Vol. 4 No. 1 (2026)
ISSN 3007-3170(O)
ISSN :3007-3162(P)
Social Sciences & Humanity Research Review

Criminological Perspectives on Cybercrime and Cybersecurity Challenges in Pakistan: Implications for National Security and Stability

Saima Noor[1], Warda Maqsood[2], Areeba Azeem[3]

[1]Lecturer, Department of Criminology, The University of Lahore, Lahore
Email: saima.noor@crim.uol.edu.pk
[2]Lecturer, Department of Criminology, Lahore Garrison University, Lahore
Email: wardamaqsood@lgu.edu.pk
[3]Lecturer , Department of Criminology, Lahore Garrison University, Lahore
Email: areebazeem@dfrsc.lgu.edu.pk

ARTICLE INFO

Keywords:
Cybersecurity, Digital Infrastructure, Identity Theft, Cyberattacks, National Security

Corresponding Author:
Saima Noor,
Lecturer, Department of Criminology, The University of Lahore, Lahore
Email:
saima.noor@crim.uol.edu.pk

ABSTRACT

Pakistan's greater than ever dependence on digital assets and use of cutting-edge technology has escalated cyber security risks. A number of cyber security risks globally and in Pakistan are data breaches, cyber attacks, identity theft, cyber warfare and cyber espionage. These threats in Pakistan pose risks to critical government and military assets as well as risks to commercial, industrial and financial sectors. Contributing to these cyber security threats are lack of technological proficiency, obsolete technology and general lack of knowledge on the risks of cyber threats. Through cyber challenges, this paper aims to highlight the challenges of national security and financial security threat and some ways of mitigating these challenges. This research employs qualitative research that is phenomenological in nature by using secondary data which is exploratory and descriptive in nature. There is need to formulate and implement comprehensive and sophisticated legal instruments, and more research is required to optimally use legal instruments to digital the assets of society. As society digitalizes, the mitigation of these threats is paramount to the society's resilience, the economy, the national security and technological advancement of the society.

Introduction

Information Technology Security, also called Cybersecurity, is a field concerned with preventing unlawful entry, attacks on, destruction of, theft of, and other harmful incidents involving systems, networks, applications, and data. Cybersecurity seeks to protect the confidentiality, availability, and integrity of data while trying to mitigate the risks and vulnerabilities to a society's technological systems. Cybersecurity involves the protection of data and computer systems from damage. More specifically, Cybersecurity is concerned with the detection and tracking of anomalous activities, cyber-attack damage mitigation, and the

recovery of systems and data that have been damaged during a cyber-attack. Cybersecurity is achieved with the combination of various activities and best practices to protect digital assets from a cyber-attack. This period has become known as Information Age when there are more non-traditional threats like cyber attacks as opposed to more conventional threats. The increase in communication and informational technology has made cyber warfare risk to national sovereignty and security due to the threat on national frontiers which has made it a significant issue. Even though cybercrime is a relatively recent phenomenon and compared to traditional crime it is newer, it has an equally adverse effect. Based on one risk survey report, there were 7.9 billion data records exposed due to data breaches in the first 9 months of 2019 and the figure more than doubled versus the same period of 2018. Medical services, retailers and public entities were the most breached sectors and there are malicious people behind the breaches of these sectors. These sectors are of particular interest to cyber criminals, in as much as the hold financial and medical records. Although any organization has a weak control of its networks and is exposed to cyber crime, there are sectors which are more susceptible due to the financial, medical and personally identifiable data of its potential customers.

As reported by Canalys in the second quarter of 2023, the global cybersecurity market continues to expand, with a 11.6% increase year-on-year at $19 billion. Following a $71 billion valuation in 2022, the market is expected to grow to $78.9 billion in 2023 (Gately, 2023). Given the increase in cyber threats, governments around the world have assisted various entities in the design and implementation of defensive network protection policies. For example, in the U.S., the National Institute of Standards and Technology (NIST) developed a Cybersecurity Framework that focuses on the active monitoring of all computing devices to limit the proliferation of malicious code and to improve early detection (Gately, 2023). Cybersecurity, in particular, aims at the mitigation of three threats, which include; cybercrime, cyber-attacks, and cyber-dependent threats. Of particular concern is the diversity of criminals, both individuals and groups, that disrupt systems for monetary gain. Panda Security 2018 framework defined cybercrime in two categories; crimes that target systems and devices and crimes that execute (illegally) through a device.

Digital technology has opened the world to unprecedented opportunities. However, there has been an accompanied rise in cybercrime, state-sponsored cyber attacks, digital terrorism, and `hacktivism. The latter has prompted some to consider cyber warfare to be the level of conflict in what has been termed fifth-generation warfare (Sadleer, 2012). The increased digitalization of critical services in Pakistan has also contributed to the increased exposure to cyber incidents, and has placed Pakistan among the bottom seven countries in the world in terms of the state of cyber security. The absence of any significant change has resulted in an unchanged overall state of cyber security in Pakistan. Hence, this paper aims to consider the nature of the cyber threats to the national security of Pakistan. This paper also identifies the patterns, norms and mentality within the national security culture, that in the absence of the complementing security to the digital assets, the culture will not provide any help in the digital security of the assets. This paper will also consider the constraints that the Government of Pakistan faces in combating Cybercrime within the context of the Digital Pakistan framework, and will offer some recommendations. Among the questions this study seeks to address include the following: What cyber security threats exist to the Pakistan National Security? What key cyber security challenges exist to the critical and major sectors of Pakistan? To what extent has the Indian Factor emerged as a cyber threat to Pakistan? In an attempt to help answer these questions, this paper relies on secondary materials such as books, and research and seminar papers.

Literature Review: The initial analysis of the digital dangers and challenges pertaining to e-government and e-governance served as the foundation of this discourse analysis, starting

with Memon (2016). Memon emphasized the need for parliamentarians and service-delivering entities structured to improve Memon's digital security suggestions and focus on the protection of citizens from threats to the digital security of citizens of the Pakistan system, designed to assist policymakers. Memon (2016) indicated the digital security of e-governance and associated services, along with the risks and challenges of e-governance and e-governance. Aslam and Tariq (2013) established the foundation for the analysis of the complete spectrum of cyber threats, from the defacement of a single website, and/or the loss of access to all content that a website established, to sophisticated and persistent Threats (Aslam & Tariq, 2013). These threats could plan, organize, and execute a cyber attack on a system. In the study that includes the title of this article, Aslam &Tariq (2013) evaluated the focus of Pakistan to respond to these threats, and the challenges of Pakistan's public sector. Deficient and weak cyber security, the protection of an information system from intrusion, or the unauthorized access of a system of information, as well as the structure of an organization, target the cyberspace of Pakistan. Aslam and Tariq (2013) recommended that the public, as well as the heads of some of the associated bodies, especially, as the Aslam and Tariq (2013) title of the article suggests, the public sector, focus on establishing public, or a series of public, high cyber security units in different strata of the public sector.

Ahmed, in her 2022 article titled, "Cyber Security threat and Pakistan preparedness: An analysis of National Cyber Security policy 2021," critiques the National Cybersecurity Policy of Pakistan in relation to preparedness for active cyber threats. Qualitative methods and policy documents which she elaborates on, inform the policy critiques for which she examines the potential policy effectiveness in relation to the more pressing issues of the policy. Imran and Murtaza in 2021 titled, "The rise of Cybercrime in Pakistan: A threat to Pakistan National Security," assess the emergent threat of cyber warfare technology to Pakistan’s National Security and the Increase of Pakistan’s Cybercrime. The research assessment recognizes Pakistan's vulnerability to multiple global state actors such as China, Russia, India, Israel, and the United States, due to a significant deficit in modern IT frameworks, and inefficient cyber security and IT educational systems. Their research findings indicated a clear and pressing deficit on the need to enhance the security of cyber systems. The study by Shan Ali titled as Impact of Cyber Terrorism on Pakistan’s National Security from 2022, discusses the growing phenomenon of cyber terrorism, detailing how terrorists may take advantage of the gaps in the internet to coordinate, recruit, and communicate bypassing national borders. Ali also discusses how even the absence of technological sophistication, terrorists could use the internet to undertake disruptive activities, thereby jeopardizing the safety of states.

The 2021 article by Khathan Patel and Dhaval Chudasama titled as National Security Threats in Cyberspace discusses the potential consequences to the world from the lack of cybersecurity. The authors discuss how the growing interconnectivity of devices and systems poses the world to even greater risks of being attacked. The authors highlight how most cyber crimes today are transactional or involve the stealing of sensitive information whereby cyber criminals work from any nation in the world. The authors explain the necessity of collaborating and sharing information in a bid to help counter cyber crimes and to help states establish a safer cyberspace.

In a contribution to the 2018 edited volume titled "Cyber Space Management in Pakistan," Dr. Tughral Yasmin identified the gaps in Pakistan's cybersecurity policy as well as possible options for formulating policy responses to the additional threats to Pakistan's cybersecurity. Yasmin argued that Pakistan's unregulated cyberscape meant that Pakistan was vulnerable to a range of threats, including cyber-attacks that disrupted government operations and caused economic inefficiencies.

Mr. Rizwan, in his 2022 article titled "Cyber Threat in a Contemporary Era: Challenges for the Security of Pakistan," surveyed the possible consequences of cyber-attacks on critical infrastructures such as the energy sector, the military, and the financial verticals of Pakistan. Rizwan noted that due to Pakistan's heavy reliance on digital technology, the cyber threats to the country had been aggravated. He pointed out that the country had tried to meet the challenges circumventing the available cybersecurity defensive options.

On the subject of Pakistan's cyber threats, Ashraf in her 2021 work, "Cyber Threats to Digital Pakistan," reaffirmed that the general populace's growing reliance on the internet and computers had opened Pakistan's cyberspace to exploitation by both state and non-state actors. She argued that in response to the threats, the state had a greater need to enhance its cybersecurity framework. Lastly, in his article “Pakistan and Cyber Crime: Problems and Preventions (2019),” Hamid Asmat elaborated the necessity of making amendments to current cybercrime legislation and cultivating the potential of international collaboration in the fight against cybercrime. Asmat acknowledged the difficulties in tracking cybercriminals due to the absence of computer forensics, an area of study underdeveloped in several countries, including Pakistan. He advocated for the establishment of strong anti-cybercrime legislation and policies to reduce the risks associated with this phenomenon.

Extensive Growth of Cyberspace in Pakistan

As of January 2023, there are 87.35 million internet users in Pakistan, which amounts to growth by approximately 4.4 million users on an annual basis between 2022 and 2023. The degree of internet penetration in the country was 36.7 in January 2023 and there were also 71.70 million social media users, of which 53.20 million were aged 18 and older as of the start of the 2023 calendar year (Kemp, 2023). In its 2023 report, the Pakistan Telecommunication Authority (PTA) stated that there are 191.8 million mobile internet users and 5.9 million mobile subscribers have been added since 2022 (Kemp, 2023). This surge in internet and mobile connectivity has also increased the outreach of the Pakistan's digital security risks as users are becoming more active online.

The National Database and Registration Authority (NADRA) is one of the key organizations in Pakistan which holds and manages sensitive data comprising individual citizens. This sensitive data is of paramount importance to the country due to its value to national security and more specifically, counter terrorism. NADRA disseminates this data to other governmental institutions (Khawar, 2019). The nature of this data, however, poses some risks, which include the possibility of cyber attacks that may aim at debilitating national structures, illicit/personal data theft, or other unlawful enterprises.

Just like the other IT-based sectors in Pakistan, banking services also attract the interest of cyber criminals. This area is also the most susceptible to cybercrime due to the increasing number of customers in this sector. Cyber criminals may breach cyber walls and perform the fraudulent transactions, and steal credit card information or account details. The increased cybercrime is a danger due to the rapidly evolving digitization of Pakistan's banking and financial services sector. Online trading and mobile banking platforms pose a host of cybercrime threats. The mobile banking services and the Pakistan Stock Exchange are also part of a network of financial services placed in a vulnerable position to online crimes (Khawar, 2019). The massive integration of information and communication technologies in Pakistan creates what can be referred to as cyberspace and the extensive ICT use creates a host of other cybersecurity issues. What can be done to protect digital infrastructures? What can individuals or organizations do to mitigate cyber threats? More awareness is needed to address the challenges posed by digital infrastructures. Once basic awareness is in place, the implementation of modern techniques and technologies designed to protect digital infrastructures will be easier.

According to the Global Cyber Security Index, Pakistan's Cyber Security Preparedness level is 79 out of 193 countries overall. According to researcher Rafay Baloch, the existing legislation on Cyber Security, namely the "Prevention of Electronic Crimes Act" (PECA), is not functioning properly. Baloch explains that Pakistan does not have a targeted cyber forensic laboratory that can provide legal evidence, as stipulated in PECA's Section 40. Moreover, PECA's Section 49 mandates the creation of national and industry-specific Computer Emergency Response Teams (CERTs) dedicated to the protection of the country's cybersecurity infrastructure (Emma, 2021) Furthermore, Pakistan is also highly susceptible to malware. Based on the Microsoft Malware Index for Asia Pacific (2016), Pakistan ranked first in malware susceptibility among countries, including Indonesia, Bangladesh, and Nepal. The country has experienced many of the major malware families including Gamarue, Skeeya, and Peals, which are notorious for stealing private data, installing other malware and granting remote access to infected systems by hackers (Microsoft, 2016).

Besides the concerns of possible malware, Pakistan has also faced several significant cyber attacks, one of the most notable being the August 2021 incident involving the Federal Board of Revenue (FBR). This attack resulted in the loss of taxpayer information, thereby forcing the FBR to shut down its data center to carry out data restoration activities. Recovering the information loss prompted the government to involve an Irish Consultancy and Tania Aidrus to analyze the cyber incident & propose actions to enhance the FBR systems protection (Business Recorder, 2021). This incident clearly indicates that cyber warfare is an evolving phenomenon, and Pakistan has to give it serious attention.

Major Cyber Sectors of Pakistan

A number of sectors within Pakistan's cyberspace domain are vital cyber-attack targets. These sectors include:

1. The bank and finance sector: Cyber phishing malware and ransomware remain favorite targets of cyber criminals. In Pakistan's banking industry, cyber attacks increased by some 114% during 2024, mainly attributed to ransomware and phishing. Groups like Lazarus and SideWinder are APT's that attack this sector: (Profit, 2024).

2. Telecommunications: Pakistan's telecom sector especially National Telecom CERT and National Telecom Security Operation Centre (SOC) addresses and improves cyber defense posture within this sector. However, the sector is still under attack. The Pakistan Telecommunication Authority (PTA) noted cyber attack incidents increased in 2023. These attacks are recorded as 200 attacks of ransomware, 300 DDoS (Distributed Denial of Service) attacks, 720 incidents of malware attacks and 550 phishing attempts (ProPkstaff, 2024).

3. Military and Government: Government systems and military infrastructures are especially at risk from identity theft, espionage and cyber attacks. In 2024, one such event occurred, a major cyber attack on Federal Board of Revenue (FBR), where millions of records of taxpayers were breached. The obtained records were subsequently sold by the hackers on a Russian website (ProPkstaff, 2024).

4. Healthcare: In the healthcare sector, disruption of services and cyber attacks on sensitive patient data, especially, are major concern. In 2023, Pakistan's healthcare sector, particularly, the APT attack Healthcare providers in Pakistan, such APT attacks on the healthcare sector were of particular concern as they compromised the patients' data and Healthcare services were impeded (ProPkstaff, 2024).

5. Manufacturing/Production: The same goes for various industrial sectors, especially the major sectors of production. There is an increasing phenomenon of cyber attacks in industrial sectors. Key sectors of manufacturing are disrupted by ransomware and APT groups, which cyber attack supply chains and production lines. Such attacks are a form of cyber extortion. Cyber extortion is a phenomenon that negatively impacts the capability of industries to function (ProPkstaff, 2024).

Challenges, Risks, and Threats to Pakistan's Cyberspace

Pakistan's cyberspace operates under a multitude of threats to its financial stability, overall security, and safety of its populace which include:

1. Cyber Crime- Cyber crimes in the form of the use of business malware, financial crime, data theft, espionage and other forms of cyber criminal activity and the victimization of companies and businesses is a notable threat to the security of Pakistan. Such crimes cause severe losses to the victim companies, disrupt business operations, and cause the loss of some data to companies (Shad 2019)

2. Cyber Terrorism: Cyber attacks and the internet pertaining to the country's critical infrastructures and foundational physical systems, energy threats, and transportation systems where the attacks can be used to cause and/or threaten instability in the systems (Shad 2019).

3. Cyber Espionage: Specifically, state supported cyber espionage attacks pose a threat as foreign entities target the governmental and military systems along with other private domains to take sensitive data needed to obtain or preserve primary stature and/or control with no regard to the security and protection of the state (Rafique, 2019).

4. Foreign Cyber Attacks: The Pakistan Foreign Affairs Committee is concerned about the potential risk of Pakistan being a target of hostile foreign cyberattacks. The committee has suggested the government improve the country's cyberdefenses by creating more specialized cybersecurity research and development. Unlike Israel and the United States, which have specific government entities charged with addressing cybersecurity (CISA and NSA, for example), Pakistan has no institutional arrangement securing its cyberspace.

5. Dependence on Foreign Technology: Pakistan's cybersecurity dependence on foreign borrowed technology is have cause for concern. The digital infrastructure Pakistan uses is largely supplied by more technologically advanced countries, with much of the software, hardware, and information technology (IT) equipment being foreign. This dependence on foreign technology is a threat to cybersecurity in Pakistan, considering the many systems and portals used within Pakistan are provided by foreign sources.

6. Shortage of Cybersecurity Proficiency: The Pakistan National Cyber Security Policy 2021 reports that the country experiences critical cyber defense resource deficits, cyber defense skill deficits, and cyber defense resource coordination deficits. The most disconcerting lack is the shortage of sophisticated cyber defense human capital, which is coupled with considerable dependency on foreign products and technology. The aforementioned circumstances culminate with the absence of robust ownership and leadership at the most senior levels of government. Such circumstances are further complicated disconcertingly by the state of the cyber defense of the country and the cyber defense of the country's national security (National Cyber Security Policy, 2021).

1. Cybersecurity Threats To Pakistan's National Security

2. Digital networks, the steady advancement of the systems underpinning them, as well as the improving defense technologies, are all intertwined with national security. Therefore, designing a proper digital defense is becoming more and more difficult as cyber threats are almost analogous to threats posed by other forms of warfare. The world's nations, in anticipation of these threats, are enhancing their capabilities in cyber warfare. This involves recruiting personnel with specialized knowledge and skills, implementing cyber battle command set-ups, and investing in cyber defense technologies (both offensive and defensive). Investment in cyber defense systems as a measure of enhancing national defense is a significant consideration due to the developments in modern communications. As Jeff Koseff noted at the 10th International Conference on Cyber Security in 2018, improving cybersecurity contributes to national security in two ways: it makes defense systems more robust and thus makes it more difficult for cyber attacks to succeed, and it acts as a deterrent by reducing the probability that potential adversaries will proactively launch cyber attacks.

This is however, not the case with Pakistan as its national security continues to suffer from multiple vulnerabilities in cyber security.

3. Cyber Threats and Critical Infrastructure: Transportation, communication, and energy infrastructures comprise the backbone of national security. Their disruption causes national emergencies and massive disorder. Absence of such infrastructures cripples the flow of everyday activities and disrupts commerce and governance. This, in turn, renders the country vulnerable to attacks and further instability (Sahar, 2021).

4. Cyber Threats and the Economy: The economic costs of cyber attacks are staggering and the economic activities of an entire nation can be seized by an attack/disruption. The attacks impact the economic core of a nation, emerging and established, and self-governed. The financial costs of cyber attacks are crippling and directly affect the economic and national security of a nation (Sahar, 2021).

5. Cyber Threats and Information Domination: Cyber espionage (especially state-sponsored) is a very serious threat to national security. It compromises sensitive military and state information and resources. It involves cyber-invading the private and public sectors, exposing private and military structures and defense systems, and neutralizing high governance systems. The acquisition of sensitive information by adversaries threatens national security and gives opponents the upper hand in future confrontations (Sahar, 2021).

6. The acts of cyber terrorism, which strike important infrastructures, distribute false information, and instill and spread fear and worry, pose an unprecedented danger (Adeel, 2021). Cyber terrorism has the potential to create panic and instability in an already unsafe country. It has the potential to create and reinforce an already unbalanced social order and create a high level of uncertainty, thereby, threatening the national security of the state.

7. There are no limits to what could happen when individuals connect to private networks, including those within government, and obtain the restricted information within (Gov, 2021). Identity theft and other cyber criminal activities remain a possibility. Such violations of databases put the public confidence in government systems at risk. It, also, jeopardizes the national defense by making highly sensitive information available to an enemy.

8. A full-fledged cybersecurity framework, reinforced by infrastructure, real-time surveillance, and preemptive defensive actions, is required to address such vulnerabilities and secure Pakistan’s National Security. With every new technological implementation, especially e-Governance and ICT, cybersecurity weaknesses stand to exacerbate. These weaknesses jeopardize the Nation’s security, and as a developing economy, the potential threats are concerning. No other country is as closely monitored as Pakistan, which adds context to the Nation's cybersecurity concerns. Internationally, cyber-espionage against Pakistan's infrastructure is a known activity by India and the USA.

9. A report from The Intercept asserts that the U.S. National Security Agency (NSA) has conducted espionage on Pakistan by employing programmers and hackers to extract valuable information from the Pakistan Telecommunication Corporation (PTC) pertaining to Pakistan’s civilian and military authorities. SECONDDATE is the program that allegedly surveilled and redirected users’ inquiries and, while they're monitored on the NSA servers, infected the users’ computers with a virus. For example, the users’ computers were routed to NSA-controlled servers. (Dawn, 2016). During this case, the protective perimeter of Pakistan’s cyberspace became unprotected, and the need to strengthen protective digital measures to safeguard the national security of the country became evident.

Indian Cyber Involvement in Pakistan

One of the focuses of India's Cold Start doctrine is engagement with Pakistan through what is now called Hybride Warfare. Hybrid Warfare is an integrated form of warfare whereby the non-kinetic domains of warfare have now become primary focus areas due to cyber warfare. The cyber warfare is aimed at destroying the target's economy, fuelling political instability,

weakening the military, engineering social problems such as unemployment and inflation, fuelling and orchestrating corruption and terrorism, undermining the social order, and passing the state. Within the context of the social-political matrix, the warfare is termed as "fifth-generation warfare". "Minhas" (2019) indicates that such warfare is characterised by the low intensity social-political conflicts of the target and the focus is on The socio-political fault lines of the target.

In 2015 India set aside 775 crores for improved cyber security capacity (Rafique, 2015). India will continue to improve its digital defenses, but is also exercising cyber offenses against Pakistan. Meanwhile, Pakistan is technologically underdeveloped, unprepared to react to hacktivism, and thus has critical gaps in its governmental and military cyberspace. One case in point is the hacking of the Ministry of Foreign Affairs of Pakistan's websites by Indian cyber hacktivists in 2016, apparently a cyberspace retaliation for the Pulwama terrorist attack against Indian military personnel by Jaish-e-Muhammad, who was based in Pakistan (ecouncil.org). In 2020, Pakistani security services reported a cyber attack directed at military and government officials. Cyber security in Pakistan underwent a breach attributed to Indian intelligence services. It was the "Confucius" hacker group, of which at least the Indian government is believed to provide support, that focused on certain Pakistani military officials, the Nuclear Regulatory Authority, and the Atomic Energy Commission (Ahmed, 2023).

Moreover, the Pakistan authorities also had to endure several DDoS attacks, including one in 2008 which resulted in the State Bank for 21 consecutive days. In 2018, data pertaining to 22 banks in Pakistan was being sold on the dark web, while the ATM systems of Habib Bank were hacked in December of the same year. In May 2020, an Iranian hacking group known as 'Greenbug' aimed to access files located on the computers of three telco providers in Pakistan (Ahmed, 2023). By 2023, an APT group labelled as Rattlesnake had an agenda centered on Pakistan's Navy web portal aimed at the extraction of secret data. Also, a power disruption recorded in January 2023 was a cause for concern regarding the potential exposure of Pakistan's national electric system to hostile cyber interventions. Although the disruption was blamed on system faults at first, later inquiries indicated that the power outage was possibly the result of a hostile cyber operation instead of system faults (Salik, 2023).

While the Pakistan Telecommunication Authority (PTA) is charged with the responsibility of blocking illegal and harmful websites, the PTA has failed, in particular, to blocking potential threats such as YouTube. The PTA has not been able to minimize potential cyber threats. In 2012 and 2013, the PTA had blocked 15,000 websites, but the PTA's inability to appropriately control the risk of online content to the Pakistanis remains a security risk (Salik, 2023).

Indian Partnerships with Israel and the United States

Prime Minister Benjamin Netanyahu explained Israel's leading position in cyber defense technology during one of his addresses in 2019. Israel has a booming technology sector alongside a thriving military industry which means Israel has a lot of cyber defense technology available. Israel also has a lot of cyber defense technology to sell. As a result of this partnership, many have begun to express concern over the cyber defense capabilities Israel has equipped India with when developing cyber campaigns against Pakistan. The Israeli partnership bolsters the cyber capabilities of India concerning Pakistan.

The cyber informative assaults India is conducting is substantially disturbing Pakistan rather than China. The rise in cyber activities from China which is directly impacting India has also ignited the possibility of cyber informative assaults against China. Countries across the world such as the United States, the United Kingdom, and Israel have also begun to strengthen the cyber informative assault capabilities partnered with India (Babar, 2022). The strengthening of Israel & India partnerships continues to raise India's efforts to assault Pakistan's cyber campaigns. The IISS has written many cyber informative undercover operations concerning India's cyber and digital intelligence capabilities. Most of the predictions only include

Pakistan because a majority of India's focus wanders about Pakistan. With this new alliance, India's lack of ability towards cyber assaults has now created a new set of complications in Pakistan.

Measures Taken for Cybersecurity Protection in Pakistan

In recent years, cyber threats have increased in both number and complexity. In response, Pakistan has undertaken a number of initiatives designed to improve the country's cybersecurity policy. The first step in this direction was the introduction in Parliament of the Prevention of Electronic Crime Act (PECA), which was signed into law in 2016. PECA established a system of sanctions against cyber law violators, including unauthorized access to data, data theft, cyber fraud, and other cyber-related crimes. PECA further called the establishment of Pakistan's first Computer Emergency Response Team (PAK-CERT), which has been operational since 2000 and assists law enforcement agencies in the identification of cyber intruders and the reduction of security vulnerabilities.

Moreover, Pakistan developed its first National Cyber Security Policy in 2021 to build an integrated cyber governance system. Still, there are notable obstacles to be overcome. No single entity exists to address cybersecurity issues and to provide the PM with recommendations on cyber dangers. There is an absence of cyber threat awareness among policymakers, and there are no proposals beyond the Cybercrime Bill that articulate an adequate response. The National Cyber Response Center (NR3C) in the Federal Investigation Agency (FIA) is responsible for cybercrime, but its limited jurisdiction means that it can't respond to cyber crises in an effective manner at the national level. Also, Pakistan's membership of the UN Group of Governmental Experts on Information Security has not led to significant public policy extremities or much effective collaboration on cybersecurity at the international level (Salik, 2023). To make this lack of resources more glaring, there has been no cybersecurity specific budget for online safety initiatives. Pakistan may be participating in international security promises, but for practical steps and collaborative governance, it is significantly behind. There is much to be done to provide a safe cybersecurity framework that deals with threats from within the country as well as from abroad.

Conclusion

Patterns of warfare continue to change with the emergence of new, unpredictable factors, especially in the area of conflict. It is now a priority for non-state actors motivated to make a profit, in addition to the states whom focus on it as well. Digital crime which includes the illegal movement of money on a massive scale, the hacking of a country's critical infrastructure, the breach of personal privacy, and the infiltrating of a country's systems is also a growing concern. As the world continues to expand on the use of the Internet, the scope and scale of cyberspace crime continues to grow. It also has a unique and Global reach which makes it a collective and cooperative problem needing a Global framework for cyberspace crime.

Pakistan's unique role as a state with atomic capabilities and a critical geopolitical position in the world makes him susceptible to these effects. The new upsurge of Internet users coupled with a growing Digital Banking and a multi folded reliance on Online Security makes the country even more vulnerable in the Digital world. The country needs to initiate and develop a comprehensive framework for Digital Security which aims to protect the country from the loss of Financial Data, Identity Theft and Cyber Espionage on Critical Infrastructure. Also it is a dire need of the time to make legislative and policy frameworks with a better coordinated approach to form collective responsibility for the protection of Digital Security in the country.

Recommendations

As an important first step in strengthening its cybersecurity, the government of Pakistan should focus on building the country's cyber-security infrastructure. As of now, Pakistan does not have a dedicated central agency whose remit is cyber security. Nations such as the USA

have a Cybersecurity and Infrastructure Security Agency (CISA), and Israel has Unit 8200 and the National Cyber Security Authority (NCSA), which protect and manage the cyber dimensions of their countries. In Pakistan, the NR3C (National Response Center for Cyber Crime), which falls under the Federal Investigation Agency (FIA), has cybercrime in its jurisdiction. However, the NR3C is under-resourced, which restricts its ability to defend the country's sensitive data. Moreover, Pakistan needs to enhance its legal framework on digitally induced threats. Whilst empty of necessary focus, the PECA (Prevention of Electronic Crimes Act) was enacted in 2016. The country needs to move towards a more comprehensive framework of protective legislation that supports the primary and secondary sectors in a country in protecting their digital infrastructure so as not to become a victim of a cyber breach. There should be a specific focus on Key Sectors (Governance, Energy, Health, and Finance) to ensure that their digital infrastructure and data is not compromised.

Sensitive infrastructure in Pakistan needs a thorough threat analysis along with focused actions aimed at securing the country's integrated systems. Protection of systems is weakening because of the increasing use of AI and integrated systems in organizations. Cybersecurity experts comment that most organizations keep cybersecurity at the bottom of their agenda unless compelled by legislation.

In Pakistan, the most pressing and the most actionable focus of the legislature should be on the threats to the digital environment of Pakistan. With the increasing challenges of cybersecurity, Pakistan is unable to protect its citizens, its economy, and its critical infrastructure. Pakistan's digital space must be protected to ensure a safe and resilient future.

References

Adeel, M. (2021). The rise of cyber terrorism and its impact on national security. *Journal of Strategic Security, 14*(2), 45–67.

Ahmed, M. (2022). Cyber security threat and Pakistan preparedness: An analysis of National Cyber Security Policy 2021. *Strategic Studies, 42*(3), 78–94.

Ahmed, S. (2023). *Cybersecurity and national defense: The role of state actors in digital espionage*. Security Studies Press.

Ali, S. (2022). Impact of cyber terrorism on Pakistan's national security. *Perspectives on Terrorism, 16*(1), 112–128.

Aslam, B., & Tariq, M. (2013). Cyber threats and incident response capability: A case study of Pakistan. *International Journal of Cyber Security and Digital Forensics, 2*(2), 1–12.

Asmat, H. (2019). Pakistan and cyber crime: Problems and preventions. *Pakistan Journal of Criminology, 11*(4), 33–50.

Babar, M. (2022). *India's cyber capabilities: A focus on Pakistan*. International Institute for Strategic Studies.

Baloch, R. (2021). Implementation of cyber laws in Pakistan: Issues and challenges. *Pakistani Law Review, 8*(1), 22–40.

Business Recorder. (2021, August 20). Cyber-attack on FBR: Analysis and future precautions. https://www.brecorder.com/news/40168919

Dawn. (2016, May 23). Cyber espionage: The US surveillance of Pakistan's telecommunication infrastructure. https://www.dawn.com/news/1259855

Emma, J. (2021). Cybersecurity and the Prevention of Electronic Crimes Act in Pakistan. *Journal of Information Policy, 11*, 345–367.

Gately, M. (2023). *Canalys report on cybersecurity market trends Q2 2023*. Canalys.

Government of Pakistan. (2021). *National cyber security policy 2021*. Ministry of Information Technology and Telecommunication.

Imran, D., & Murtaza, G. (2021). The rise of cybercrime in Pakistan: A threat to Pakistan national security. *Asian Journal of Social Science and Management Studies, 8*(2), 56–71.

Kemp, S. (2023). *Digital 2023: Pakistan*. Datareportal. https://datareportal.com/reports/digital-2023-pakistan
Khawar, A. (2019). Cybersecurity challenges in Pakistan's public and private sectors. *Business and Economic Review, 11*(2), 89–110.
Memon, M. (2016). Security of e-government services and challenges in Pakistan. *Proceedings of the International Conference on e-Government* (pp. 201–210). IEEE.
Microsoft. (2016). *Microsoft security intelligence report: Volume 21*. Microsoft Corporation.
Minhas, I. (2019). Hybrid warfare: The evolution of fifth-generation warfare. *Defence Journal, 23*(5), 12–24.
Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. *Global Security Review, 5*(3), 101–115.
Profit. (2024, March 10). Cyber-attacks on the financial sector in Pakistan: A surge in attacks. *Pakistan Today*.
ProPkstaff. (2024, February 15). Cybersecurity in Pakistan: Sector-specific vulnerabilities and threats. *ProPakistani*. https://propakistani.pk
Rafique, S. (2015). India’s cybersecurity strategy and its impact on Pakistan. *Strategic Analysis, 39*(5), 589–603.
Rafique, S. (2019). Cyber espionage and national security: Pakistan’s vulnerabilities in cyberspace. *Journal of Strategic Security, 12*(4), 1–18.
Rizwan, M. (2022). Cyber threat in a contemporary era: Challenges for the security of Pakistan. *South Asian Studies, 37*(1), 55–73.
Sadleer, P. (2012). Cybersecurity and the new age of warfare. *Journal of Digital Security Studies, 4*(1), 22–39.
Sahar, S. (2021). Cyber threats to Pakistan’s critical infrastructure and national security. *Pakistan Horizon, 74*(4), 7–28.
Salik, M. (2023). *Cybersecurity in Pakistan: Challenges and national security implications*. Islamabad Policy Research Institute.
Shad, M. (2019). Cyber crime in Pakistan: Trends and impacts on national security. *Crime and Justice Review, 14*(2), 88–105.
Tughral, Y. (2018). Cyber space management in Pakistan. In A. Khan (Ed.), *Digital frontiers of South Asia* (pp. 145–162). Academic Press.