be consulted for their opinion. Basic criminology theories cannot be adopted here because the person doing such activities is behind the screen. And for cyberwar, every state must be prepared. Moreover, the security of citizens on internet should also fall under the duties of the state as it does the defence of its citizens on borders.

## References


Bullwinkel, J. (2005). International cooperation in combating cyber-crime in Asia: Existing mechanisms and new approaches. *Cyber-Crime: The Challenge in Asia*, 269–302.

Council of Europe. (2001). Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Council of Europe. (2004). Convention on Cybercrime. Retrieved from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*.

Dawn. (2022). Cybercrime Complaint Data 2021. Retrieved from

https://www.dawn.com/news/1667248

Federal Investigation Agency. (2007). Cyber Crime Wing. Retrieved from https://fia.gov.pk/ccw

Hinduja, S. (2007). Computer crime investigations in the United States: leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology*, 1(1), 1–26.

HKSAR v Sum CheukWa, FLS 700017 (2003).

Moitra, S. D. (2005). Developing Policies for Cybercrime-Some Empirical Issues. *Eur. J. Crime Crim. L. & Crim. Just.*, 13, 435.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Willan.

Prevention of Electronic Crimes Act. (2016). Retrieved from https://na.gov.pk/uploads/documents/1470910659_707.pdf

Rahman, M. M., Ahmed, F., Rahman, M. O., & Hoque, A. (2011). Settlement of cyber disputes through terrestrial provisions: Law and technology converge in the US practice. *Journal of International Trade Law and Policy*.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 7(3), 321–326.

Williams, K. S. (2008). Using tittle's control balance theory to understand computer crime and deviance. *International Review of Law, Computers & Technology*, 22(1–2), 145–155.