CYBERSECURITY AND CHALLENGES FACED BY PAKISTAN

Muhammad Fahim Khan
PhD Scholar
Department of Political Science
University of Peshawar
Peshawar - Pakistan
fahimkhan@uop.edu.pk

Dr. Aamer Raza
Assistant Professor
Department of Political Science
University of Peshawar
Peshawar – Pakistan
aameraza@uop.edu.pk

Dr. Noreen Naseer
Lecturer
Department of Political Science
University of Peshawar
Peshawar – Pakistan
noreennaseer22@gmail.com

Abstract

Due to significant growth in cyberspace, Pakistan is becoming one of the world's most dynamic digital economies. Because to Pakistan's expanding internet and teledensity, the country is becoming increasingly connected to the rest of the world. Electricity, financial services, water, transportation, health care, and food all rely on ICT networks to function, be distributed, and be integrated in today's world. A wide range of actors, from individuals to corporations and governments, can take advantage of these opportunities and weaknesses. This shows that the modern-day information revolution is both a blessing and a curse. It's a problem because of the 'enabling function' that ICTs have in causing chaos, crime, and state-level aggressiveness. Social unrest, political strife, and other horrifying occurrences might exacerbate the vulnerability of our reliance on ICT. Pakistan is currently experiencing a rapid growth in the use of ICT in various industries, yet the country has a major shortage of cyber readiness. A hostile security environment exists both within and without

the country. It is vulnerable to a variety of cyberattacks because to these factors. An examination of Pakistan's cyber danger landscape using the securitization theory is the topic of this article, which aims to look at all of Pakistan's cyber risks from hacking to severe and organised cybercrime, terrorism and conflict. To assess Pakistan's cyber preparedness profile, the International Telecommunication Union's (ITU) five-pillar criteria are used: legal and technical; organisational; capacity-building and international collaboration; and international cooperation.

Keywords: Cybersecurity, Telecommunication, Pakistan, ICT, Cyberattacks.

Introduction

Jason Andress and Steve Winterfeld say that in order to collect, analyse, modify, transmit, store, and secure information, the term "cyberspace" refers to a "notional environment" or "global domain" made up of disparate networks of information technology infrastructure such as telecommunication networks, computers, and the internet. Communication and networking were its primary goals. While humans' dependence on cyberspace and dangerous technical breakthroughs has grown, it has also turned into a battlefield where information technology and data are being used as the means and targets of warfare to cause instability, destroy essential infrastructure, and engage in espionage. To the detriment of Pakistan's national security, internet has been criminalised and militarised. Pakistan is vulnerable to a wide range of cyber dangers, including identity theft, computer malware, cyber frauds, financial data theft, critical infrastructure information and surveillance on key infrastructure. Pakistan's national security cannot be adequately safeguarded unless these dangers are dealt with effectively. In light of this, the purpose of this study is to shed light on the nature of Pakistan's cyber security concerns. It also outlines the national security culture's standards, behaviours, and attitudes that obstruct Pakistan's successful securitization of cyber risks. It also seeks to propose the necessary modifications in order to fix the problems. The following questions are addressed in the paper: What are the cyber dangers to Pakistan's national security? How is the securitization of internet being hampered by Pakistan's security culture?

Due to the fact that cybersecurity is still a relatively young area of study in Pakistan, there is a dearth of published research. From theoretical to case study, the review of the literature is arranged in this manner. Digital disaster, cyber security, and the Copenhagen School are all discussed in the authors' article (Hansen and Nissenbaum, 2009).

Researchers Lene Hansen and Helen Nissenbaum use the securitization theory to examine how cybersecurity emerged in the wake of shifting geopolitical dynamics and technological advancement throughout the post-Cold War period. They also applied this theoretical framework to the 2007 Estonian cyberattacks. Cyberspace and Pakistan are compared in Richard A Clarke and Robert Knake's book, Cyber War: The Next Threat to National Security and What to Do About It. While discussing the chaotic nature of cyberspace, they've drawn a parallel between it and Pakistan's tribal areas. They also compare cyber threats to Pakistan's drone assaults in terms of their type and severity. This book provides a complete legal examination of Pakistani cyberspace, which is authored by Khalil-ur-Rehman Khan. A comprehensive assessment of the need for a legal framework to regulate and protect individuals, institutions, and the state of Pakistan in cyberspace is provided in his legal opinion. Furthermore, he brings out some serious concerns about the lack of a cyber-specific legal framework and makes predictions about potentially hazardous circumstances. The Prevention of Electronic Crime Act (PECA), 2016 in particular, is also examined in depth by him. The classic realism school of thinking that dominates Pakistan's security discourse offers a dated vision of Pakistan's cyberspace when viewed through the securitization theory lens. The theoretical framework, followed by Pakistan's cybersecurity and the issues of cyber securitization in Pakistan, are the three sections of the study.

Cybersecurity and Pakistan

The United Nations has Pakistan's digital economy as the eighth best in the world. 6.3 percent of Pakistanis have access to the internet in 2005. In 2016, the internet penetration rate rose to 17.8% as a result of greater availability to 3G and 4G technology. Pakistan saw a growth of 16 million internet users in the three years from 2012 to 2015. In 2018, 47% of internet users were first-time newcomers like this. Mobile internet penetration in Pakistan stands at 25.32 percent, with a total of 51 million customers, according to the Pakistan Telecommunication Authority (PTA). With 54 million customers, the broadband penetration rate is 26.46 percent. Pakistan has a teledensity of 72.90 percent, with 148 million cell phone subscribers contributing to this figure. Pakistan is now ranked ninth in the world in terms of mobile subscription growth. Pakistan has a mobile phone penetration rate of 39%. Pakistan, together with nine other nations, would account for 60% of the worldwide subscriber market by the year 2025. Cyberspace has arisen as a new area of security in Pakistan as a result of the country's extensive and growing usage of information and communication technologies. A comprehensive national cybersecurity architecture is being developed in Pakistan as a result of new initiatives. The PECA 2016 is the most significant accomplishment. Protecting essential data and systems from interference, unauthorised access, transmission and interception is the goal of this law.

Online terrorism, online glorifying of offences such as racism and sexism as well as cyberstalking, spamming as well as cyberbullying are also addressed in this section. Pakistan was placed 67th out of 193 countries in the International Telecommunications Union's Global Cybersecurity Index (GCI) in 2017. (ITU). Pakistan is lagging behind in terms of both technological and organisational metrics, according to the Global Competitiveness Index (GCI).

Pakistan had one of the world's largest concentrations of malware hosting sites in 2017. (15 - 20 malware hosting sites per 1,000 hosts). In the first three months of 2017, Pakistan had the second-highest malware encounter rate in the world, with a rate of 27.48 percent. Malware infections are on the rise in Pakistan, according to the Microsoft Malware Infection Index for Asia Pacific Region 2016. Second, third, fourth, and fifth place went to Indonesia, Bangladesh, Nepal, and Vietnam. The eighth place goes to India. A computer infected with Peals, Gamarue, or Skeeya, or other malware that can spread and steal personal information, is particularly vulnerable in Pakistan. The DDoS attack and identity theft are the second and third most dangerous cyber risks, respectively. In 2018, Pakistan's banking industry was a major victim of cyberattacks, which resulted in significant financial losses. Personal information for over 8,000 Pakistani bank accounts can be found on the Dark Web. India's "Cold Start Doctrine" includes "cyber warfare" in addition to biological, nuclear, chemical, conventional, and subconventional forms of conflict. A variety of tools and tactics are used to compromise, degrade and destroy computer systems at all levels of the organisation. Aside from that, it intends to obliterate all of the nuclear command and control systems' crucial data (C2). "Hybrid or Fifth Generation Warfare" includes cyber warfare as an integral component in the Joint Doctrine of the Indian Armed Forces 2017. Future wars will be waged in cyberspace, according to this philosophy.

Fundamentals of Cyber Design

Despite the fact that the technical intricacies of cyber dangers are outside the scope of this study, knowing the basic ideas is critical for analysing cyber issues within the socio-political framework. Cyber and cyberspace, vital infrastructure, and cybersecurity are just a few of the terms that fall under this umbrella. A controversial term, "cyber" has diverse connotations for different individuals, and should not be considered interchangeable with the internet, according to Andrew Futter. The term "cyber" is defined as having two characteristics: electronic media and internet communication. As a result, the term "cyber" refers to communication by electronic methods, such as via a website or email. (Futter, 2016) Cyber refers to the "command and control of computers" in a broader meaning. There are individuals or users and venues where they can communicate in "cyberspace," along with the features of cyber. "A time-dependent set of interconnected information

systems and human users that interact with these systems" is the definition of cyberspace as a whole. Embedded systems and processors, as well as networks of (online/offline) telephones, computers, and other electronic devices, are all included in the concept of cyberspace (Fang, 2018).

There may be "actions that may result in unauthorised access, exfiltration of information from an information system or information that is being processed by or being transported through an information system," according to the definition of "cyber danger." Cyber-attacks and cyber exploitation are two types of cyber threats. The term "cyberattack" refers to a cyber-operation to "alter, disrupt, mislead, degrade, or destroy computer systems or networks or the information and/or programmes resident in or transiting these systems or networks." Cyber exploitation is the illegal, clandestine acquisition of private information over the internet. Cybercrime, cyberterrorism, cyberwar, and cyberespionage are all examples of different forms of cyber dangers. Account takeovers, impostor frauds, denial-of-service attacks and computer network operations are just some of the ways in which cyber threats might take place. Targeted assaults on key infrastructures of an organisation or even a state are commonplace in serious cyber-attacks. This definition of infrastructure defines it as "a framework of interconnected networks and systems, typically integrated at many different levels, such as industries, institutions and distribution capacities that enable a flow of products or services." Information and communication, banking and finance, energy, transportation networks, and human services are all key infrastructures in modern industrialised countries. These include information and communication infrastructures, which may be directly targeted by cyber-attacks. In order for other vital infrastructures to be at danger of cyberattacks, they must be interconnected via information and communication networks. To put it another way, "cybersecurity" or "information technology security" refers to the technologies and methods used to protect information on the internet from being harmed. According to this broad definition, cybersecurity encompasses both technological and non-technical aspects. (Roscini, 2014)

The Cybersecurity Threat Design of Pakistan

The degree to which a state or organization's ICT-dependent infrastructures are vulnerable shapes the cyber threat environment of that state or organisation. It is tied to both technological and societal variables that cause this vulnerability. As a result of its involvement in internal or international warfare, a state that doesn't have adequate cybersecurity measures in place is at risk of encountering a disproportionately large number of cyber threats, including cyberwar. A cyber threat landscape is formed by Pakistan's increasing dependence on internet governance and service delivery, as well as the country's vulnerability to cyber threats due to inadequate cybersecurity preparedness,

and the hostile socio-political environment that Pakistan faces both domestically and internationally. (Bayuk & Healey, 2012)

Pakistan's Rapid Growth in the Cyber World

ICTs, particularly the Internet, has led to a boom in e-commerce and e-government during the past two decades. Countries throughout the world are becoming increasingly dependent upon cyberspace as they rely more and more on information and communication technologies (ICTs). As of June 2018, more over four billion individuals (55.1% of the global population) were online, compared to only 16 million (0.4% of the population) in December 1995. As a result, a state must assume an ever-increasing duty to protect its virtual borders as well as its physical ones. Because of the country's history of violent regional warfare, religious extremism, and terrorist activity, this is especially true for Pakistan's rapidly expanding e-government, e-commerce, and e-business sectors. Pakistan has faced risks to physical security since its independence, and now it must deal with threats to information security in order to protect its growing usage of ICTs. In Pakistan, more than 31% of the population has internet connectivity, according to the Pakistan Telecommunication Authority (PTA February's 2019 data). In its 2017 Information Economy Report, the United Nations Conference on Trade and Development listed Pakistan as one of the world's top ten fastest-growing digital and internet economies. Over the course of just three years (2012-2015), internet connectivity increased from 3% to 15% of Pakistanis, according to the survey. The development of 3G/4G technologies in Pakistan in recent years has largely been the result of this exponential rise in internet access. Currently, 63 million people use 3G or 4G smartphones to access the internet out of 65 million broadband customers.

As described by Ahmed, public and commercial organisations in Pakistan are increasingly depending on online management and service systems to operate in this fast-growing country. Having Pakistan's national ID database, NADRA is Pakistan's most important government organisation. Banks, the Pakistani Election Commission, the Department of Immigration and Passports, mobile networks, and security agencies all have access to internet data on Pakistani citizens through the NADRA. This organisation. Economic, social, and safety services provided by public firms in Pakistan are becoming more and more electronic as a method of modernisation and efficiency. National Information Technology Board was renamed in 2014 as a result of a merger with Pakistan Computer Bureau, which was established as E-Government Directorate as part of the IT Ministry in 2002. ICT-based services, such as ATMs, internet banking, online payments, and virtual stock markets are common in the country's economy because of this (VSEs). Other social sectors, including schools, hospitals, and police units, also provide e-government services

(Khyber Pakhtunkhwa). Military and nuclear arsenal upgrading is a hallmark of 21st-century progress, and Pakistan is no exception. (Ahmed, 2017)

Cybersecurity Frailty of Pakistan

In the digital era, cyberspace is becoming a weapon of crime, terrorism, and war, supplementing and, at times, replacing the old means of criminality. In today's virtual environment, national security faces a major issue since bad actors have the opportunity to target essential infrastructure. Pakistan's rising reliance on cyberspace compromises the country's national security due to a dearth of efficient cybersecurity measures, despite its importance and benefits. When it comes to cybersecurity commitment, Pakistan came in at 67th place out of 193 nations in the Global Cybersecurity Index (GCI) annual report for 2017. As a result of a lack of measures — legislative, technological, organisational, capacity building and collaboration — the country's cybersecurity is ranked low in the world, according to this research. A few examples demonstrate Pakistan's inadequate cybersecurity measures. Guardian published an exposé in March 2013 based on Snowden revelations showing that the US National Security Agency has set Pakistan as its second most-wanted target after Iran (NSA). UK spy agency Government Communications Headquarters (GCHQ) was later alleged by Intercept to have hacked into Pakistan's major communications infrastructure to access popular websites, using the same source. In the second half of 2015, Microsoft reported that Pakistan had the most malware assaults, and the Senate Committee on Foreign Affairs of Pakistan later discovered that Pakistan was one of the top countries targeted by foreign espionage. (Cassidy, 2013)

Because of Pakistan's vulnerability to cyber attacks and the absence of law, policy, and execution to fight such threats, the current situation of cybersecurity in Pakistan is alarming. (Shad, 2019) With Pakistan's lack of cybersecurity preparation and the country's overall lack of security, the country is vulnerable to four distinct forms of cyber threats:

1) Organised Cybercrime

Organized and skilled criminals are drawn to cybercrime as the world's financial and commercial transactions become increasingly computerised. Dark Market and other black market networks, such as Silk Road, are engaged in a variety of cybercrime operations, including the theft and sale of personal data from bank accounts and credit cards, social security numbers and passwords, and the trafficking of botnets. By moving organised crime from offline to online, the global economy suffers greatly. Center for Strategic and International Studies study found that cybercrime costs the global economy an estimated $445 billion each year (CSIS). When it comes to cybercrime, authorities from around the

world have yet to agree to work together. As e-banking and e-government take hold, cybercrime is on the rise in Pakistan. When it comes to cybercrime, which may range from account hacking to illegal cash withdrawals and money transfers, the country has to deal with it frequently. The Federal Investigation Agency's (FIA) cybercrime unit, the National Response Center for Cyber Crimes (NR3C), received a total of 2019 complaints in 2017. These complaints may be divided into three basic categories: There were 1592 (76 percent) cases of social media harassment, slander, and extortion; 307 (14 percent) of financial fraud; 116 (5 percent) of threats via telephone; and 186 cases of email hacking. Due to a lack of knowledge about cyber laws and faith in law enforcement, many cases go undetected.

The financial sector looks to be the most vulnerable to massive cybercrime based on the above ranking. Habib Bank Limited (HBL) ATMs were the subject of a sophisticated cyberattack that employed skimming devices to gain access to 579 accounts and steal Rs10 million. 34 The bank was also targeted by cyberattacks in 2015 and 2016, respectively. In recent years, computer hacking and phishing/email scams have become increasingly common forms of cybercrime. These methods are used by cybercriminals to obtain access to a computer network and steal secret or personal data, allowing them to commit fraud. (Siddqui, 2017)

2) Cyberwarfare

State-sponsored cyberattacks that are well-funded, well-organized, and carried out by highly skilled professionals are referred to as cyberwarfare. Such cyber-attacks are typically carried out by governments for political, security, and strategic objectives. Warfare has entered a new phase marked by the strategic use of cyberspace in support of conventional military operations. A 'cyber-enabled physical strike' impacts critical infrastructures before a direct military target is targeted. When Israel took down Syria's air defences in 2007 using a cyber-attack, it was able to sneak up on the country's nuclear site and conduct an unannounced air strike. In 2008, Russia is said to have utilised the internet strategically in its conflict with Georgia over South Ossetia. It was reported in McAfee's 2007 annual report that around 120 countries were developing offensive cyber capabilities—the manipulation of denial of service, disruption or degradation of computer and information systems. On this list, India is unquestionably significant among other important countries such as the United States and China, as well as Russia, Israel, North Korea, and Iran.

India's cyberwarfare capabilities are most likely to target Pakistan because of their long-standing animosity. Since the beginning, India's military strategy has always incorporated a cyberattack stance. "Cold Start Doctrine," India's strategy of limited conflict, includes

seven categories of information warfare, including cyberwarfare (attacks on the adversary's computer systems). Joint Doctrine issued by Indian forces in April 2017 emphasises the importance of cyberspace operations in supporting military operations in a similar way. In order to standardise its cybersecurity architecture, India inked 17 agreements/memorandums of understanding in 2016-17 with a number of countries, including the US, the UK, Israel, France and Australia. More than 100,000 IT employees are annually produced in India, making it one of the major software exporters in the world. It may be able to develop offensive cyber capabilities and wage cyberwarfare against Pakistan with this enormous financial and human resource advantage. With regards to cyberwarfare, former Indian Navy Chief Admiral Suresh Mehta remarked, "Information technology is a well-known advantage to India; utilising this power would be in our benefit." As a result, India and Pakistan may resort to cyberwarfare after waging conventional war on land, air, and sea.

Pakistan has yet to be the victim of a massive cyberattack, although the confrontation between Pakistan and India is becoming increasingly common. The Indian Computer Association and the Hindustan Hackers Organization are two examples of the country's many organised hacker organisations. The use of web vandalism and cyber espionage by India against Pakistan is now under investigation by the FBI. The possibility that India may attack Pakistan's vital infrastructure cannot be discounted. As reported by India's Hindu newspaper, an Indian cybersecurity firm has allegedly penetrated Pakistan's critical infrastructure, including its military systems. In addition, the Indian cyber threat to Pakistan is made more serious by the fact that India and Israel are working together on cybersecurity under the pretext of a broader strategic partnership. As part of this agreement, the two countries have agreed to work together on cybersecurity education and training (HRD). Israel's Talpiot programme acts as an inspiration and a motivator for India's modernization of its cybersecurity infrastructure. ' Israel's military created Talpiot in the 1970s and is notable for training cybersecurity personnel. The Stuxnet cyber-attack on Iran's nuclear programme in 2010 is said to have included it. India is capable of conducting offensive cyber-attacks on Pakistan, to sum it all up. (Dipert, 2013)

3) Hacking Attacks

First and foremost among cyber risks is hacking, the unauthorised entry into computer systems for the purpose of damage, disruption, or any other unlawful action. The motivations and abilities of hackers might vary widely. It's conceivable that hackers are acting out of revenge or ideological campaigns on a national or global scale when they participate in hacking activities. Individuals who hack for personal or political motives, as well as those who hack for criminal or state-sponsored causes, can all be classified as cybercriminals. Hacking is significantly less dangerous than other severe cyber dangers

since it is a disorganised activity with low-level implications. Even so, it's a severe concern since it has the potential to trigger more serious criminality and cyberwarfare in addition to causing significant harm to those who are already vulnerable.

Indian hackers, who appear to be working for or with the Indian government, pose a much greater threat to Pakistan than the actions described above. An increasing number of Denial-of-Service (DoS) assaults have been launched by Indians against the websites of Pakistani government and security organisations since 1998. According to the research, Indian hackers attacked 1600 Pakistani websites from 1999 to 2008. Increased organisation and scalability have been hallmarks of India's Cyber Army (ICA) since its founding in August 2010. Among the 36 Pakistani websites targeted by the hacking group were those of the NAB and NADRA, the Pakistan Navy, and the departments of finance, foreign policy, and education. Hackers from India were claimed to have been eavesdropping on Pakistan since 2010, according to an investigation conducted by a Norwegian cybersecurity firm in 2013. The company said that hackers were going after senior officials in both private sector companies and government agencies. Independence Day and tit-for-tat cyber-attacks between India and Pakistan are common occurrences. According to the ICA, Pakistani hackers defaced 270 Indian websites in retaliation for their 40 attacks on Pakistani websites, including those on the State Bank of Pakistan (CBI). In retaliation for Pakistan's pronouncement of the death sentence for Indian spy Kulbhushan Jadhav, Indian hackers recently hacked 30 official websites in Pakistan. In response to the Pakistani hacker's strike, the Indians reacted with their own. Pakistan and India face an ever-increasing cyber danger from each other. However, the frequency of strikes implies that the attacks on Pakistani websites by Indians are more than simply a nuisance for the time being. The regular hacking exchange between the Indians and Pakistanis might evolve to significant and sophisticated cyber-attacks, which could escalate to cyberwarfare. (Khan, 2017)

4) Cyberterrorism

Internet-based terrorists, many of them ideologically and politically motivated, are gathering in cyberspace to carry out their local and worldwide goals. Communication, propaganda, indoctrination and radicalization are just a few of the actions they may perform via cyberspace. Aside from damaging their rivals' websites and networks, they may also steal money and coordinate operations in the real world using ungoverned cyberspace. As a result of its anonymity, cost-effectiveness, and global reach, cyberspace is a lucrative and convenient tool for terrorists to utilise. Pakistan has seen the worst forms of political and religious terrorism in the years following September 11, mainly from the Tehreek-i-Taliban Pakistan (TTP) and other sectarian groups in the country. This is accompanied by violence and ethnic separatism. Terrorist groups in Pakistan have used

online to brainwash/recruit people and propagate their narrative, despite the fact that they have mostly used physical attacks.

As a result of Zarb-e-Azb, the military operation against several militant organisations in FATA, notably North Waziristan, has destroyed terrorist hideouts and safe havens. As a result, terrorist organisations no longer have as much room to operate as they formerly did. This may encourage them to turn to illegal means such as the Internet to accomplish their malicious goals. To achieve this goal, there are two key considerations to keep in mind. First and foremost, terrorist groups like TTP, ISIS, and al-Qaeda have the means and capabilities to adapt to virtual battle. Second, the security services that are opposed to Pakistan are said to be supporting TTP, which is renowned for its extreme antipathy for Pakistan. As a result of this, the organisation might conceivably utilise cyberspace to carry out retributive actions against Pakistan with the help of international backing. Terrorists may therefore use cybercrime to steal money instead of attacking physical facilities, which they have done in the past. (Shad, 2019)

Pakistan's preparedness for the threat

Although no government can claim to have achieved foolproof cybersecurity in the digital age, states may at least ensure the safety of its IT systems. SYMANTEC, the world's largest database keeper of cyberthreats, issued a dire warning in its March 2018 report: the volume and variety of cyberthreats are only going to grow. According to the report's results, there was an increase in the range of cyber threats in 2017. An rise of 600% in IoT assaults has been seen, according to this report. Malware assaults have surged by 200 percent, while Ransomware, malicious software that encrypts a computer and demands a fee to unlock it, has become available to even the most ordinary criminal. Even more concerning is the fact that in 2017, the number of new mobile malware types grew by 54%, with an average of 24,000 dangerous applications being discovered every day. Information gathered for the Symantec research focuses primarily on cybercrime issues that impact civilians. Consideration of both security and politically motivated hacking heightens the dangers of the current cyber threat scenario. The governments are responding to the ever-increasing and diversified cyber threats with a variety of measures. The UN agency International Telecommunication Union (ITU) assesses security commitment using five criteria: legal, technical, organisational, capacity-building, and international partnership. The International Telecommunication Union (ITU) examines the nations' cybersecurity commitment. When it comes to cybersecurity, there are leading, mature, and beginning states. Singapore, the United States, and Malaysia are the most committed leading states, according to the 2017 GCI report from the ITU. Among the world's most developed

countries in 2017 are India (23rd), China (32nd), Bangladesh (53rd), Iran (59th), and Pakistan (66th). (Kamal, 2017)

Overall, states appear to be stronger at enforcing cybersecurity laws than they are at defending themselves from cyberattacks, according to the survey. In spite of Pakistan's growing commitment to cybersecurity, a look at the country's performance in each of the aforementioned categories paints a bleak portrait. This is especially true in view of the enormity of cyber threats to the country. Pakistan hasn't taken enough legislative measures to safeguard its own security, according to an ITU research on the country's cyber well-being profile in Pakistan. Criminal sanctions for data breaches and other harm to the information system have been introduced by the Electronic Transaction Ordinance of 2002 (ETO 2002). The biggest shortcoming of ETO was its inability to deal with various forms of cybercrime. Due to a lack of support from lawmakers, the Preventing Electronic Crimes Ordinance (PECO 2007) was never made into a law and was eventually repealed in 2009. Preventing espionage, cyberstalking, electronic forgery, cyberterrorism, and cyberhate speech are all included in Pakistan's Prevention of Electronic Crimes Bill 2015. (PECB 2015). Criticism has been levelled at the PECB for curtailing free expression by employing vague wording and allowing the PTA unrestricted authority.

Pak CERT and the Pakistan Information Security Association's Computer Emergency Response Team (CERT) are Pakistan's technical bodies for cybersecurity (PISA-CERT). They provide a wide range of services, from cyber threat intelligence to cybersecurity help and capacity building. Under the auspices of the Cybersecurity Task Force, the Senate Defense Committee also created a Pakistan Research Centre for Cybersecurity. The first-ever National Center for Cybersecurity (NCCS) was established in May 2018 at Air University, Islamabad. The government, on the other hand, lacks a formal structure for enforcing international norms for cybersecurity. There is no certification system for cybersecurity experts or agencies to follow. It is because of this that Pakistan has not yet established an official agency or developed a large number of public sector cybersecurity specialists in accordance with globally recognised norms. There is a major lack of focus, planning and efforts in the country's cybersecurity capacity-building. Pakistan's performance in terms of organisational parameters is yet to improve. Cybersecurity is still lacking in Pakistan, despite the country's 2017 Digital Pakistan Policy. In addition, there is no formal government body or department tasked with ensuring the safety of computer networks. The NR3C, a division of the FIA, handles cybercrimes.

Another factor is the strength of the institution. It's unfortunate that the NR3C has been accused of missing the resources and infrastructure needed to properly track down the anonymous hacking activities of the hackers themselves. Many ethical or white-hat hackers

exist in Pakistan, however they are underutilised. In addition, it lacks a well-established structure of coordination between civil and military cybersecurity agencies. In order to deal with cyber threats as a global concern, international collaboration and coordination are required. This is why the ITU has been unable to build a UN-wide framework for cybersecurity consensus among member nations. In any case, it encourages regional and multilateral cooperation among member governments in the areas of cybercrime investigation and prosecution. Pakistan's cyberlaw allows for 'international collaboration' in this area. Take part in International Multilateral Partnership Against Cyber Threats (ITUIMPACT) and Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). However, in international discussions and accords, cybersecurity does not appear to be a significant priority for the government. (Campbell, 2017)

Conclusion

Many opportunities and difficulties arise from today's world's ICT revolution and internet's widespread use. ICTs have brought with them a wide range of cyber dangers, from hacking to severe and organised crimes to cyberwarfare. Both governmental and commercial organisations in Pakistan are rapidly expanding their use of online administration and service platforms. Because of the hostile regional and internal security environment and the absence of cybersecurity, the country is vulnerable to all of the aforementioned cyber threats. Pakistan is one of the most often assassinated countries in the world. Hackers from India frequently target Pakistani official websites because they act in an organised fashion. In recent years, Pakistan's financial industry has been the target of an increasing number of cyberattacks. Terrorist groups may also use cyberattacks to retaliate against Pakistan. As conflict moves from land, air, sea, and space into the fifth domain — cyberspace — Due to India's cyber defence strategy, historical conflicts, and a history of hostilities between the two countries, Pakistan is better equipped to counter Indian cyber warfare.

UN-specialized agency ITU, which analyses governments' cybersecurity commitment, ranked Pakistan 66th on the GCI of 2017 as a developing state. Even if the country's legal measures for cybersecurity have improved, it has made little headway in setting up technical organisations, organisational frameworks, institutional capability, or international collaboration. That's why it's imperative that Pakistan prioritise cyber preparation on its policy agenda, as well as take exceptional measures to improve cyber security. As a result, the most important step is to develop an e-governance and cybersecurity strategy that works in tandem. Cybersecurity policies should be comprehensive and integrated, with the goals of all relevant economic, administrative, and security organisations being aligned. Secondly, there is a lack of coordination and collaboration among the many security agencies involved in cybersecurity initiatives. An integrated institutional framework

linking the infrastructure and services of key agencies and fostering coordination and collaboration are needed in Pakistan to overcome this anomaly. Finally, Pakistan needs to talk about technology and cybersecurity education for internet users. Human capital may be effectively leveraged in one way, while cybersecurity awareness can be educated and sensitised in another.

References

"Almost all Pakistani Banks Hacked in Security Breach, says FIA Cybercrime Head," Dawn, November 6, 2018, https://www.dawn.com/news/1443970.

"Global Cybersecurity Index (GCI) 2017," International Telecommunication Union, last modified October 5, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-GCI.01-2017-PDF-E.pdf.

"Information Economy Report 2017: Digitalisation, Trade and Development," United Nations Conference on Trade and Development (UNCTAD), October 2, 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

"Internet Security Threat Report," Symantec, vol. 23, 5-6, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

"Microsoft Malware Infection Index for Asia Pacific," Microsoft Asia, https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016- highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoftreport/#sm.0001c8j2ld213dupxw82ps93k6pbp

"Microsoft Security Intelligence Report (January – March 2017, Volume 22)," Microsoft, August 17, 2017, https://www.microsoft.com/en-sa/security/Intelligencereport

"Telecom Indicators," Pakistan Telecommunication Authority, https://www.pta.gov.pk/en/telecom-indicators

"Telecom Indicators," Pakistan Telecommunication Authority, last updated February 2018, http://pta.gov.pk/en/telecom-indicators

"The Mobile Economy 2018," GSM Association, February 2018, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/2/The-MobileEconomy-Global-2018.pdf

Ahmed, A. (2017). "Pakistan Among Top 10 Economies in Terms of its Internet Users," Dawn, October 4, 2017, https://www.dawn.com/news/1361586

Andress, J. and Winterfeld, S. (2014). "What is Cyber Warfare," in Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (Waltham, Massachusetts: Elsevier, 2014), 3-5.
Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons.

Campbell, R. J. (2017). The smart grid and cybersecurity: Regulatory policy and issues. *Current Politics and Economics of the United States, Canada and Mexico*, *19*(2), 169-200.

Cassidy, J. (2013). Why Edward Snowden is a hero. *The New Yorker*, *10*.

Clarke, R. and Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It (New York: Harper Collins Publishers, 2010).

Dipert, R. R. (2013). Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. *Journal of Military Ethics*, *12*(1), 34-53.

Fang, B., Fang, & Zhang. (2018). *Cyberspace sovereignty*. Springer Singapore.

Futter, A. (2016). Is Trident Safe from Cyber Attack?. *European Leadership Network*, *1*.
Ghernaouti, S. (2013). "Cyber Conflicts, Cyberwars and Cyber Power," in Cyber Power: Crime, Conflict and Security in Cyberspace (Lausanne, Switzerland: EPFL Press, 2013), 176.

Government of India, Integrated Defence Staff, Indian Army Doctrine 2004, October 4, 2004, http://ids.nic.in/indian%20army%20doctrine/indianarmydoctrine_1.doc

Government of Pakistan, Prevention of Electronic Crimes Act, 2016, August 19, 2016, http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

Hansen, L. and Nissenbaum, H. (2009). "Digital Disaster, Cyber Security and the Copenhagen School," International Studies Quarterly 53: 1155-1175.

Kamal, D. (2017). „Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill". *Jinnah Institute, Policy Brief*, 3-8.

Khan, A. (2017). "Cyber Securitisation: Need of the Hour for Pakistan," South Asia

Journal 24 (2017), http://southasiajournal.net/cyber-securitization-need-of-the-hour-forpakistan/

Khan, R. (2016). "Cyber Laws in Pakistan," Supreme Court of Pakistan, http://supremecourt.gov.pk/ijc/articles/10/1.pdf.

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), 1-19.