CYBERSECURITY IN PAKISTAN: REGULATIONS, GAPS AND A WAY FORWARD

Umair Pervez KHAN*

Orcid ID: https://orcid.org/0000-0003-1978-4020

Muhammad Waqar ANWAR**

Orcid ID: https://orcid.org/0000-0002--1395-5856

Abstract

We live in the age of information and globalization. From paying online utility bills to advance health structure, up to date transportation, use of artificial intelligence, developed communication system and technical warfare, modern states are in continuous progress. Technology has reduced the distances, yet new threats and fears have emerged due to its usage. The digital world is under constant cyber threats and crimes such as hacking, bank frauds, money laundering, information theft, state secrets acquired, and even threats to critical infrastructure have become the evolving trends in cyber warfare. Both the developed states as well as developing nations are exposed to such threats leading to national security dilemma. However, developing country, having nuclear capabilities, like Pakistan, is more vulnerable to these threats. Pakistan also has large number of internet users with low information technology knowledge, thus making it further complex for the government and law-making authorities to regulate its digital world. Recently, Pakistan has faced serious cyber-attacks on important institutional websites and hackers have been able to successfully penetrate the cyber space of important installations. To prevent this from happening, legislators in Pakistan have introduced the cyber laws, which do not seem to cover the threats in depth and totality. This research paper focuses on the cybersecurity framework present in Pakistan while what are the policy options for the state of Pakistan to deal with serious cybersecurity issues is the actual matter of concern? The research methodology is qualitative in nature and researchers have used primary as well as secondary sources to draw the conclusions. At the end, few recommendations regarding the improvement in cyber protocols of the country are also put forth.

* PhD scholar at Selcuk University, Turkey and a prolific column writer for number of international publications.

** Doctoral candidate at Massey University, New Zealand and has been a regular contributor for different periodicals.

Keywords: Cybersecurity, Pakistan, Regulations, Challenges

Introduction

In the past few decades there has been an increased use of automated technologies, big data, the Cloud, Artificial Intelligence, making the life of human beings much easier than before, but also bringing forth with new kinds of threats and challenges. These challenges related to cyber space affect data privacy, security, storage, and online crimes. Dealing with these new challenges is an arduous task and a point of grave concern since advancements in the field of technology has also given rise to competition in cyber space with the eruption of proxy actors and organizations to achieve their political objectives and ideological goals (Hundley et al., 1995).

Globally, Cybersecurity has gained increasing importance in the present times due to the use of the computers in all fields of life. Cybersecurity has become increasingly pertinent for the developing third world countries due to the presence of imminent threats and the weak institutional mechanisms in place. Pakistan is a case in point. The country has constituted/ implemented cyber security laws to control cyber threats and attacks, but the threat still looms large, due to a lacuna in the implementation of these practices due to a plethora of reasons.

Moreover, Pakistan has also widened its internet base in last two decades to 87 million broadband subscribers with 39% penetration (PTA, 2020). The state has shifted from conventional infrastructure to digitized system thus being vulnerable to threat of cyber-attacks or in fact to cyber-attacks. According to Federal Investigation Agency (FIA), it reported 29,577 cybercrime complaints in last two years and have made one hundred and sixty arrests in 2017 alone (Yasin, 2021). An estimated 20 cyber related cases are registered on daily basis in the metropolitan city of Karachi (Islam et al., 2019). 37 banned terrorist outfits use more than 400 social media accounts to spread their message and propaganda against Pakistan (Iqbal, 2019). Similarly, recent report published by EU Disinfo lab, a European based organization, revealed that India is busy in maligning the image of Pakistan at international level by running a fifteen year old network of more than 550 fake online registered domains and 750 bogus media outlets, in almost 119 countries (EU Disinfo Lab, 2020). The growing cyber related crimes domestically and hostile online activities by foreign states like India are indeed a warning for the national security policy makers of Pakistan to frame and implement laws in a way which could curtail the growing influence of the cyber criminals.

Defining Cybersecurity

Before proceeding further, it is important to define important concepts related to cyber studies which include: Cyber, Cyber-crimes and Cybersecurity, so that issue may be analyzed in more professional manner and it may help the readers to grab the concepts more easily.

Most of the people take the term cyber as interchangeable with internet however cyber has two traits: electronic medium as its components and online communications as its capability (Fang, 2018) so it may be said that cyber means communication through electronic medium (Futter, 2016).

As far as the 'Cybercrime' jargon is concerned, if not talking in legal framework, it refers to the range of offences including conventional computer crimes and network crimes. The common understanding of the cybercrime is as any activity in which computers or networks are a tool, a target or a place of criminal activity (Gercke, 2012). United Nations (UN) is also of the point of view that there is no international definition of cybercrime however, it broadly put it as, "Cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse (United Nations Office on Drugs and Crime, 2013).

The history of cybercrime initiates in 1970's by the advent of ARPANET (Advance Research Projects Agency Network), used by the US military. The project was funded by US department of Defence to secure their military communications though the technology paved the way for regenerating the original message which was misused in future (Islam et al., 2019).

Moreover, the term 'Cybersecurity' is also vague as it is relatively new term in the arena of international relations. In the decade of 1970, the concept of computer security was somehow present, but it was only in late 1980's that real computer security was being thought of. Then in 1990's the companies started to provide the scanner applications. After the start of the new century the term 'Cybersecurity' is used frequently in the cyber literature but still lacks proper definition. According to different experts the term has different meanings for different people (Akyeşilmen, 2016). For the convenience of our readers we share the definition crafted by the US department of defence. It defines 'Cybersecurity' as the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (Department of Defence, 2010:57).

Cybersecurity Landscape in Pakistan

As a developing country in the Global South, Pakistan got internet availability in the early 1990's. As of now Pakistan constitutes the tenth largest population of internet users in the world (Kemp, 2020). The digital economy of the country ranks ninth by UN standards, and after getting access to 2G and 4G technologies, the internet penetration augmented to 17.8 % in 2016 (Statista, 2020). As per Pakistan Telecommunication Authority (PTA), the broadband penetration is 40.95 % with 87 million subscribers, a tele density of 79.65 % with 169 million cellular subscribers (PTA, 2020). Currently, 54% of the population of the country has access to mobile broadband, with mobile internet penetration standing at 26% (GSMA, 2020).

With such a huge populace using the information and communication technologies, cyberspace has emerged as a new domain and hence the accompanying challenges vis-à-vis cybersecurity regulation. According to the Global Cyber Security Index Report (GCI) of 2018 Pakistan was ranked 94th globally (International Telecommunication Union, 2018).

Pakistan was included in the five locations with the highest malware encounter rates during the January-December 2018 period with 18.94%. Interestingly Pakistan was also included in the five countries with the highest crypto-currency mining encounter rates in 2018 with a staggering percentage of 1.47 (Microsoft, 2018). There was a hacking incidence when the mobile phones of senior Pakistani officials were hacked, in 2019, through WhatsApp, with a special type of malware named 'Pegasus'. The concerns regarding this incident, became more viral, when reports regarding the use of the same malware by Indian intelligence, emerged which was being used by them to spy domestically on lawyers, politicians and so on. Pakistan also is one of the main targets of surveillance by the US National Security Agency (Qadeer, 2020).

The financial sector of the country is no exception. It also faces serious cyber threats. The card skimming, misuse of ATM cards, hacking and frauds in online payment are the most observed phenomenon. Approximately 8,000 to 10,000 out of 25 million bank accountholders have fallen prey to hackers across the industry (Malik, 2019). Pakistani banks lost heavy amounts due to cyberattacks (Iqbal, 2021).

In the current context of the formation of cybersecurity laws in Pakistan, the major challenge remains that of the implementation. As mentioned earlier, the weak institutional structure in Pakistan is one of the major hurdles in the implementation of the cyber security laws, coupled with other immanent challenges, like the presence of hostile intelligence networks and anti-state elements. In the following

section, the evolution of cyber regulations, dynamics of the implementation of the cybersecurity laws in Pakistan, along with the challenges, opportunities and the way forward will be discussed.

Cyber Regulation in Pakistan

The cyber regulations of Pakistan evolved over period of time and the country introduced its first document on cybercrime through "Electronic Transactions Ordinance, 2002," (ETO) which addressed limited number of crimes, as the main purpose of the Ordinance was "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers." (Electronic Transactions Ordinance, 2002). It was considered as an important step as far as the future legislation regarding cybercrimes was concerned.

In the year 2004, the Ministry of Information and Technology, Government of Pakistan (GOP), prepared "Electronic Crimes Act" based on the ETO, 2002, dealing with cyber stalking, electronic fraud, cyber war, data damage, electronic forgery, spoofing, cyber terrorism and punishments for cybercrimes (Iqbal, 2021). As the time passed, emergence and increase in the electronic crime in the country demanded serious legislation on the issue. Subsequently, "The Prevention of Electronic Crimes Ordinance, 2007" was promulgated by the then president of Pakistan, General Pervez Musharraf (Munir, 2010). However, this ordinance was also of the preliminary nature, dealing with only few of the existing e-crimes. The same Regulation was implemented thrice through presidential order, i.e. in May 2008, February 2009 and the lastly on 4th July 2009. The Ordinance was however not brought to the agenda of the parliament and lapsed due to constitutional strain[9].

Other efforts to improve the cybersecurity landscape of the country included the 'Seven Points Action Plan' proposed by the Chairman of Senate Committee on Defence and Defence Production after the alarming revelations made by Edward Snowden that NSA of USA is involved in espionage activities in Pakistan through internet (Senate of Pakistan, 2013). The Senate Action Plan laid down the strategy to defend the sensitive infrastructure in the country which later helped the efforts to frame the cybersecurity agenda at national level. The historic National Action Plan (NAP) announced at the end of the December 2014, by GOP to deal with terrorist activities also included a clause on online radicalization though it was not enough (Iqbal, 2021).

[9] The Presidential Ordinance in Pakistan is only applicable for one hundred and twenty days from the date of its promulgation.

The steps taken by GOP in different times were provisional in nature which provided no or little help to judicial system and law enforcement agencies to deal with the menace of cybercrime until Pakistan passed cybersecurity legislation in the lower house of the parliament, on 11 December 2016, which resulted in the creation of Prevention of Electronic Crimes Act (PECA), 2016 (*Pakistan*, 2016). The passing of the act was a lengthy process which required 18-month long deliberations by the lawmakers, cyber experts and relevant industry men on the draft, though many of the sections of the law are still controversial which is discussed in coming paragraphs. The included measures in the act are like ensuring protection against unauthorized access, interception and protection of transmission of critical data and information system. It also includes clauses intended to eradicate cyberterrorism, online glorification of offence, hate speech, electronic fraud, identity theft, cyberstalking, spamming, spoofing and so on.

The cyber regulations in Pakistan are very weak which are easily manipulated and evaded by anyone, even having a little computer knowledge. The Challenges being faced by Pakistan due to the unregularly of the cyber space are discussed in detail in following text.

Challenges

Since Pakistan, is still facing a plethora of issues, like corruption, penury, lack of technological prowess, and lack of a sound democratic system there remain several challenges to its internal security, of which cyber-security is an important component. The challenges to Pakistan's Cybersecurity landscape are manifold.

There is a lack of proper technological prowess to control, especially vis-à-vis the surveillance of the foreign spy agencies, like the National Security Agency of the United States (Qadeer, 2020). In addition to this, the country is also vulnerable to malware like Gamarue, Skeeya and Peals, which can install other malware and steal all the personal information from the infected computer system. The Distributed Denial of Service (DDOS) attack or the transmission of data within the computer to attack without the permission and knowledge of the PC user, forms another kind of vulnerability. A good example is the banking sector in country, which is also vulnerable to cyber-attacks, the most recent of which was the revelation by the Federal Investigation Agency's Cyber Crime wing of stealing of data from all Pakistani banks (Qarar, 2018). This is resulting in a trust deficit between the customers and the banks.

Furthermore, presence of terrorist organizations complicates the cybersecurity landscape, as there is a persistent vulnerability of the important government websites being hacked or theft of important

information for example regarding the strategic assets. Terrorist organizations like Islamic State (IS) and Tehreek-e-Taliban Pakistan (TTP) use Cyber propaganda to disseminate their message. Many individuals fell prey to their propaganda and joined the ban outfits (Khan, 2019). Terrorist attack like the Bacha Khan university (2016) was a clear-cut example of using Information Communication Technology (ICT) which was planned and executed by the preparators while sitting in a neighboring country (ibid).

Adding, there is generally a lack of awareness among the masses regarding the protection of their data from illegal access, and this sometimes results them in becoming victims of abuse, like identity theft which forms another kind of cybersecurity threat.

Moreover, the other challenges related to cybersecurity include incorrect media framing of cybersecurity, which mostly frames the debate in a generic perspective resulting in the creation of a half- baked concept of cybersecurity among the masses. Also, there is a lack of institutional structure to tackle with this challenge along with a wide range of security debates concerning the external threats often neglecting cybersecurity issues being faced by the country. The traditional security culture of the country focusing on threats like border security, threat of nuclear attack, terrorism etc. cover the national security spectrum, thus putting cybersecurity at the back burner. The non-inclusion of the audience in devising the cybersecurity policy also proves a major block, as the lack of feedback from the concerned personnel makes the policy more like a bureaucratic or technical jigsaw.

Nevertheless, the above-mentioned cybersecurity law passed in 2016, also put some measures which became contested because of weak democratic system in the country and was labelled as ‘draconian’ (Khan, 2016) which is not uncommon to be used in developing country like Pakistan. The critics are of the point of view that the law has given enormous powers to the authorities to which are misused by them at times (Sridharan, 2016). It also lacks proper protection for the data breach that is a constant threat (Kalyar, 2019). The law is also unable to differentiate between cybercrime form cyber warfare and cyber terrorism thus making punishments too hard which are not adequate for the respective nature of the crime. Moreover, some of the commentators call PECA as a state tool used to repress the free voices in the pretext of “national security” and “anti-state” rhetoric (Aziz, 2018). This type of criticism and shortcomings also refers to a pertinent challenge in the domain of formulation and implementation of cybersecurity measures.

As Pakistan lacks support from private partners to help build cybersecurity infrastructure, therefore has to rely on internal investment. There are two main organizations tasked with the maintenance of cybersecurity, National Response Centre for Cyber Crimes (NRCCC), under the Federal Investigation Agency (the primary law enforcement agency) and secondly the non-governmental agency called the Pakistan Information Security Association (PISA), which works alongside the private sector to mitigate commerce related threats (Baker, 2014).

However, despite all the cybersecurity measures taken by the country, it can only be classified as the starter as much more has to be done. Effective coordination and planning between the various civilian and military agencies is needed to formulate, devise and implement an effective cybersecurity mechanism which can be at par with other developed countries to tackle this challenge (Baker, 2014).

Overall, the cybersecurity posture of the state remains weak. There seems to be a lack of a proactive, comprehensive and grass-roots security program, as the cybersecurity measures in place appear to be reactive focusing on 'putting out the fire.' Moreover, the cybersecurity measures in place lack depth, with understaffed programs with most of the measures as merely being cosmetic. The approach to solve the cybersecurity related problems is 'security box centric' which denounces any kind of 'out of the box solution', with an over emphasis on the former. The cybersecurity problem solving involves a lack of consensus between the different stake holders even within the same organization as risk, compliance, security and IT Audit at the intra-departmental level. This disagreement is detrimental as it results in a wastage of time and resources. Adding to this are the issues related to governance & documentation overkill, where most of the cybersecurity efforts and initiatives are academic in nature, with voluminous policy and procedures, without any substantial strategy for implementation (barely 5-10% of the approved policy in almost all cases).

Furthermore, the data theft is a serious challenge faced by the country. The National Database & Registration Authority (NADRA) is country's only independent agency which is responsible for government database and statistics of its citizens. The vulnerability of the data theft is increased as the data is being linked and provided to defence institutions as well as many other government projects like Punjab Safe Cities Authority, Benazir Income Support Program and others. The incident of one of the largest data breaches in the history of Pakistan occurred two years back when the data of millions of citizens from Punjab Information Technology Board was compromised (Kalyar, 2019).

Way Forward

Cyberspace is considered 5th warfare domain other than conventional arenas of air, sea, land and space. It is often referred to as a new zone of conflict and will have significant implications on the social, economic, political and ethical realms. Cybercrimes have implications for economies world-wide, with 1% of global GDP being lost to cybercrimes each year, which has been calculated around 445 billion (Lewis, 2018). Pakistan needs to tackle the problem of cybersecurity in many fronts.

To start, as there are several terrorist groups operating inside the country there is a need to counter their narrative. With more than 120 countries expanding their cyber capabilities in offensive domain, including manipulation, degradation, blockage, or destruction of information and computer networks, these will be the important areas, in the cybersecurity domain which will need to work on a war footing. Pakistan must step up its efforts and work in collaboration with other states at the policy, federal, educational, military, provincial and strategic level which can prove to be the first line of defence against any cyber-attack. According to an estimate by 2030, 20 billion devices will be connected, and the country has to take up that challenge through proper management, cyber legislation, cybersecurity structures worldwide, establishment of Cyber Emergency Response Team (CERT) at federal and provincial levels, and most importantly, setting up a strong institutional setup.

The government needs to have a national cybersecurity policy, with laws related to cybercrimes, cyber warfare, cyber terrorism, cyber pornography, data privacy and so on. There is a dire need to make regulations which could help curtail the modern trends in Cybercrime like Phishing, Remote Access Attacks, use of artificial intelligence etc.

In addition, state must create research centers related to cyber research along with center for excellence, related to cybercrime. The National Centre for Cyber Security (NCCS) was created in 2018 at Air University, Islamabad, but it is not doing much to serve its purpose. A cyber workforce needs to be established, and the Higher Education Commission should start courses related to cybersecurity, in order to produce human resource, to cater the needs of the country. Currently, National Defence University, Islamabad is the only university in Pakistan to offer cybersecurity as an elective subject (Khan, 2019).

The country also relies on computer hardware accessories being imported through other countries and they pour into the state without much check and balance. Then this equipment is transferred to important institutions without any special scrutiny. Factory based built in viruses could be installed and they can create chaos in the infrastructure of important installations. Therefore, PTA and FIA

must be directed to have tight check on the import of electronic items and for the future it is advised to work on making the indigenous computer hardware in Pakistan. (Ibid.)

Finally, the law enforcement agencies need capacity building, in the form of training and equipment to combat cybercrimes. Cyber campaigns can be run in the form of media advertisements to raise awareness among the masses regarding issues related to cybersecurity, and cyber day can also be commemorated. Seminars and awareness campaigns need to be conducted, for youth and common citizens on how to use the internet. In addition to this, Pakistan can also become an active participator in the international effort to build cyber norms, catering to its national interest whilst joining the comity of like-minded nations to tackle this challenge. The Shanghai Cooperation Organization (SCO) can also be used to formulate regional cybersecurity strategies and help the members in this domain (Iqbal, 2021). The challenges remain manifold, however, if combined with political will, proper policy outlines and implementation strategies the outcomes can be robust and efficient.

Immediate Recommendations

- Government must strive to devise a comprehensive cybersecurity policy which should address all the current shortcomings in PECA and other relevant regulations. The policy must give protection to NADRA data base, Passport and Immigration, the data of all law and enforcement agency's employees including military, Airline travel data and all respected ministries data.

- Proper mechanism for international cooperation must be introduced on the subject as the nature of cybercrime is global.

- Considering the threat posed to the national security of Pakistan, it is highly recommended that state should establish a 'National Cyber Coordination Centre' which should not only work to devise the comprehensive cybersecurity framework but also act as a coordination council between civil and military institutions which could defend the economic assets as well as be prepared to act against cyber-attacks against important institutions.

- CERT headquarters at national level be developed having provincial offices in concerned regions.

- NCCS, established at Air University, Islamabad must be made active so that requisite output could be generated.

- Special courts to deal with cyber cases should be setup and proper judicial training must be initiated for the judicial fraternity in the country.

- Banks must be compelled by law to follow global standards like PCI, DSS and State Bank should ensure the compliance of international banking standards.

Conclusion

The advancement of the technology has brought new threats and challenges for the security of states as hostile states and even non-state actors are constantly busy in breaching the cyberspace of governmental institutions, telecommunication companies, military installations and banking infrastructure. Developing country like Pakistan is also facing severe cyber related issues which need to be addressed on immediate basis. The breach of citizens data, hacking of government websites, penetrating into the personal WhatsApp accounts of government officials, evading cybersecurity of financial institutions, efficient use of ICT by terrorist organizations and a well-organized malicious cyber campaign against Pakistan at international level by hostile states, like India, is a serious warning to the policy makers to craft a comprehensive cybersecurity policy as already existing cybersecurity framework is unable to cater the emerging trends in world of cybercrime. Along building its professional capacity in the field, state also needs to develop the 'National Cyber Coordination Centre' so that coordination between civil and defense institutions could be enhanced. Consequently, the better cooperation between law enforcement agencies would lead to strict implementation of cybersecurity policy thus improving the cybersecurity landscape of Pakistan.

References

Abdul Qadeer, M. (2020). *The Cyber Threat Facing Pakistan*. https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

Akyeşilmen, N. (2016). Cyber Security and Human Rights: Need for a paradigm shift. *Cyberpolitik Journal*, *1*(1), 32-55.

Aziz, F. (2018, February 7). *Pakistan's cybercrime law: Boon or bane?* Heinrich-Böll-Stiftung. https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

Baker, E. W. (2014). A Model for the Impact of Cybersecurity Infrastructure on Economic

Department of Defence.(2010). Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan. *Information Technology for Development*, *20*(2), 122–139. https://doi.org/10.1080/02681102.2013.832131

Electronic Transactions Ordinance, 2002. (2002). Government of Pakistan. http://www.lawsofpakistan.com/wp-content/uploads/2015/05/ETO.pdf

EU Disinfo Lab. (2020, December 9). *Indian chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests*. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

Fang, B. (2018). *Cyberspace Sovereignty* (3rd ed.). Springer, Beijing.

Futter, A. 2016, 'Is Trident Safe from Cyber Attack?', European Leadership Network, vol. 1, <https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safefrom-cyber-attack-1.pdf>.

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. ITU. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

GSMA. (2020). *Pakistan: Progressing towards a fully-fledged digital economy*. https://www.gsma.com/asia-pacific/wp-content/uploads/2020/06/24253-Pakistan-report-updates-LR.pdf

Hundley, R., Anderson, R. H., Arquilla, J., & Molander, R. C. (1995). *Security in Cyberspace: Challenges for Society: Proceedings of an International Conference*. https://www.rand.org/pubs/conf_proceedings/CF128.html

International Telecommunication Union. (2018). *Global Cybersecurity Index (GCI)*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Iqbal, Z. (2021). *Cyber Threats to Pakistan's Digital Landscape*. Sustainable Development in a Digital Society, Lahore. https://sdpi.org/sdpiweb/publications/files/SDC-Anthology-2020.pdf

Iqbal, Z. 2019, 'Cyber Threats in Pakistan's Digital Landscape', Presentation, 22nd Sustainable Development Conference, Sustainable Development Policy Institute, Islamabad, Pakistan, <https://www.sdpi.org/sdc/paper_details.php?event_id=867&paper_id=653>.

Iqbal Z. (2018, January 12). *Cyber security in Pakistan: Myth or reality*. Eurasia Review. https://www.eurasiareview.com/12012018-cyber-security-in-pakistan-myth-or-reality-oped/

Islam Z., Khan, M. A., & Zubair M. (2019). Cybercrime and Pakistan. *Global Political Review*, *4*(2), 12-

19. https://www.gprjournal.com/jadmin/Auther/31rvIolA2LALJouq9hkR/7EFv9UDoIP.pdf

Kalyar, J. A. (2019, December 22). Cyber Insecurity. *The News*. https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity

Kemp, S. (2020). *Digital 2020*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2020-pakistan

Khan, I. A. (2019). Cyber-Warfare: Implications for the National Security of Pakistan. *NDU Journal*, *33*, 117-132.

Khan, R. (2016, August 11). Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried. *Dawn*. https://www.dawn.com/news/1276662

Lewis, J. A. (2018). *Economic Impact of Cybercrime*. https://www.csis.org/analysis/economic-impact-cybercrime

Malik R. (2019, October 25). Cyber security challenges and solutions for banks, national institutions — II. *The News*.

Microsoft. (2018). *Microsoft Security Intelligence Report*. file:///C:/Users/mwanwar/Desktop/Cyber%20Crime%20Implemetation/Microsoft%20Security%20Intelligence%20Report%202018.pdf

Munir, M. A. (2010). Electronic Crimes Ordinance: An Overview of Its Preamble and Extent. *Pakistan Journal of Criminology*, *2*(1), 189-202. http://www.pjcriminology.com/wp-content/uploads/2019/01/14-5.pdf

Pakistan: National Assembly Passes New Cybercrime Law. (2016, September 21). [Web page]. //www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law/

PTA. (2020). *Telecom indicators*. Pakistan Telecommunication Authority. https://www.pta.gov.pk/en/telecom-indicators

Qarar, S. (2018). 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head. *Dawn*.

Senate of Pakistan. (2013). *Report of the Senate Committee on Defence and Defence Production* (6). https://www.senate.gov.pk/uploads/documents/1378101374_113.pdf

Sridharan, V. (2016, August 11). Pakistan passes 'draconian' cybercrime law threatening civil liberties. *International Business Times*. https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatening-civil-liberties-1575530#.)

Statista. (2020). *Pakistan: Internet penetration rate 2017*. Statista. https://www.statista.com/statistics/765487/internet-penetration-rate-pakistan/

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*. United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Yasin M. (2021). Cyber Security and Cybercrime in a Digital Society. In *Sustainable Development in a Digital Society* (pp. 33-43). Sang-e-Meel publications