March 2022, Vol. 10, No. 1
ISSN 2163-758X

Cybercrime: An Emerging Global Challenge for the States

Maria Kanwal, Qurat Ul Ain Zahoor, Saira Mussarat, Dr. Nadia Khadam, Ms. Zainab Iqbal

Fatima Jinnah Women University Rawalpindi, Pakistan

Abstract

With an ever-increasing use of the internet and technology, cyber crimes have become a crucial global concern. Cybercrimes refer to all the illegal activities carried out using technology. It is buying and selling of malware, and individuals' personal information illegally. This research focuses on different types of cybercrimes, such as hacking, cyber pornography, and cyber terrorism, etc. Cybercrime not only affects personal, business information, and Intellectual property but also damages reputation. According to the CSIS report, 2,299,682 cases of cybercrime are reported in 2020 and as a result of financial embezzlement carried out on the internet, individuals and the government had lost more than 1 trillion dollars per year around the world. Cybercrime has a direct and significant impact on jobs, innovation, economic growth, and investment. This paper strives to find out the causes of cyber perpetration and also suggest measures for its control. Cybercrime can be controlled by implementing digital and physical security methods, maintaining asset lists, patches, and updates, etc. This paper suggests a system of administrative regulations backed by criminal penalties that will provide the reason necessary to create a workable deterrent to cybercrime.

Introduction

Crime and criminality have been linked to man from the time of his creation. People of different eras adopted different methods according to their approach, to connect themselves with a crime. (Dashora, 2011) With the increasing use of the internet, especially in the pandemic era, people are suffering from cyberattacks globally. Cybercrime is an activity that involves using or targeting a computer network or network device to carry out activities that damage one's money or image. Cybercriminal activities are carried out for personal, political, or monetary reasons. Cybercrimes may include illegal intercepting or stealing data, infringing copyright, selling illegal items online, producing or processing child pornography, and more. (McGuire *et al.*, 2013). The benefits which are brought by the rapid expansion of the internet are accompanied by crimes that have a devastating effect on our individual and collective life.

1. Definition of Cybercrime

Cybercrime is committed by using a computer, another digital network or other forms of information communication technology either as a tool or to target a victim. These crimes are committed online, which is the reason why the prefix *cyber* is attached to *crime*. (McGuire *et al.*, 2013). The three categories of cybercrime are a crime which targets a computer device, e.g. to gain access and then spread the malware to the whole network; a crime that uses the computer as a weapon, e.g. using numerous compromised computers to carry out malicious activity known as distributed Denial of Service; a crime that uses the computer as an accessory to crime, e.g. using a computer to save illegal data. (Sarre *et al.*, 2018)

March 2022, Vol. 10, No. 1
ISSN 2163-758X

A cybercriminal mainly chooses countries with weak cyber laws to carry out their activities to reduce the chance of detection.

2. Types of Cybercrime

a. Malware Attacks

Malware is a virus or code delivered over a network to infect or steal information from the network by the hacker. A computer compromised by malware could be used by cybercriminals for numerous purposes. (McGuire *et al.*, 2013)

b. Phishing

Phishing is fraudulent communication that appears to come from reputable sources. It aims to steal a person's login information and personal data or to affect the person's computer. It fools the victim by presenting information that is from some trustworthy site and compels the user to share their personal information. (Hong, 2012)

c. Software Piracy

It is the illegal distribution, selling, use, installation, and copying of software. It is usually done by end-users and dealers. This causes a serious hindrance to the success and progress of the software industry globally. (Hinduja and Behavior, 2008)

d. Credit Card Fraud

Credit card fraud involves any crime using a credit card. Cybercriminals use credit cards to get information from a person's bank account. More than 270,000 cases of fraud were reported in the year 2017, according to the Federal Trade Commission. (Ramdinmawii *et al.*, 2014)

e. Cyber Pornography

Cyber pornography is the publication, distribution, importation, and designing of pornography through cyberspace. As the internet is easily available, people can view and upload pornographic videos easily. Child pornography is increasing at a rate of 3 million cases a year. One of the factors includes the accessibility of these websites. It is estimated that more than 10,000 Internet locations provide access to these materials nowadays. (Ramdinmawii *et al.*, 2014)

f. Identity Theft

Identity theft is the theft that includes the stealing of personal information of someone and then using that information in crime. This personal information gives access to bank accounts credit cards or other accounts. The graph below shows the identity theft complaints data over five years. (Roberds and Schreft, 2009)

March 2022, Vol. 10, No. 1
ISSN 2163-758X

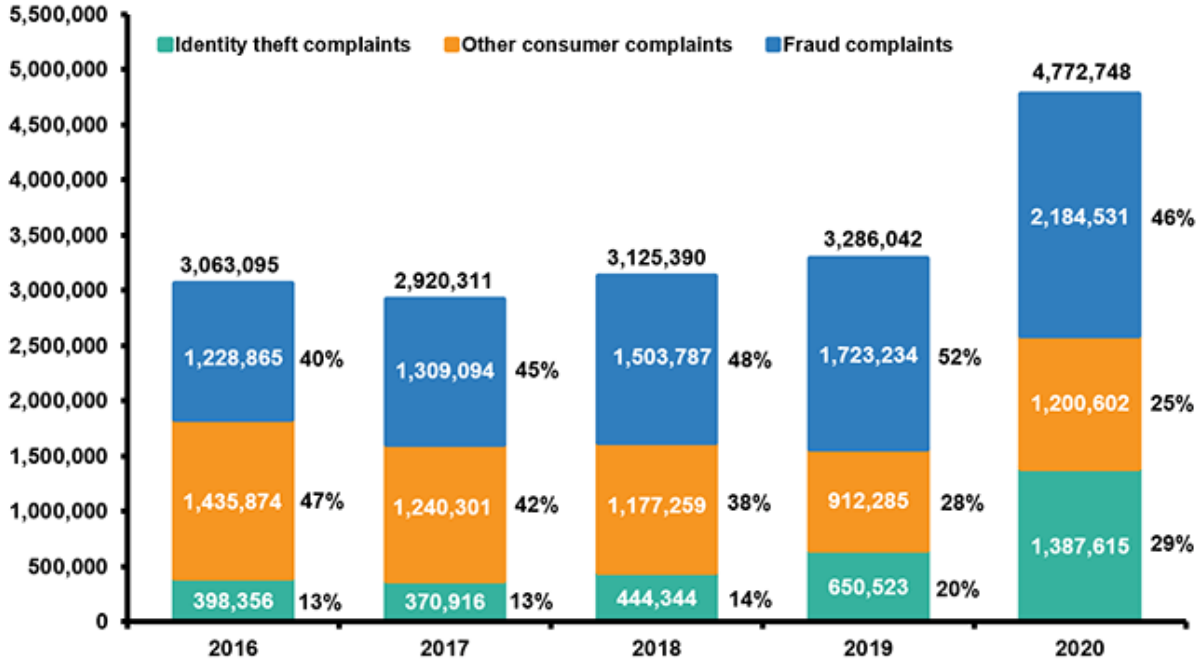

Figure 1: *Source: Internet Crime Complaint Center, Facts + Statistics: Identity Theft and Cybercrime, 2021*

3. Cybercrime Techniques

Some of the most common techniques which cybercriminals use to access personal or private computers are:

a. Botnet

It is the network of interconnected devices that are infected by malware in a way that these devices are in a hacker's control. Cybercriminals first gain access to botnet devices with the help of special viruses called trojans and attack the computer security system taking control of software and implementing commands and carrying out large-scale malicious activity. (Tyagi and Aghila, 2011)

b. Zombie Computer

A zombie is a computer connected to a network that is hacked by criminals to gain access to a private network. The computer is then used for a malicious task. (Broadhurst, 2010)

c. Distributed Denial of Service (DDoS)

The main focus of a DoS attack is to overload the targeted machine with junk data, resulting in Denial of Service to additional requests. DoS attack is of two types: a buffer overflow attack and a flood attack. (Hasbullah *et al.*, 2010)

d. Metamorphic Malware

One of the more advanced techniques, metamorphic malware, repeatedly adjusts its code, making it extremely difficult to detect by even the most advanced anti-virus software. (Walenstein *et al.*, 2007)

March 2022, Vol. 10, No. 1
ISSN 2163-758X

4. Statistics Related to Cybercrimes

a. In 2020, 60% -70% of businesses have been the victims of cybercrime, which made the thousands of companies suffer millions and led to the closing of these businesses. (Lazic, 2021)
b. By the year 2021, half a million zoom passwords were available for sale in dark web crime forums at the time when the whole world was using zoom for business or educational purposes.
c. Cybercrime statistics show that there is a rise in security breaches from the year 2018 to 19 and mostly to small businesses.
d. Cybercriminals attack someone online every thirty seconds and in this way, the rate of cyberattacks is 2244 times per day, with numerous attacks on the healthcare industry. In 2020 and 2019, data breaches affected 300.6 million people, and 887.3 million people respectively.
e. Likewise, attacks using emails or texts for provoking people to give their personal information are about 44%; 18% of cyberattacks are due to ransomware and 12% are due to malware. (Lazic, 2021)
f. The health care industry and finance industry are usually bigger targets of cybercriminals because they contain a large number of personal information and numbers.
g. In 2019, the health care industry lost $25 billion to ransomware attacks. In the past three years, more than 93% of health care industries experienced a data breach.
h. Financial services have 352,771 exposed sensitive files on average, which are open targets to cybercriminals, while healthcare, pharma, and biotech have 113,491 files on average. (Sobers, 2021)
i. Of the total of cybercrime breaches in the industrial sector, 56% of them are social media breaches, 27% are in the governmental sector, other industrial breaches include 8%, retailers include 4% and technology include 4%.
j. $18.3 million per company is spent on the financial service industry to combat cybercrime. (Morgan, 2020)
k. Cybercrime complaints also increased and the figure reached 791790 in the year 2020.

March 2022, Vol. 10, No. 1
ISSN 2163-758X

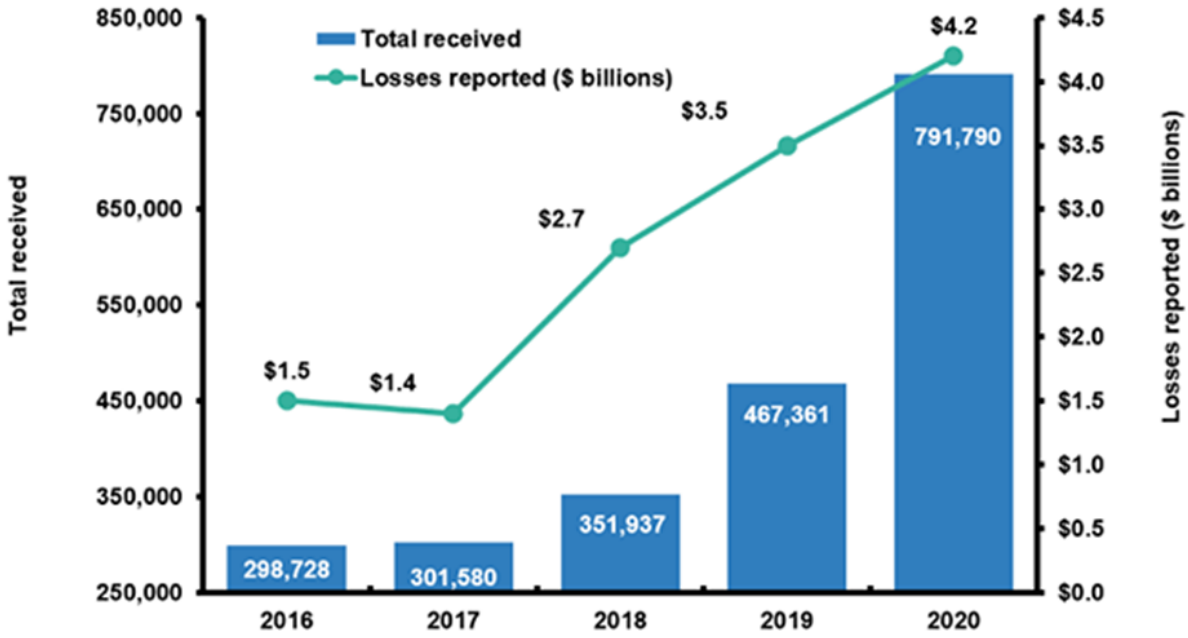

Figure 2*: (Source: Internet Crime Complaint Center, Facts + Statistics: Identity Theft and Cybercrime, 2021)*

5. Challenges for the States

Nowadays, states are facing many challenges to prevent cybercrime. In modern states, technology advances very fast. Because of this technology, where people are benefiting a lot on one hand and misuse it on the other, states face difficulties in protecting national and international safety. The rise in cybercrime cases in recent years has raised new challenges for states to combat cybercrimes if they want to eliminate them the threat. Some challenges are discussed below:

a. Investigation of Cybercrimes

The nature of cybercrime is complex and difficult to understand. A complex investigation is required for the prosecution of cyber cases. The gathering of authentic proof is needed if legal action against cybercriminals is to be initiated. State investigating agencies have faced difficulty in finding the basic source of information. Law enforcement units also face difficulty in applying cyber laws and selecting methods to investigate this digital crime. It is more difficult when the criminal is an outsider because they are not under the jurisdiction of the state. Therefore, help from International Law is needed in such situations. (Serwanga, 2019)

i. Investigation Method and Its Trans-Border Nature

Cybercrimes can be committed from any place and against anyone who is using the internet worldwide. For proper investigation of cybercrime, the criminal activity must be tracked across different national borders. Investigations may be carried out at an international level. The internet experts who are providing internet service all over the world may be the part of investigating team for effective investigation of crime. (Kasper and Laurits, 2016)

March 2022, Vol. 10, No. 1
ISSN 2163-758X

ii. ***Mishandling of Electronic Evidence***

Investigators are inexperienced in collecting digital evidence according to admissibility rules. That is why, courts reject improper electronic evidence, which is the important basis on which further cases might proceed. Sometimes electronic pieces of evidence related to cybercrime are easily deleted or stolen by criminals because of the lack of internet experts in courts and Cyber Crime Units. (Antwi-Boasiako and Venter, 2017)

iii. ***Failure to Protect the Chain of Digital Evidence***

During the prosecution of cybercrimes, the pieces of evidence are passed among various institutions to check the validity of evidence, but due to lack of experts and the nature of the evidence, they are rejected or easily changed by cybercriminals to decrease their validity. There is a need for time to manage the digital evidence. Our courts and investigating teams must find different and innovative ways to handle the large amount of electronic evidence. (Roscini and Law, 2016)

iv. ***Lack of Modern Instruments for Investigation***

Internet-specific tools are required for the investigation and proceeding of cyber cases and only these instruments can help investigators to carry out an investigation. Specific modern tools are required for the proper investigation of this crime. During the fight against cybercrime, we face unique challenges that need special attention from both investigators and lawmakers. The main challenges are the unavailability of guidelines on how to collect pieces of evidence and how to present these pieces of evidence in courts, day-by-day development in technology, and the use of hacking techniques by criminals. Police are poorly equipped to understand cybercrimes and they do not know how to investigate cybercrime cases. (Moore, 2014)

v. ***Speed of Data Exchange Process***

The internet has made it possible for people to communicate between the two countries in a matter of seconds and is the main reason for the success of the Internet. Criminals easily take advantage of this facility of the internet and exchange data from one place to another. That is why there is a problem in investigating cyber cases and real pieces of evidence are lost and the culprit easily escapes. The invention of the internet has left our traditional investigation process far behind. There is a need for time to speed up our investigation processes if we want to get rid of cybercrimes. (Losavio *et al.*, 2018)

vi. **Absence of One Universal Law Governing Cybercrimes**

This type of crime is committed in one country but has had effects in other countries. Cybercrimes are borderless, international, and global crimes that are committed in cyberspace. The laws for cybercrimes are either national or regional and are not applicable at the international level or outside of the specific region. (Weber, 2003)

The extradition process is a challenge due to the absence of universal law. Many countries do not extradite cybercriminals to other countries, making it a major challenge to enforce cybercrime laws around the world. Each country has its jurisdiction and it is the biggest impediment to the extradition of criminals to other states, because states deny extradition of the criminals to requesting states although they do have jurisdiction to take action against criminals. The requested country cannot do anything unless another country sends its criminals there. Due to the absence of one universal law, it is a challenge for one state to punish those criminals who are not citizens of that state but sit in their state and commit crimes that harm this state. (Ajayi and Systems, 2016)

March 2022, Vol. 10, No. 1
ISSN 2163-758X

b. Lack of Effective Reporting of Cybercrime

Many women who fall victim to these crimes are reluctant to report these cases because they think that doing so could bring them disrepute. Even great leaders of society, parents, and intelligent people prefer to settle these cases out of court. (Menon and Siew, 2012)

i. Limited Reporting of Crime

It is important to report a case first before investigating as it may be the first step. If it is not reported, then it will not be investigated, and the fact is that many cases around the world are not reported. Only a limited number of cybercrimes are reported because people are not taking them seriously like other crimes, due to which the culprit gets more support and that is why cybercrime is increasing. (Bidgoli *et al.*, 2019)

ii. Lack of Trust in Reporting Methods

There is no guarantee of confidentiality during reporting of cybercrime. People are afraid of reporting cybercrime because they cannot trust the reporting methods. Many cases are not reported because of security issues, as people are afraid of being exposed in front of the public which will damage their business and respect.(Brenner and Schwerha IV, 2007)

c. Challenges for Businesses

Whenever a person starts a business they get so busy that they forget about cybercrime. If they have not considered their company's cybersecurity needs, their business and customers could be at risk. Nowadays businesses are done online, which increases the risk of cybercrimes. So far, many businesses have been affected by criminals through the internet by their data being hacked or their business ideas being stolen. (Teng, 2017)

i. Increase in Costs

Many companies spend a lot of money to protect themselves from online theft. Spending a lot of money for protection damages their business a lot. (Bernik and Security, 2014)

ii. System Malfunction

Along with financial losses, companies also face some challenges indirectly from cyberattacks. Since today all the data of every company is online, a cyberattack changes their entire system of working causing them a lot of problems that can result in lost profits. Cybercrime uses all sorts of tactics to stop company activities. Computers are hacked by inserting malware that removes all valuable information and installing malicious codes on the server which deprives them of access to their websites. (Yeboah-Ofori *et al.*, 2019)

iii. *Changing Business Methods*

After a cyber-attack, many companies are forced to think about how they can restore their information and customers' trust. It is difficult to convince customers that the information they provide will not be leaked. As a result, companies stop taking their customers' data. When companies feel they cannot protect themselves from further cyber-attacks they shut down their online business, suffering huge losses.

iv. Damage to Reputation

A company that is a victim of a cyber-attack cannot prevent its brand from being destroyed. It is very difficult for both the supplier and customer to have their sensitive

March 2022, Vol. 10, No. 1
ISSN 2163-758X

information in the hands of a company whose IT set-up was broken or hacked at least once before. They feel less secure. (Speer and change, 2000)

v. Decreased Income

The worst consequence of a cyber-attack is a drop in income. Customers choose the products of other companies to protect themselves from cyber-attacks. Companies waste a lot of money trying to catch hackers. Because of this, their revenue is greatly reduced. (Okeshola and Adeta, 2013)

vi. Stealing Personal Thoughts

The most valuable thing about a company is its ideas, its technology, and its market plans. And all this intellectual property is stored in the cloud, where it is most at risk of cyber-attacks. (Prakash *et al.*)

6. Steps Taken by IGOs, NGOs & U.S. Government Agency Resources

Below are some steps taken by different governmental agencies to deal with cybercrimes.

a. International and Inter-Governmental Organizations

The Council of Europe has established the "European Cyber Security Organization", the main function of which is to act against cybercrime.

Below are the two main functions performed by this organization:

i. assisting countries in strengthening their criminal justice systems to meet the challenges posed by criminals operating in cyberspace.
ii. Sponsoring an annual cybercrime conference.

b. International Criminal Police Organization (Interpol)

Interpol's core mission is to enable law enforcement agencies in its 190 member countries to work together to fight against transnational crime, including cybercrime, and crimes related to children. In addition to serving as a hub for data exchange and intelligence sharing, it also supplies technical skills, instructions, and capacity building.

c. International Telecommunication Union

The ITU is a specialized organization of the United Nations that promotes the harmonization of technical standards for information and telecommunications technologies. It also encourages international cooperation to improve cyber security through its Global Cyber security Agenda and its partnership with UNODC (United Nation Office on Drugs and Crime). In addition, the ITU has affiliated with UNICEF to publish Guidelines for Child Online Protection. (Levin *et al.*, 2013)

d. Non-Governmental Organizations

i. Spamhaus

This international non-profit company based in London and Geneva tracks cyber hazards (spam, phishing, malware, and botnets) and delivers real-time, actionable threat intelligence to all network operators, corporations, and security vendors. For the

March 2022, Vol. 10, No. 1
ISSN 2163-758X

identification of spam and malware resources, it is also working with various law enforcement agencies worldwide.

ii. Internet Watch Foundation

This Internet Watch Foundation (IWF) is a UK-based, industry-funded non-profit organization. Their works are to firstly recognize, locate, and remove/delete online pictures and videos of child sexual abuse with the help of law enforcement agencies worldwide.

iii. The European NGO Alliance for Child Safety Online

Funded by the European Commission, the executive arm of the EU, it has offered a platform for child protection NGOs throughout Europe to share various expertise and best practices on policy matters related to the online safety of the child. (Taraszow, 2013)

iv. National Cyber Security Strategy

To create a comprehensive and effective national cyber security strategy, the 2018 ITU Guide to developing a national cyber security strategy proposes the inclusion of the following thematic areas in the strategy:

1. Governance
2. Risk management (i.e., the process of identifying, evaluating, and controlling or eliminating threats)
3. Preparedness and resilience
4. Capacity and capacity building and awareness-raising in public
5. Legislation and regulation
6. International cooperation

Other organizations have also guided the evolution of cyber security policy and regulatory frameworks, technical and organizational measures, capacity building, and cooperation e.g., the Commonwealth Telecommunications Organization's Commonwealth Cyber governance Model of 2014. (Świątkowska *et al.*, 2017)

7. Suggestions

While it may not be possible to completely eradicate cybercrime and ensure complete internet security, it can be reduced by maintaining an effective cyber security strategy. There are some suggestions and solutions to avoid cyber-attacks.

a. Owing to the volatile nature of electronic evidence, international cooperation to combat cybercrime needs a quick response and the ability to perform specialized investigative actions, including the preservation and production, and analysis of data by private sector providers.
b. Effective international cooperation in cases involving electronic evidence, therefore, requires mechanisms for the advance preservation of data, pending the consideration of further investigative measures.
c. Strengthened national and international bonding between governments, law enforcement, and the other independent sector with increased the knowledge of cybercrime risks in public. (De Paoli and Studies, 2020)
d. The plan behind creating international guidelines is to fight cybercrime and facilitate a straightforward process to run digital investigations in

March 2022, Vol. 10, No. 1
ISSN 2163-758X

which computers from more than one country are involved, as well as to eliminate those gaps where a cybercriminal is far away from the reach of the national laws.

e. Mutual legal assistance requires writer tools for the following two purposes: as a practical guide for practitioners from developing countries that could accelerate the submission of MLA (Mutual legal assistance) requests; as a way to generate a format of application that could be accepted by developed countries acting as applications states.

f. Countries need to cooperate because cybercriminals are not confined by national or geographic boundaries, and digital proof relating to a single crime can be dispelled over multiple regions.

g. Law enforcement and IT professionals need to work more closely with the companies to build a cyber-fighting team that has the abilities, the means, and the authority necessary to reduce the instances of cybercrime on the Internet. (Ciupercă et al., 2021)

h. Countries must become sharper in updating or developing any national cyber security plan, as well as legal and regulatory framework related to cyberspace. The contribution of the technical community and the independent sector is essential to building effective resilience capabilities because it is impossible for the government to act alone.

i. Cyber security requires governments as well as private sector cooperation, therefore there is a need to increase trust among governments, at all levels, between countries and industries, and independent sectors.

j. Governments and the private sector should join together to work toward broader awareness campaigns in all countries. “Stop. Think. Connect” is a national public awareness program in the US which aims to introduce the knowledge of cyber threats and empower the public to be safer and more secure online. Furthermore, the public should play a vital role in self-educating and expanding the reach of awareness campaigns. Cyber security is a type of shared responsibility

k. While countries need to have cybercrime laws in place, it is equally necessary that these countries have the legal authority to assist foreign countries in an investigation, even if that country didn’t report any activity by itself and is merely the location of the intruder or a pass-over site. (Ciupercă et al., 2021)

Conclusion

Cybercriminals are developing new ways to damage organizations, individuals, and even the government's online and private data. New cyber laws are introduced by the government to combat cybercrimes and reduce their rate, but it is not easy and not possible without the cooperation of different countries. (Yar and Steinmetz, 2019). The non-binding nature and lack of strict enforcement mechanisms of International Law concerning cybercrime laws appear to have stultified the enforcement of cybercrime laws. (Kshetri, 2010) Cybercrime is causing tremendous losses not only to the economy but also to our personal information. It is essential to overcome this problem because technology not only causes harm but humans are doing so. Every citizen must remain alert and timely complain about any incident and the governments must enforce

March 2022, Vol. 10, No. 1
ISSN 2163-758X

cyber laws and make new laws to eliminate this devastating crime. (Ramdinmawii *et al.*, 2014)

References

Ajayi, E.F.G.J.J.O.I. and I. Systems. 2016. Challenges to enforcement of cyber-crimes laws and policy. 6:1-12.

Antwi-Boasiako, A. and H. Venter. A model for digital evidence admissibility assessment. IFIP International Conference on Digital Forensics, 2017. Springer, 23-38.

Bernik, I.J.V.J.O.C.J. and Security. 2014. Cybercrime: The Cost of Investments into Protection. 16.

Bidgoli, M., B.P. Knijnenburg, J. Grossklags and B. Wardman. Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting. 2019 APWG Symposium on Electronic Crime Research (eCrime), 2019. IEEE, 1-10.
Brenner, S.W. and J.J.J.B.L.T. Schwerha Iv. 2007. Cybercrime Havens Challenges and Solutions. 17:49.

Broadhurst, R.J.P.J.O.C. 2010. A new global convention on cybercrime. 2:1-10.

Ciupercă, E., A. Stanciu and C.E. Cîrnu. POSTMODERN EDUCATION AND TECHNOLOGICAL DEVELOPMENT. CYBER RANGE AS A TOOL FOR DEVELOPING CYBER SECURITY SKILLS. Proceedings of INTED2021 Conference, 2021. 9th.

Dashora, K.J.J.O.a.P.I.T.S.S. 2011. Cybercrime in the society: Problems and preventions. 3:240-259.

De Paoli, S.J.T.-I.J.O.S. and T. Studies. 2020. New solutions for cybersecurity. 11:101-105.

Hasbullah, H., I.a.J.I.J.O.E. Soomro and C. Engineering. 2010. Denial of service (DOS) attack and its possible solutions in VANET. 4:813-817.

Hinduja, S.J.C. and Behavior. 2008. Deindividuation and internet software piracy. 11:391-398.

Hong, J.J.C.O.T.A. 2012. The state of phishing attacks. 55:74-81.

Kasper, A. and E. Laurits 2016. Challenges in collecting digital evidence: a legal perspective. *The future of law and eTechnologies.* Springer.

Kshetri, N.J.T.W.Q. 2010. Diffusion and effects of cyber-crime in developing economies. 31:1057-1079.

Levin, A., D.J.P. Ilkina and T.R.S.O.M. Cyber Crime Institute, Ryerson University. 2013. International comparison of cyber crime.

March 2022, Vol. 10, No. 1
ISSN 2163-758X

Losavio, M.M., K. Chow, A. Koltay, J.J.S. James and Privacy. 2018. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. 1:e23.

McGuire, M., S.J.S.O.K.F. Dowling and I.H.O.R. Report. 2013. Cyber crime: A review of the evidence. 75.

Menon, S. and T.G.J.J.O.M.L.C. Siew. 2012. Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation.

Moore, R. 2014. *Cybercrime: Investigating high-technology computer crime*, Routledge.

Morgan, S.J.C.M. 2020. Cybercrime to cost the world $10.5 Trillion annually by 2025. 13.

Okeshola, F.B. and A.K.J.a.I.J.O.C.R. Adeta. 2013. The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. 3:98-114.

Prakash, F., H.K. Sadawarti and K. Baskar. Cyber Crime: Challenges and its Classification.

Ramdinmawii, E., S. Ghisingh and U.M.J.I.J.O.W.T. Sharma. 2014. A study on the cyber-crime and cyber criminals: A global problem. 3:172-179.

Roberds, W. and S.J.E.P. Schreft. 2009. Data security, privacy, and identity theft: The economics behind the policy debates. 33.

Roscini, M.J.J.O.C. and S. Law. 2016. Digital evidence as a means of proof before the international court of justice. 21:541-554.

Sarre, R., L.Y.-C. Lau and L.Y. Chang 2018. Responding to cybercrime: current trends. Taylor & Francis.

Serwanga, R. 2019. *Legal mechanisms for enforcing electronic transactions in Rwanda.* University of Rwanda.

Speer, D.L.J.C., Law and S. Change. 2000. Redefining borders: The challenges of cybercrime. 34:259-273.

Świątkowska, J., I. Albrycht and D. Skokowski 2017. *National Cyber Security Organisation, Poland*, NATO Cooperative Cyber Defence Centre of Excellence.

Taraszow, T.J.T.a.B.I.F.C. 2013. The influence of NGOs on safer Internet policy making.173-192.

Teng, A. 2017. *Jurisdictional Barriers: Cybercrime Prosecution Challenges.* Utica College.

March 2022, Vol. 10, No. 1
ISSN 2163-758X

Tyagi, A.K. and G.J.I.J.O.C.A. Aghila. 2011. A wide scale survey on botnet. 34:10-23.

Walenstein, A., R. Mathur, M.R. Chouchane and A. Lakhotia. The design space of metamorphic malware. 2nd International Conference on i-Warfare and Security (ICIW 2007). 2nd International Conference on i-Warfare and Security (ICIW 2007)(2007), 2007. 241-248.

Weber, A.M.J.B.T.L.J. 2003. The Council of Europe's Convention on Cybercrime. 18:425-446.

Yar, M. and K.F. Steinmetz 2019. *Cybercrime and society*, Sage.

Yeboah-Ofori, A., J. Abdulai, F.J.I.J.O.C.-S. Katsriku and D. Forensics. 2019. Cybercrime and Risks for Cyber Physical Systems. 8:43-57.

Author Notes

Maria Kanwal is a hardworking and intelligent student of LLB at Fatima Jinnah Women's University Rawalpindi, Pakistan. She was born in Harronabad and completed her early and intermediate education in Rawalpindi. She is strongly motivated by the idea of women empowerment and is very keen to spread awareness among people of the world about the current issues, that is why she participated in the 6th Global International Conference and gave a presentation. She has chosen to study law inspired by Asma Javed, a great human rights lawyer who did a lot for empowering women. Contact email: mariaakanwal72@gmail.com

Qurat Ul Ain Zahoor has completed her intermediate education in pre-medical. Now she is studying law at Fatima Jinnah Women University, Rawalpindi. She originates from Azad Kashmir. She has an interest in many social activities. She participated in many debate competitions. She likes to talk about social issues. She also participated in GIC to highlight the different issues that are faced by COVID-19. She has choosen law inspired by advocates' struggle to defend people's lives. She thinks that a good and truthful lawyer can also save a life like a doctor. Contact email: quratulainzahoor6@gmail.com

Saira Muassart was born in Rawalpindi. She has done her intermediate education in computer science. She is currently studying law at Fatima Jinnah Women University. Her ambitioon since childhood has been to be a lawyer in the future because she wants justice for people. She has the interest to work for her country and that is why she chose law. She loves to participate in extra-curricular activities like debates, poetry competitions. She participated in GIC to show her presentation talent. Contact email: Sairaamussarat74@gmail.com

Zainab Iqbal is currently working as a Lecturer in the Department of Law at Fatima Jinnah Women University Rawalpindi, Pakistan. She has completed her Master's Degree (LLM International Law) in 2019 from International Islamic University, Islamabad. In her LLM, she wrote a thesis on "The Need for a Comprehensive Arms Trade Treaty to Prevent Violations of International Humanitarian Law". She has served as a consultant for various international organizations, including UN Women, British Council, and EU. The contact email is zainab.iqbal412@gmail.com

March 2022, Vol. 10, No. 1
ISSN 2163-758X

Dr. Nadia Khadam is currently serving as Assistant Professor/Head of the Department of Law at Fatima Jinnah Women University, Pakistan. After getting practical advocacy experience, she joined the Ph.D program in Criminal Law, Policy and Procedure. Her areas of research are criminal law, cybercrime laws, cyber security policies, e-commerce policy, and reform in the justice sector of Pakistan. She is associated with different initiatives concerning internet governance in Pakistan. Moreover, she represented Pakistan at different national and international forums. The contact email is nadiakhadam@gmail.com.