Global Social Sciences Review (GSSR)
Vol. IV, **No.** I (Winter 2019) | **Pages:** 485 – 493

Cyber Laws and Cyber Security in Pakistan: Myths and Realities

Muhammad Tahir Assistant Professor, Dadabhoy Institute of Higher Education, Karachi, Sindh, Pakistan.

Tahreem Farrukh Assistant Professor, School of Law, Karachi University, Karachi, Sindh, Pakistan.

Muhammad Shahid MA, LLM, Advocate High Court, Pakistan.

Abstract *The evolving nature of warfare is characterized by technology's ability to adapt and attack enemies in different ways at different times and places. This adaptability also extends to the realm of cybersecurity, where billions of dollars are illegally transferred, data breaches occur, national secrets are compromised, and critical public infrastructure is hacked. Pakistan, like many other countries, is not immune to these challenges. Pakistan recently experienced a massive cyberattack against a major institutional website, resulting in a successful intrusion by hackers. In response, Pakistani lawmakers introduced a cyber law, but at the time the scale and complexity of these new threats were not fully recognized. To protect itself from such risks, it is important for Pakistan to stay vigilant and continuously adapt its cybersecurity measures to meet the evolving cyber threat landscape.*

Key Words:
Cybersecurity, Warfare Adaptation, Global Threat, Illicit Transfers, Cyber-Attacks, Cyber Laws, CERT (Computer Emergency Response Team)

Introduction

Virus attack is as older as the computer is; it is often overlooked from a security perspective. In the early days of computer science, the main focus was on exploring the potential of this new technology, and the concept of protection against malicious attacks was not yet fully realized. As computers become more interconnected and the Internet grows explosively, the exposure of large numbers of machines to the Internet allows cybercriminals to exploit vulnerabilities, test their skills, and carry out illegal activities. A real playground is provided for execution.

Development in the field of computing and information digitisation has greatly changed the cybersecurity landscape. Data integrity was widely recognized until the value and sensitivity of personal and sensitive information became apparent. Dollars in Billions were transferred/stolen illegally, massive breaches of privacy occur, state secrets are obtained by unauthorized parties, and critical public infrastructure is under constant threat from hacking attacks.

The term "cybercrime" has emerged primarily to refer to illegal activities that use computers as a means of execution or theft. The Justice Department of the US has expanded its description of cybercrimes as the broader offence of using computers to gather evidence. These include crimes such as network hacking, spreading computer viruses, identity theft, and Crime related to computers i.e. Bullying, Stalking, and Terrorism. This cybercrime poses a major challenge to individuals, organizations & even entire nations. Rapid technological advances over the last few decades have introduced new complexities and threats to the digital landscape. Automation technologies, big data, cloud computing, and artificial intelligence have undoubtedly made life easier for people, but they have also opened up new avenues for cybercriminals. As our reliance on connected systems and online platforms grows, privacy, security, storage and online crime are becoming pressing concerns.

Addressing these new challenges is a daunting task, as the ever-evolving technology landscape offers both benefits and risks. The emergence of sophisticated cyber criminals, state-sponsored hacker groups, and hacktivist organizations further exacerbates the cyber threat landscape. It's no longer limited to a single actor. Instead, agents and organizations are infiltrating the cyber realm and using technology to further their political and ideological goals.

The ubiquitous use of computers in almost every aspect of modern life has made cybersecurity of paramount importance worldwide. Governments, businesses and individuals alike struggle with the need to deploy robust cybersecurity measures to protect digital assets, sensitive information and critical

p-ISSN 2520-0348 | e-ISSN 2616-793X | L-ISSN 2616-793X | DOI: 10.31703/gssr.2019(IV-I).62 | URL: http://dx.doi.org/10.31703/gssr.2019(IV-I).62

infrastructure. However, developing countries, including Pakistan, face special challenges in this area. The presence of looming cyber threats, coupled with weak institutional mechanisms, requires concerted efforts to strengthen cybersecurity capacity, develop legislation, and promote cybersecurity awareness (Munir, M. A., 2010). . Pakistan recognizes the importance of cyber security and has taken steps to address the challenges it faces. However, concerns remain about the effectiveness of these measures. Implementation gaps, limited resources, and evolving cyber tactics pose major hurdles to achieving comprehensive cybersecurity protection. Further efforts are needed to improve our ability to effectively respond to incidents. Evolving cyber threats pose an ongoing challenge to individuals, organizations and nations, and the connected digital world requires a proactive and comprehensive approach to cybersecurity. By recognizing the importance of cybersecurity, investing in resources and skills, and promoting international cooperation, we can mitigate risk, protect critical infrastructure, and ensure a secure digital future.

Defining Cybersecurity

Virus threats have been around since computers existed, but they often don't get enough attention from a security perspective. In the early days of computer science, exploring the potential of this new technology was a major focus, with little consideration for protection from malicious attacks. However, as computers became more connected and the Internet grew exponentially, more and more machines appeared on the Internet, providing cybercriminals with virtual playgrounds to exploit vulnerabilities to commit illegal activities.

The importance of data integrity was not widely recognized until the value and sensitivity of personal and confidential information became apparent. The constant threat of illegal transfers of billions of dollars, widespread breaches of privacy, unauthorized acquisition of state secrets, and hacking of critical public infrastructure is rife in our increasingly connected world.

The term "cybercrime" was coined to refer to illegal activities that are primarily carried out through the use of computers (Gercke, M., 2012). This cybercrime epidemic poses a major challenge for individuals, organizations and even entire nations. Rapid technological advances over the last few decades have introduced new complexities and threats to the digital landscape (McAfee Labs, 2015) . Automation technology, big data, cloud computing, and artificial intelligence have definitely made life easier for humans, but they have also opened up new avenues for cybercriminals. As our reliance on connected systems and online platforms grows, concerns over privacy, security, storage and online crime become more pressing.

Addressing these new challenges is a daunting task given the ever-evolving technology that brings both benefits and risks. The emergence of sophisticated cyber criminals, state-sponsored hacking groups, and hacktivist organizations further complicates the cyber threat landscape (Rasool, S. 2015). Cybersecurity is no longer confined to individual actors but has become a battlefield for agents along with organizations seeking for achieving political as well as ideological goals through technological means.

With the widespread use of computers in various areas of modern life, the importance of cybersecurity is increasing on a global scale. Governments, businesses and individuals alike face the daunting task of implementing robust cybersecurity measures to protect digital assets, sensitive information and critical infrastructure. However, developing countries, including Pakistan, face special challenges in this area. The presence of looming cyber threats combined with weak institutional mechanisms calls for concerted efforts to improve cybersecurity capacity, enact comprehensive legislation, and promote cybersecurity awareness. Pakistan recognizes the importance of cyber security and has introduced and enforced laws and regulations in order to curb cyber threats (Naseer et al, 2018). However, concerns remain about the effectiveness of these measures. Implementation gaps, limited resources, and ever-evolving cyber tactics are major obstacles to achieving comprehensive cybersecurity protection, and more must be done to strengthen incident response capabilities.

Evolving cyber threats continue to challenge individuals, organizations and nations alike. In this connected digital world, a proactive and comprehensive approach to cybersecurity is essential (Malik, R., 2019). By recognizing the importance of cybersecurity, investing in resources and skills, and promoting international cooperation, we can mitigate risk, protect critical infrastructure, and ensure a secure digital future.

There exist various acceptable definitions of cybersecurity, each providing insight into the scope and purpose of safeguarding digital environments:

a) The IOS (International Organization for Standardization) defines cybersecurity or cyberspace-security as "The preservation of confidentiality, integrity, and availability of information in Cyberspace." In turn, Cyberspace is defined as "The complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". (Department of Defense ,2010).

b) The CNSS-4009 (Committee on National Security Systems) define cybersecurity as "The ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace, for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure or destroying the integrity of the data or stealing controlled information. (Khan, I. A., 2019)"

As technologies advance worldwide and new opportunities arise, there will always be individuals seeking to exploit them for personal gain. Therefore, cybersecurity focuses on protecting enterprises from the target peers in the market by utilizing others' systems.

Cyber warfare

Once confined to science fiction, cyber warfare is now a reality and most major nations have established dedicated cyber warfare units within their militaries. In the modern world, cyberspace is considered an important military domain alongside air, sea and land. There are a relatively very small amount of documented examples of coordinated cyberattacks against physical targets, it doesn't take a crystal ball to predict the inevitable increase in cyberattacks in the future. It is clear that we live in a time when political groups, governments, corporations and criminals could participate in cyber espionage/warfare or terrorism (Awan, J. et al, 2016). The consequences of these activities often have far-reaching effects on the physical world, even though they take place in the virtual realm. In this new era, warfare is entirely virtual, and the battlefield exists in a digital environment. Cyberwarfare between nation-states, like the introduction of nuclear weapons in the 1950s, has the potential to serve as a balancing act in many international relations and reshape power relations. Given the power of cyber warfare to disrupt nations, economies, and even the daily lives of individuals, it is imperative that we recognize its importance and impact. As technology continues to evolve, the need for robust cybersecurity measures and international cooperation to protect against the emerging threat of cyberwarfare becomes ever more important.

Opportunities Get by Cyber Attackers

Criminals will follow to a place where there are social interactions. This is especially noticeable in the area of so-called "computer crime". As modern society becomes more dependent on technology and the internet (Gade, et al 2014), cyber attackers are using these advances to their advantage. These predominantly male attackers engaged in cyber espionage/warfare/terrorism based on financial motives, social or political intent, or purely malicious intent.

Cyber attackers enjoy several advantages when conducting cybercrimes.

a) Selectivity and Controlled Effects

A targeted cyberattack can affect the economy of an entire country without necessarily destroying critical infrastructure. It can paralyze civilian life, undermine nations through economic losses, and cause public panic.

b) Ease of Execution and Low Visibility

Cyberattacks can be launched with the click of a button, requiring minimal physical human intervention. This tactic reduces the danger of being caught by Law maintaining agencies and provides cost and visibility advantages.

c) Low Cost

Acquiring a botnet containing thousands of compromised machines can cost thousands of dollars and still cause hundreds of times more damage and disruption. This eliminates conventional weapons and operational risks.

d) Areas of Expertise and Expertise

Cybercriminals can choose the timing, location and tools of their crimes while focusing on specific areas of expertise. Attackers often have extensive knowledge and understanding of the means and nature of cybercrime, while defenders have more general knowledge but limited expertise in specific areas. Tend to.

e) Unlimited Range

Cybercriminals operate without borders. Your actions can affect targets thousands of miles away or across states or borders. The agencies who are taking care of these aspects typically have jurisdictional boundaries and require coordination with other agencies who are not dedicated to working accordingly.

The prevalence of cybercrime highlights the need for robust cybersecurity measures and international cooperation to combat this evolving threat landscape. Cyberattacks have far-reaching effects and can have devastating effects on individuals, organizations, and even nations, so society must remain vigilant and proactively respond to cyberattacks.

Cyber Attack Targets

Global cyberattacks registered a 24% increase in the ending year of 2017. Manufacturing accounted for more than a third of all documented attacks in Q2, which seems to be in the top three among five Geographic region attacks in 2016 (Guramani, N, 2017).

The most affected sector includes 34% of Manufacturing, 25% of Finance and 13% of Healthcare. For over a decade, experienced cybercriminals have consistently chosen banks as their preferred targets. This translates into significant costs for financial institutions in fighting fraud and theft. The Banks are reported to spend 3 times more than any other financial institution on Cyber security and regulators perceive cybercrime as a "systemic" threat to financial stability.

Although the media and entertainment sector attacks decreased slightly year-on-year with 39%, this is the most targeted industry in order to steal personally identifiable information (PII). It is growing in popularity. Additionally, the industry offers hackers high profile and potential recruitment opportunities.

The internet and telecommunications industry is often targeted in its DDoS attacks, with a significant percentage of these attacks targeting gaming websites (Hundley, 1995). The association says the gaming industry is the most targeted industry in the Internet and telecommunications sector. Internet and telecom company reputations are highly dependent on resilience and uptime, as service disruptions on financial performance.

Position of Pakistan?

The growth of Cyberspace through evolving Information technology (IT) and telecommunications, presents hackers with opportunities for exploitation & sabotage that could be utilized. Hackers have broader targets and can now disable networks at their discretion.

In recent years, there have been countless cyberattacks against critical infrastructure and services. Hackers often rely on ransomware to take advantage of victims. Therefore, it is important not only to increase defences and also to counterattacks on the Internet.

However, this task is difficult because it is difficult to identify the attacker, especially when he hides behind the anonymity of his infrastructure on the Internet. This anonymity is particularly pronounced in the case of government-sponsored cyberattacks or due to the inherent imbalance in the nature of the attacks.

Nevertheless, countries should take effective measures to ensure cybersecurity. As technology advances rapidly, home appliances also become vulnerable to hacking and interference. Ensuring cybersecurity is therefore a huge and difficult undertaking that requires a lot of effort.

The past century has seen a major shift in the methods that state and non-state actors employ in waging war. This century, even with its downsides, is often referred to as the "information age." Pakistan, like many other countries, is not immune to these cyber threats. The country also struggles with challenges arising from the cyber sector. For Pakistan, cyberspace has permeated various sectors including banking, education, telecommunications, military and government agencies.

Cybersecurity Landscape in Pakistan

Internet availability in Pakistan peaked in the early 1990s, making the country the 10th largest Internet user in the world. According to United Nations standards, Pakistan's digital economy ranks ninth, due to the introduction of 2G and 3G the internet penetration increased by 17.8% in the year 2016. Broadband penetration is counted to be 40.95% having more than 87 million subscribers, the teledensity has 79.65%. with the stats of 169 million mobile subscribers (PTA,2020). 54% of the people have access to Mobile Broadband and 26% with mobile internet penetration. With so many people using information and communication technologies, cyberspace has become an emerging area that poses cybersecurity regulatory challenges. The Global Cybersecurity Index Report which was published in 2018 by the ITU (International Telecommunication Union) ranked Pakistan as 94th in the world (MISR, 2018.

In 2018, Pakistan witnessed a significant increase in malware attacks, with the highest annual attack rate of 18.94%, making it one of the top five regions in the world. Additionally, Pakistan was among the top five countries

with the highest incidence of cryptocurrency mining incidents at 1.47% (Qadeer, M. A. 2020). In particular, we observed a particular type of malware called "Pegasus" being used. The seriousness of the situation became even more apparent when reports surfaced that Indian intelligence agencies were using the same malware to monitor domestic lawyers, politicians, and others.

Moreover, Pakistan remains a major target of surveillance by the US National Security Agency, raising privacy and security concerns. Pakistan's financial sector is also vulnerable to serious cyber threats such as card theft, ATM card abuse, hacking and online payment fraud. About 8,000 to 10,000 of the 25 million bank account holders across the industry were hacked, causing huge economic losses for Pakistani banks.

In the current state of cybersecurity law in Pakistan, the main challenge lies in its enforcement. Pakistan's weak institutional structure, along with other challenges, poses a major obstacle to the enforcement of cybersecurity laws. The following sections discuss the evolution of cyber regulations, the dynamics of cybersecurity law enforcement in Pakistan, challenges, opportunities and future directions (Lewis, J., 2018).

Regulation on Cyber in Pakistan

Pakistan's cyber regulations have modernised from time to time. The country's first instrument to combat cybercrime was the Electronic Trade Ordinance (ETO) of 2002, which focused on the detection and facilitation of electronic documents, records, information, communications and transactions (Ali, K., 2018). In 2004, the Ministry of Information Technology introduced the Electronic Crimes Act. Building on his ETO, the law addressed cyberstalking, electronic fraud, cyber warfare, data corruption, electronic counterfeiting, identity theft, cyber terrorism and related penalties. Subsequently, the 2007 Electronic Crime Prevention Ordinance was enacted by President Pervez Musharraf of Pakistan. However, the regulation was limited in scope and targeted only a small number of existing electronic crimes. The same regulation was enforced three times by presidential resolutions in 2008 and 2009 but did not receive the attention of Congress and was suspended.

The "seven-point action plan" which was proposed by the chairman of the Senate Defense & Defense Production Committee following Edward Snowden's revelations of NSA espionage in Pakistan. " was included. The plan was intended to protect the nation's sensitive infrastructure and later helped set the nation's cybersecurity agenda. The National Action Plan (NAP) announced in December 2014 also included provisions to combat online radicalization, but it was insufficient.

Interim measures taken by the government have been ineffective and have failed to provide significant support to the judicial system and law enforcement agencies to combat cybercrime. Most recently, on December 11, 2016, Pakistan passed the Electronic Crime Prevention Act (PECA), resulting in a comprehensive cybersecurity law. The process of passing the law required extensive consultation among lawmakers, cyber experts and industry experts. However, some sections of the law remain controversial.

The cyber regulations n Pakistan are very weak are easily manipulated and evaded by anyone, even having little computer knowledge. The challenges being faced Pakistan due to the irregularity of cyberspace are discussed n detail n the following text.

Prevention of Electronic Crimes Act, 2016

The Electronic Crime Prevention Act, passed in 2016, reflects Pakistan's perception of the threats and challenges it faces in cyberspace. This law provides penalties for various cyber crimes. The falsification of communication information, electronic fraud, acts contrary to personal morality and decency, creation of malicious code, cyberstalking, hate speech, and glorification of criminal offences are all covered by the Penal Code. Applicable. law. The law contains provisions for fines and imprisonment for these crimes.

The law also introduces a Computer Emergency Response Team (CERT), made up of cybersecurity and critical infrastructure experts. These teams also include operatives. International cooperation has been proposed to address cybersecurity threats.

Essential Services in Pakistan

NADRA is the IT-based working body of Pakistan which is responsible to register and store information of the Population. NADRA shares this information with other government agencies for their own purposes. However, this confidential information is also at risk of theft or alteration. NADRA itself can be a target for cyber terrorism, with attackers intent on blocking or sabotaging critical services, hacking sensitive human information, and misusing it for illegal purposes. Protecting the NADRA system and the data stored in it is critical to protecting the privacy and security of the public's information.

Computer Emergency Response Team (CERT)

In Pakistan, the PTA has developed an implementation framework titled "CERT (Computer Emergency Response Team) – Pakistan Telecommunications Sector Implementation Plan" for establishing CERTs in the country's telecommunications sector. This framework describes the functions and roles of CERT. Given Pakistan's high telecommunications density and reliance on the internet, any disruption or damage to the telecommunications sector could have serious consequences such as data breaches and security breaches. CERT serves as the first line of defence against cyberattacks for the telecommunications industry and its users.

Pakistan has experienced numerous cyberattacks over the years. Incidents such as the hacking and defacement of government ministry websites on Pakistan Independence day and the 2010 government website hacking highlight the country's fragility. Private companies such as Careem were also targeted in attacks, resulting in the disclosure of user information. Cyberattacks against banks are also on the rise. Nearly every bank in Pakistan was reportedly hacked in 2018, resulting in financial losses. The nature of the threat and the best approach to addressing it remains a matter of debate and confusion.

These incidents have raised concerns about Pakistan's cybersecurity capabilities, particularly its nuclear weapons and facilities. In recent years, global pressure on Pakistan's nuclear weapons program and attacks on military installations have prompted calls for the introduction of nuclear doctrine in Cyberspace to strengthen security protocols.

Challenges

The challenges facing the cybersecurity landscape in Pakistan are truly diverse. The country faces a range of problems such as corruption, poverty, lack of technological capacity, and unstable democratic institutions, all of which contribute to domestic security challenges, making cybersecurity critical. It is an element.

Lack of Technical Competence

Pakistan faces a technological deficit, especially when it comes to monitoring and countering foreign espionage activities like the US National Security Agency. This technological gap makes the country vulnerable to malware attacks such as her Skeeya, Peals and Gamarue, which have the ability to install other malware from infected computer systems to steal personal information.

Distributed Denial of Service (DDoS) attacks

A DDoS attack involves the unauthorized transfer of data w in order to destroy or overload the victim's computer without his consent or knowledge. This type of attack poses significant vulnerabilities, especially in areas such as banking. The recent data theft incident at a Pakistani bank has eroded trust between customers and financial institutions.

Terrorist Organization

The presence of terrorist organizations further complicates the cybersecurity situation in Pakistan. His websites of major governments are constantly at risk of being hacked, which can lead to the theft of critical information, including strategic asset data. Terrorist groups such as ISIS and TTP also use cyberspace to spread their hate speech and propaganda and lure individuals for their cause. In some cases, such as the Bacha Khan University attack in 2016, terrorist attacks were planned and carried out using information and communication technology (ICT) from neighbouring countries (Qarar, S. 2018).. Lack of awareness and protection:

A lack of public awareness of protecting information from unauthorized access leads to individuals becoming victims of abuses such as identity theft. The media portrayal of cybersecurity is often inaccurate and specific, resulting in a limited understanding of the concept among the general public. Moreover, the institutional structures to address cybersecurity challenges are inadequate, and various security discussions often ignore the cybersecurity challenges facing the country.

Controversial Cybersecurity Laws

The cybersecurity law passed in 2016 has been criticized for being "harsh" and giving authorities too much power, which can sometimes be abused (Khan, R. 2016). The law lacks adequate protection against data breaches, struggles to distinguish between cybercrime, cyberwarfare and cyberterrorism, and imposes penalties that may not be appropriate to the nature of the crime. Some commentators see the law as a means of suppressing voices under "national security."

Lack of Private sector Support

Lacking support from private partners, Pakistan relies heavily on domestic investment to build cybersecurity infrastructure. The two main organizations responsible for maintaining cybersecurity are the Federal Investigative Agency (FIA) National Cybercrime Response Center (NRCCC) and (PISA) which works with the private sector to mitigate related threats to e-commerce. However, these efforts are just the beginning and much more needs to be done.

To effectively meet these challenges, Pakistan needs coordinated planning and cooperation among various civilian and military authorities. Aligning countries with international standards and practices requires strong coordination and effective implementation of cybersecurity mechanisms (Qarar, S. 2018).

Pakistan's cybersecurity regime has several weaknesses and challenges. Existing controls often take a reactive rather than proactive approach and lack a comprehensive and realistic security program. Additionally, the depth of these measures is limited, with understaffed programs focused primarily on surface solutions. Box-centric approaches are overemphasized, out-of-the-box solutions are ignored, and innovation is stifled.

Disagreement among stakeholders within an organization, especially in the areas of compliance, and risk, exacerbates the problem in security and IT audit. Lack of agreement leads to wasted time and resources. In addition, cybersecurity efforts tend to be overly academic and characterized by extensive policies and procedures without substantive implementation strategies, creating governance and documentation issues.

Data theft is a major challenge for Pakistan as the National Database Registration Authority (NADRA) is responsible for government databases and national statistics. Data theft vulnerabilities are exacerbated by ties to defence agencies and other government projects. To meet these challenges, Pakistan needs to adopt a proactive and comprehensive cybersecurity approach that prioritizes prevention over reaction. This includes investing in skilled cybersecurity professionals, fostering innovation, fostering collaboration among stakeholders, establishing strong governance frameworks, and implementing effective privacy and breach response strategies. increase. Additionally, public awareness and education on cybersecurity are critical to fostering a cybersecurity culture and effectively mitigating risks.

Way Forward

Cyberspace is the fifth domain of warfare, alongside the traditional domains, often referred to as the new conflict zone, it has profound implications for social, economic, ethical and political spheres. The global economy is suffering from the effects of cybercrime. It is estimated that he loses 1% of the world's GDP, or about $445 billion, each year. Pakistan needs to address cybersecurity issues on multiple fronts.

First, it is important to counter the claims of terrorist groups operating in the country. These areas become important in the field of cybersecurity. To act as the first defence against cyberattacks, the country needs to start steps and cooperate with various countries at various levels, including political, federal, educational, military, local and strategic. With an estimated 20 billion connected devices by 2030, Pakistan needs to implement appropriate controls, cyber laws, a global cyber security structure, and the establishment of federal and local Cyber Emergency Response Teams (CERTs), and We need to address this challenge through the most important things. Which could be helpful in Establishing a strong institutional framework.

The Lawmakers and government should improvise and facilitate the laws on cybercrime, cyberwarfare, cyberterrorism, cyberpornography, privacy, etc (Baker, E. W.2014). Regulation is necessary to curb modern cybercriminal trends. In addition, the state should establish research centers on cyber research and cybercrime. The National Cyber Security Center (NCCS) was established at Islamabad's Aviation College in 2018, but it has not served its purpose effectively. The Education Sector should adopt the Cyber Security topic as now only one of the universities in Islamabad is offering cyber security to be elective subject.

The FIA also have to monitor the import of Hardware item as it is also one of the major cause of introducing any virus to the country, the PTA along with FIA have to monitor the import and contentions of Hardware materials.

Finally, awareness and training program in the field of Cyber security is needed. You can initiate cyber campaigns through media promotions to raise public awareness of cyber security issues and celebrate Cyber Day. Seminars and awareness campaigns on Internet use should be conducted for young people and the general public. Furthermore, Pakistan can actively participate in international efforts to set cyber norms, aligning itself with national interests and joining forces in order to tackle this challenge. The Shanghai Cooperation Organization (SCO) can also be used and would be helpful in developing regional cyber security strategies along with providing support to member states in this area. Despite the challenges, with the political will, the right political guidelines and an execution strategy, solid and efficient results can be achieved.

Conclusion

Advances in technology have introduced various modern challenges along with threats to national security. Developing nations like Pakistan also face serious cyber challenges that require immediate attention. Violations of citizens' privacy, hacking of government websites, infiltration of government employees' personal WhatsApp accounts, circumvention of financial institutions, use of ICT by terrorists, and adversarial nations like India attacking Pakistan at the international level. A systematic malicious cyber campaign against the WHO, warns policy makers to take a serious stand and develop a comprehensive cybersecurity policy. Existing cybersecurity frameworks are not good enough to keep pace with emerging trends in the world of cybercrime. In addition to building expertise in this area, states should also develop a "National Cyber Coordination Center" in order to improve coordination between civil and defence agencies. Stronger coordination among law enforcement agency and can lead to rigorous enforcement of cybersecurity policies.

References

Ali, K. (2018, November 9). *FIA takes up banking fraud and hacking with SBP*. Dawn.

Awan, J., & Memon, S. (2016). *Threats of Cyber Security and Challenges for Pakistan*. In Proceedings of the 11th International Conference on Cyber Warfare and Security (pp. 1-10). USA.

Aziz, F. (2018, February 7). Pakistan's cybercrime law: Boon or Bane?

Baker, E. W. (2014). *A Model for the Impact of Cybersecurity Infrastructure on Economic Department of Defense*. In Dictionary of Military and Associated Terms (pp. xx-xx). Publisher.

Department of Defense. (2010). *Dictionary of Military and Associated Terms*. Publisher.

Gade, N. R., & Reddy, U. J. G. (2014). A study of cyber security challenges and its emerging trends on latest technologies. International Journal of Engineering and Technology, 4(1). 10.48550/arXiv.1402.1842

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges, and legal response*. Publisher.

Guramani, N. (2017, July 19). *Senators term Prevention of Electronic Crimes Act, 2016 a 'black law'*. Dawn.

Hundley, R., Anderson, R. H., Arquilla, J., & Molander, R. C. (1995). *Security in cyberspace: Challenges for society: Proceedings of an international conference*. Publisher.

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

Khan, R. (2016, August 11). *Cybercrime bill passed by NA: 13 reasons Pakistanis should be worried*. Dawn.

Lewis, J. (2018). *Economic Impact of Cybercrime—No Slowing Down*. Report, Center for Strategic and International Studies (CSIC).

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

McAfee Labs. (2015, 2016). *Threats Predictions*, October.

Munir, M. A. (2010). Electronic Crimes Ordinance: An overview of its preamble and extent. *Pakistan Journal of Criminology, 2*(1), 189-202.

Naseer, R., & Amin, M. (2018). Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security. *A Research Journal of South Asian Studies, 33*(1), 35-48.

Qadeer, M. A. (2020). *The Cyber Threat Facing Pakistan*. Publisher.

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

Rasool, S. (2015). Cybersecurity threat in Pakistan: Causes, challenges, and way forward. SocioBrains, Issue 12, August 2015, xx-xx.